



JPPI Vol 8 No 2 (2018) 97 - 107

Jurnal Penelitian Pos dan Informatika

771/AU1/P2MI-LIPI/08/2017

32a/E/KPT/2017

e-ISSN: 2476-9266

p-ISSN: 2088-9402

DOI:10.17933/jppi.2018.080201



SISTEM PENGAMAN PINTU RUMAH DENGAN TEKNOLOGI BIOMETRIK SIDIK JARI BERBASIS ARDUINO

HOME DOORLOCK SECURITY SYSTEM WITH BIOMETRIC FINGERPRINT BASED ON ARDUINO

Apri Siswanto¹, Ana Yulianti², Loneli Costaner³

^{1,2,3} Teknik Informatika, Fakultas Teknik, Universitas Islam Riau
Jalan Kaharuddin Nasution No. 113 Marpoyan, Pekanbaru 28284

¹ aprisiswanto@eng.uir.ac.id, ² anayulianti@eng.uir.ac.id, ³ lolyfrem@gmail.com

Naskah diterima: 7 Oktober 2017 ; Direvisi : 15 Maret 2018 ; Disetujui : 25 Juli 2018

Abstrak

Penggunaan konsep rumah cerdas dalam bidang sekuriti meningkat cukup signifikan akhir-akhir ini. Salah satu bidang yang menjadi perhatian adalah penggunaan teknologi *biometric* sidik jari untuk sistem otentikasi, misalnya otentikasi untuk masuk kedalam rumah. *Paper* ini bertujuan untuk menjelaskan sebuah *prototype* baru untuk otomasi dan keamanan pintu rumah yang mengkombinasikan teknologi biometrik sidik jari dan Arduino. Diharapkan sistem ini membantu meningkatkan keamanan dan kenyamanan para penghuni rumah dengan instalasi yang mudah dan biaya yang murah. Sistem ini secara otomatis mengontrol (buka atau tutup) pintu berdasarkan sidik jari pengguna yang telah didaftarkan dalam basis data di mikrokontroler Arduino. Sistem utamanya terdiri dari mikrokontroler Arduino, sensor sidik jari dan *doorlock system*.

Kata kunci: biometrik sidik jari, rumah cerdas, *smart home*, arduino, sekuriti

Abstract

The use of the concept of smart home across the field of security has increased significantly recently. One area of concern is the use of biometric fingerprint technology for authentication systems, such as authentication for entry to the home. This paper aims to explain a new prototype for home automation and home security that combines biometric fingerprint and arduino technology. It is expected that this system will help improve the safety and comfort to the residents with easy installation and low cost. This system automatically controls (open or close) doors based on user fingerprints that have been registered in the Arduino microcontroller database. The main system consists of arduino microcontroller, fingerprint sensor and door lock system.

Keywords: fingerprint biometrics, smart home, smart home, arduino, security,

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi saat ini menawarkan kemudahan kepada para pengguna dalam berbagai sendi kehidupan. Salah satu teknologi yang sedang tren dikembangkan adalah teknologi *smart home* atau biasa dikenal dengan istilah rumah cerdas. Rumah cerdas adalah istilah yang biasa digunakan untuk menentukan tempat tinggal yang memiliki peralatan, pencahayaan, pemanas, pendingin ruangan, TV, komputer, sistem audio dan video hiburan, keamanan, dan sistem kamera yang mampu berkomunikasi satu sama lain dan dapat dikendalikan dari jarak jauh dengan jadwal waktu tertentu, dari setiap ruangan di rumah, serta dari jarak jauh dari lokasi manapun di dunia melalui telepon atau internet. Sedangkan menurut Demiris and Hensel (2008), rumah cerdas adalah rumah yang menyediakan kenyamanan, keamanan, efisiensi energi bagi rumah, kenyamanan dan efisiensi setiap saat, terlepas dari apakah ada orang di rumah.

Ada beberapa kategori dalam fokus pengembangan rumah cerdas, diantaranya adalah dalam bidang akses kontrol dan otentikasi, keamanan, pengawasan dan perlindungan properti, pengendalian lingkungan dan produk hemat energi, distribusi hiburan dan audio, pengontrol rumah, pencahayaan dan kontrol alat. Pada makalah ini menjelaskan tentang rancangan prototipe rumah cerdas untuk keamanan pintu rumah atau garasi dengan sensor sidik jari dan mikrokontroler Arduino.

Keamanan merupakan perhatian utama dalam kehidupan kita sehari-hari, dan kunci digital telah menjadi bagian penting dari sistem

keamanan ini. Ada banyak jenis sistem keamanan yang tersedia untuk mengamankan rumah. Beberapa contohnya adalah, Sistem Keamanan berbasis RFID, *Digital Lock System*, sistem biometrik, Kunci Kode Elektronik.

Saat ini sistem biometrik menjadi pilihan untuk sistem otentikasi. Otentikasi biometrik berasal dari bahasa Yunani yaitu *bios* yang artinya hidup dan *metron* yang artinya mengukur, maka dapat diartikan sebagai studi tentang metode otomatis untuk mengenali manusia berdasarkan satu atau lebih bagian tubuh manusia atau kelakuan dari manusia itu sendiri yang memiliki keunikan. Dalam dunia teknologi informasi, biometrik relevan dengan teknologi yang digunakan untuk menganalisa fisik dan kelakuan manusia untuk autentikasi. Contohnya dalam pengenalan fisik manusia yaitu dengan pengenalan sidik jari, retina, iris, pola dari wajah (*facial patterns*), tanda tangan (*signature*) dan cara mengetik (*keystroke*). Di antara bagian tubuh manusia unik yang terdaftar, sidik jari adalah bagian yang paling sering digunakan untuk otentikasi. Hal ini diimplementasikan melalui teknologi pengenalan sidik jari (FRT) yang membandingkan pola sidik jari manusia untuk mengidentifikasi seseorang. Dalam konteks sistem keamanan rumah, sidik jari bisa digunakan oleh penghuni rumah untuk memberi otorisasi akses ke rumah dan membuka pintu atau pintu masuk utama lainnya. Karena sidik jari itu unik, akses ke rumah hanya akan diijinkan ke pihak yang berwenang saja. Mekanisme ini melindungi warga dan rumah agar tidak diakses oleh orang tak dikenal (Siswanto, Katuk, & Ku-Mahamud, 2016).



JPPI Vol 8 No 2 (2018) 97 - 107

Jurnal Penelitian Pos dan Informatika

771/AU1/P2MI-LIPI/08/2017

32a/E/KPT/2017

e-ISSN: 2476-9266

p-ISSN: 2088-9402

DOI:10.17933/jppi.2018.080201



SISTEM PENGAMAN PINTU RUMAH DENGAN TEKNOLOGI BIOMETRIK SIDIK JARI BERBASIS ARDUINO

HOME DOORLOCK SECURITY SYSTEM WITH BIOMETRIC FINGERPRINT BASED ON ARDUINO

Apri Siswanto¹, Ana Yulianti², Loneli Costaner³

^{1,2,3} Teknik Informatika, Fakultas Teknik, Universitas Islam Riau
Jalan Kaharuddin Nasution No. 113 Marpoyan, Pekanbaru 28284

¹ aprisiswanto@eng.uir.ac.id, ² anayulianti@eng.uir.ac.id, ³ lolyfrem@gmail.com

Naskah diterima: 7 Oktober 2017 ; Direvisi : 15 Maret 2018 ; Disetujui : 25 Juli 2018

Abstrak

Penggunaan konsep rumah cerdas dalam bidang sekuriti meningkat cukup signifikan akhir-akhir ini. Salah satu bidang yang menjadi perhatian adalah penggunaan teknologi *biometric* sidik jari untuk sistem otentikasi, misalnya otentikasi untuk masuk kedalam rumah. *Paper* ini bertujuan untuk menjelaskan sebuah *prototype* baru untuk otomasi dan keamanan pintu rumah yang mengkombinasikan teknologi biometrik sidik jari dan Arduino. Diharapkan sistem ini membantu meningkatkan keamanan dan kenyamanan para penghuni rumah dengan instalasi yang mudah dan biaya yang murah. Sistem ini secara otomatis mengontrol (buka atau tutup) pintu berdasarkan sidik jari pengguna yang telah didaftarkan dalam basis data di mikrokontroler Arduino. Sistem utamanya terdiri dari mikrokontroler Arduino, sensor sidik jari dan *doorlock system*.

Kata kunci: biometrik sidik jari, rumah cerdas, *smart home*, arduino, sekuriti

Abstract

The use of the concept of smart home across the field of security has increased significantly recently. One area of concern is the use of biometric fingerprint technology for authentication systems, such as authentication for entry to the home. This paper aims to explain a new prototype for home automation and home security that combines biometric fingerprint and arduino technology. It is expected that this system will help improve the safety and comfort to the residents with easy installation and low cost. This system automatically controls (open or close) doors based on user fingerprints that have been registered in the Arduino microcontroller database. The main system consists of arduino microcontroller, fingerprint sensor and door lock system.

Keywords: fingerprint biometrics, smart home, smart home, arduino, security,



JPPI Vol 8 No 2 (2018) 97 - 107

Jurnal Penelitian Pos dan Informatika

771/AU1/P2MI-LIPI/08/2017

32a/E/KPT/2017

e-ISSN: 2476-9266

p-ISSN: 2088-9402

DOI:10.17933/jppi.2018.080201



SISTEM PENGAMAN PINTU RUMAH DENGAN TEKNOLOGI BIOMETRIK SIDIK JARI BERBASIS ARDUINO

HOME DOORLOCK SECURITY SYSTEM WITH BIOMETRIC FINGERPRINT BASED ON ARDUINO

Apri Siswanto¹, Ana Yulianti², Loneli Costaner³

^{1,2,3} Teknik Informatika, Fakultas Teknik, Universitas Islam Riau
Jalan Kaharuddin Nasution No. 113 Marpoyan, Pekanbaru 28284

¹ aprisiswanto@eng.uir.ac.id, ² anayulianti@eng.uir.ac.id, ³ lolyfrem@gmail.com

Naskah diterima: 7 Oktober 2017 ; Direvisi : 15 Maret 2018 ; Disetujui : 25 Juli 2018

Abstrak

Penggunaan konsep rumah cerdas dalam bidang sekuriti meningkat cukup signifikan akhir-akhir ini. Salah satu bidang yang menjadi perhatian adalah penggunaan teknologi *biometric* sidik jari untuk sistem otentikasi, misalnya otentikasi untuk masuk kedalam rumah. *Paper* ini bertujuan untuk menjelaskan sebuah *prototype* baru untuk otomasi dan keamanan pintu rumah yang mengkombinasikan teknologi biometrik sidik jari dan Arduino. Diharapkan sistem ini membantu meningkatkan keamanan dan kenyamanan para penghuni rumah dengan instalasi yang mudah dan biaya yang murah. Sistem ini secara otomatis mengontrol (buka atau tutup) pintu berdasarkan sidik jari pengguna yang telah didaftarkan dalam basis data di mikrokontroler Arduino. Sistem utamanya terdiri dari mikrokontroler Arduino, sensor sidik jari dan *doorlock system*.

Kata kunci: biometrik sidik jari, rumah cerdas, *smart home*, arduino, sekuriti

Abstract

The use of the concept of smart home across the field of security has increased significantly recently. One area of concern is the use of biometric fingerprint technology for authentication systems, such as authentication for entry to the home. This paper aims to explain a new prototype for home automation and home security that combines biometric fingerprint and arduino technology. It is expected that this system will help improve the safety and comfort to the residents with easy installation and low cost. This system automatically controls (open or close) doors based on user fingerprints that have been registered in the Arduino microcontroller database. The main system consists of arduino microcontroller, fingerprint sensor and door lock system.

Keywords: fingerprint biometrics, smart home, smart home, arduino, security,

Dalam penelitian ini akan mengimplementasikan biometrik sidik jari dengan mikrokontroler Arduino untuk membangun prototipe sidik jari penguncian pintu rumah atau garasi. Arduino merupakan *platform* elektronik *open source* yang berbasis pada perangkat keras dan perangkat lunak yang mudah digunakan. Papan Arduino dapat membaca masukan, menyalakan sensor, merekap data sidik jari pada tombol, dan mengubahnya menjadi *output*, kemudian dapat juga mengaktifkan motor, menyalakan LED, mempublikasikan sesuatu secara *online*. Arduino dapat melakukan suatu pengiriman satu set instruksi ke mikrokontroler di papan elektronik (*board*). Untuk melakukannya Arduino didukung bahasa pemrograman Arduino yang biasa dikenal dengan nama IDE Arduino.

Selanjutnya sidik jari dianggap sebagai salah satu kunci teraman untuk mengunci atau membuka sistem apapun karena dapat mengenali seseorang secara unik dan tidak dapat ditiru dengan mudah (Shankar, Sastry, Ram, & Vamsidhar, 2015). Sidik jari digunakan untuk proses otentikasi, dimana hanya user yang terdaftar di basis data saja, yang diizinkan untuk bisa masuk mengakses rumah secara sah.

Kajian Terdahulu

Pada penelitian ini untuk mendapatkan hasil penelitian yang optimal, penulis melakukan kajian dari penelitian-penelitian terdahulu yang berkaitan dengan penelitian ini sehingga bisa dijadikan referensi dalam penelitian.

Ada beberapa kajian penelitian yang sudah dilakukan peneliti-peneliti sebelumnya, di antaranya penelitian yang dilakukan Adriansyah

and Dani (2014) yaitu *Design of Small Smart Home Sistem Based on Arduino*. Pada penelitian ini menawarkan rancangan rumah cerdas dengan memanfaatkan jaringan WLAN berbasis mikrokontroler Arduino. Sistem ini mampu memantau dan mengontrol lampu rumah, suhu kamar, alarm dan peralatan rumah tangga lainnya. Hasil dari pengujian menunjukkan sistem kontrol yang tepat dan pemantauan fungsi kontrol bisa dilakukan dari perangkat yang terhubung ke jaringan yang mendukung HTML5.

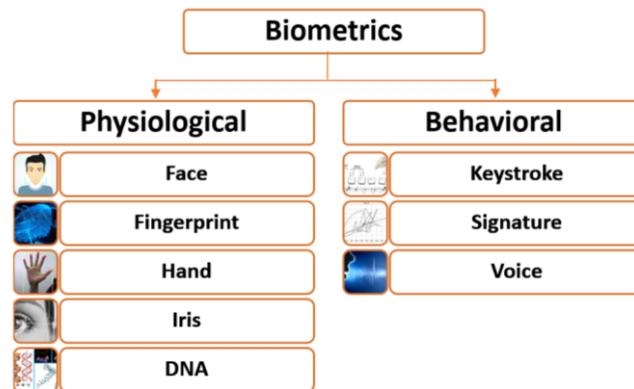
Penelitian berikutnya dilakukan oleh Ishengoma (2014), yang berjudul *Authentication Sistem for Smart Homes Based on ARM7TDMI-S and IRIS-Fingerprint Recognition Technologies*. Pada penelitian ini menyajikan pendekatan untuk merancang sebuah sistem otentikasi untuk rumah cerdas berbasis pada IRT, FRT dan sistem mikrokontroler ARM7TDMI-S. Sistem mempekerjakan dua mekanisme biometrik untuk keandalan yang tinggi dimana pada awalnya, sistem pengguna harus mendaftarkan sidik jari dan mata mereka ke kamera. Iris dan sidik jari kemudian *discan* dan gambar disimpan dalam database. Pada tahap otentikasi, FRT dan IRT sidik jari memindai dan menganalisis poin dari iris masukan pengguna dan sidik jari sehingga sesuai dengan isi *database*. Jika satu atau lebih foto yang diambil lakukan pencocokan dalam satu *database*, maka sistem tidak akan memberikan otorisasi.

Tobing (2014) melakukan penelitian tentang rancang bangun pengaman pintu menggunakan sidik jari dan *smartphone* android berbasis mikrokontroler Atmega 8. Pada sistem keamanan ini peneliti membuat sistem keamanan rumah menggunakan sidik jari sebagai alat akses

masuk ke rumah serta menggabungkan selenoid sebagai pengaman tambahan dan bluetooth digunakan untuk mengirimkan kondisi dari pintu ketika dalam posisi terbuka dan tertutup.

Sistem Biometrik

Sebuah sistem biometrik pada dasarnya adalah sebuah sistem pengenalan pola untuk menentukan atau memverifikasi seseorang berdasarkan pada fitur yang berasal dari karakteristik fisiologis atau perilaku tertentu yang dimiliki seseorang. (Prabhakar, Pankanti, & Jain, 2003). Karakteristik fisiologis atau perilaku yang khas, menyediakan pengukuran dasar biometrik. Biometrik fisiologis didasarkan pada pengukuran langsung dari bagian tubuh manusia, seperti sidik jari (*fingerprint*), pengenalan iris (*iris recognition*), pengenalan retina dan pengenalan wajah (*face recognition*). Sedangkan biometrik perilaku (*behaviour*) didasarkan pada pengukuran dan data yang berasal dari tindakan, karena itu secara tidak langsung mengukur karakteristik tubuh manusia, seperti tanda tangan, suara, dan ketikan di komputer. Dalam biometrik perilaku biasanya memerlukan waktu yang lebih lama untuk verifikasi dibandingkan biometrik fisiologis. Terdapat 2 terminologi pada biometrik, yaitu verifikasi dan identifikasi. Verifikasi adalah mencocokkan pengguna biometrik untuk mengklaim satu identitas, sedangkan identifikasi adalah membandingkan pengguna biometrik untuk semua orang lain dalam *database* untuk memastikan mereka tidak terdaftar sebelumnya. Bagan karakteristik dari biometrik dapat dilihat dari gambar di bawah ini :



Gambar 1. Karakteristik Teknologi Biometrik

Dalam beberapa tahun terakhir, sistem biometrik banyak digunakan untuk mengotentikasi dan mengidentifikasi individu, untuk mengenali identitas pengguna dengan cara yang aman. Sistem semacam ini telah dikembangkan oleh para peneliti untuk tujuan mengamankan *platform* perangkat lunak dan perangkat keras. Walaupun sistem biometrik dapat meningkatkan kenyamanan dan keamanan pengguna, namun juga rentan terhadap berbagai ancaman. Menurut D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar (2009b) ancaman yang mungkin terjadi pada sistem biometrik adalah sebagai berikut :

1. *Denial of service (DoS)*: Penyusup merusak sistem biometrik sehingga pengguna yang sah tidak dapat mengakses sistem.
2. *Repudiation (Penolakan)*: Pengguna yang sah tidak mengakui atau mengetahui bahwa dia telah mengakses sistem. Misalnya, dalam distribusi manfaat kesejahteraan pemerintah, pengguna yang berwenang mungkin akan menerima manfaatnya, dan kemudian menyangkal bahwa dia telah menerima manfaat apa pun.
3. *Circumvention* : Pengguna yang tidak sah secara tidak sah mengakses sistem dan data.

Penyingkapan bisa berupa serangan privasi atau serangan subversif. Dalam serangan privasi, penyusup mendapatkan akses ke data yang mungkin tidak diizinkan untuk diakses. Dalam serangan subversif, penyusup dapat memanipulasi sistem untuk menggunakannya untuk aktivitas ilegal.

4. *Collusion* : Beberapa pengguna memiliki status *super-user* yang memungkinkan mereka untuk melewati komponen pengenalan dan menolak keputusan yang dibuat oleh sistem. Fasilitas ini tergabung dalam alur kerja sistem untuk memungkinkan penanganan situasi luar biasa, misalnya pengolahan individu tanpa jari dalam sistem pengenalan berbasis sidik jari. Hal ini berpotensi menyebabkan penyalahgunaan sistem dengan cara kolusi antara pengguna super dan pengguna lainnya. Seringkali disebutkan bahwa cara termudah untuk memecahkan sistem keamanan adalah dengan kompromi dengan administrator sistem.

5. *Coercion* : Pengguna asli berpotensi dipaksa untuk mengidentifikasi diri mereka sendiri. Pengukuran pengakuan dapat diperoleh secara paksa dari pengguna untuk mendapatkan akses ke sistem. Misalnya, pengguna mesin *teller* otomatis (ATM) dapat dipaksa untuk memberikan kartu ATM dan nomor identifikasi pribadinya (PIN) dengan todongan senjata. Penting untuk mendeteksi paksaan dengan andal tanpa membahayakan kehidupan pengguna asli.

6. Kontaminasi atau akuisisi terselubung: Cara pengakuan mungkin bisa dikompromikan tanpa sepengetahuan pengguna yang sah. Mereka kemudian bisa disalahgunakan. Misalnya, sidik jari pengguna yang sah bisa diangkat oleh musuh. Musuh kemudian menciptakan cetakan tiga

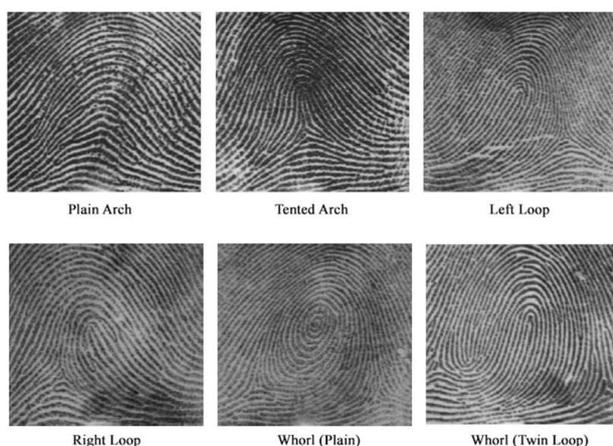
dimensi dan menggunakan cetakan untuk mendapatkan akses. Sidik jari untuk satu aplikasi dapat digunakan untuk aplikasi lain.

Sidik Jari

Sebuah sidik jari adalah pola seperti *ridge* (gundukan) dan alur-alur yang terletak di ujung setiap jari. Sidik jari telah digunakan untuk identifikasi pribadi selama berabad-abad dengan akurasi kecocokan sangat tinggi (Maio, Maltoni, Cappelli, Wayman, & Jain, 2002). Sidik jari juga merupakan garis yang muncul di kulit ujung jari. Sidik jari bekerja untuk memberi gaya gesek yang lebih besar agar jari bisa menahan benda lebih dekat (Purbani, 2010). Sistem keamanan sidik jari sudah digunakan di Amerika Serikat oleh E. Henry pada tahun 1902. Henry menggunakan metode sidik jari untuk identifikasi pekerja dalam rangka mengatasi masalah upah. Salah satu alasan untuk memilih sidik jari dalam penelitian ini didasarkan pada popularitas penggunaan sidik jari. Sidik jari banyak digunakan di berbagai bidang seperti untuk sistem absensi, imigrasi, akses ke bangunan rumah dan lain-lain. Sidik jari adalah pilihan utama untuk keunggulan sebagai pengenal biometrik, sidik jari telah lama digunakan untuk tujuan otentikasi. Keandalan dan keunggulan sidik jari dalam sistem otentikasi telah melampaui jenis biometrik lainnya seperti wajah atau iris. Pada saat yang sama, karena penurunan biaya dan ukuran sensor sidik jari, sangat mungkin sidik jari terus digunakan secara luas dalam sistem pengenalan biometrik di masa depan. Dalam laporan pasar biometrik baru-baru ini, sebuah rangkuman yang tersedia di Wall Street Journal, memperkirakan bahwa pengenalan

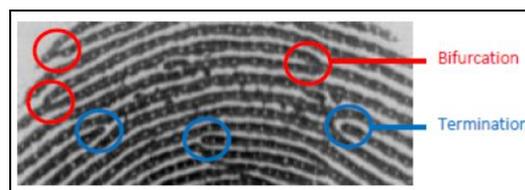
sidik jari akan terus mendominasi pasar biometrik di masa depan.

Sidik jari terdiri dari pola gunung *interleaved* (bagian yang naik ke atas) dan sebuah lembah (*dips*). Langkah pertama dalam pengenalan sidik jari biasanya melibatkan pengkategorian sidik jari menjadi satu dari lima kelas dasar, yang disebut kelas Henry terdiri dari *Plain Arch*, *Tented Arch*, *Left Loop*, *Right Loop*, dan *Whorl* (*Whorl* terbagi menjadi dua lingkaran polos dan kembar) (D. Maltoni, D. Maio, A. Jain, & S. Prabhakar, 2009a).



Gambar 2. Pola Sidik Jari (Krivokuca, 2015)

Langkah kedua dalam pengenalan sidik jari adalah menganalisa sidik jari di tingkat lokal. Analisis tingkat lokal melibatkan pemeriksaan diskontinuitas *ridge* kecil yang disebut *minutiae*. Dua jenis *minutiae* yang paling umum adalah bifurkasi hubungan dan penghentian *ridge*. Pada bifurkasi terjadi pada titik di mana garis punggung mengarah ke dua segmen terpisah, sedangkan penghentiannya adalah ujung punggungnya yang prematur. Sidik jari yang khas mengandung hingga 80 hal kecil, namun lebih sedikit lagi yang akan ada pada gambar yang diambil dari pemindai biasa yang digunakan dalam sistem biometrik karena tangkapan-tangkapan kecil.



Gambar 3. Tipe *minutiae* sidik jari. (Krivokuca, 2015)

Sensor sidik jari akan mencari titik-titik ini dan membuat pola dengan menghubungkan-hubungkan titik-titik tersebut. Pola yang didapat dari menghubungkan titik-titik inilah yang nantinya akan digunakan untuk melakukan pencocokan bila ada jari yang dipindai. Jadi, sebenarnya mesin sidik jari tidak mencocokkan gambar, tapi mencocokkan pola yang didapat dari *minutiae-minutiae* ini.

Sensor sidik jari bekerja dengan mengambil gambar dari sidik jari dan membedakan setiap pola atau alur dari sidik jari tersebut. Sebenarnya banyak cara dapat dilakukan untuk mengambil gambar dari sidik jari tersebut, namun metode umum yang dilakukan adalah dengan menggunakan 2 (dua) cara, yaitu dengan sensor optikal dan sensor kapasitansi.

Arduino

Arduino merupakan suatu sistem *platform* berbasis *open source* yang dapat digunakan untuk membuat prototipe proyek elektronika. Arduino terdiri dari papan sirkuit, yang dapat diprogram biasa dikenal dengan mikrokontroler dan perangkat lunak siap pakai yang disebut Arduino IDE (*Integrated Development Environment*), yang digunakan untuk menulis dan mengunggah kode komputer ke papan fisik. Ketika membicarakan Arduino maka ada dua hal yang terlintas dalam pikiran

para penggunanya, yaitu *hardware* dan *software*. Dua bagian ini seakan satu kesatuan utuh yang tidak bisa di pisahkan (Bell, 2014).

Mikrokontroler Arduino dapat membaca sinyal *input analog* atau *digital* dari sensor yang berbeda dan mengubahnya menjadi *output* seperti mengaktifkan motor, menyalakan LED *on/off*, terhubung ke internet dan banyak aksi lainnya. User dapat mengontrol fungsi *board* dengan mengirimkan satu set instruksi ke mikrokontroler di papan tulis melalui Arduino IDE (disebut sebagai perangkat lunak pengunggahan). Arduino tidak memerlukan perangkat keras tambahan (disebut pemrogram) untuk memuat kode baru ke papan tulis, cukup menggunakan kabel USB.



Gambar 4. Arduino (Evans, Noble, & Hochenbaum, 2013)

METODE PENELITIAN

Lokasi Penelitian

Penelitian ini dilaksanakan di Laboratorium Jaringan Komputer Fakultas Teknik Universitas Islam Riau Pekanbaru, hal ini dikarenakan saat ini beberapa fasilitas dan alat yang mendukung hanya terdapat di dalam laboratorium tersebut.

Tahapan Penelitian

Metodologi yang digunakan dalam penelitian ini adalah eksperimental yang dibagi menjadi empat tahap yaitu (Ross & Morrison) :

a. Studi Literatur

Metode ini dilakukan untuk mencari dan mendapatkan sumber-sumber kajian yang berkaitan, landasan teori yang mendukung, data-data, atau informasi sebagai acuan dalam melakukan perencanaan, desain, pembuatan, percobaan, dan penyusunan laporan penelitian.

b. Desain Rancangan Perangkat Keras

Metode ini dimaksudkan untuk menghasilkan suatu rangkaian alat sensor *fingerprint* dan mikrokontroler Arduino yang tepat sehingga diperoleh hasil rancangan yang sesuai dengan tujuan penelitian.

c. Pembuatan Koding

Tahap ini adalah penyusunan kode-kode program untuk mengintegrasikan antara sensor dan Arduino agar dapat mendaftarkan dan mengotentikasi user penghuni rumah.

d. Pengujian

Metode ini dilakukan untuk penyesuaian antara perencanaan dan hasil yang telah dicapai sehingga diharapkan tidak adanya penyimpangan (*error*) yang tidak diinginkan, sehingga akan sesuai dengan apa yang telah direncanakan.

e. Pengambilan Kesimpulan

Metode ini dilakukan dalam perencanaan, pembuatan, dan pengujian alat kerja sehingga didapatkan komponen dan rancangan yang

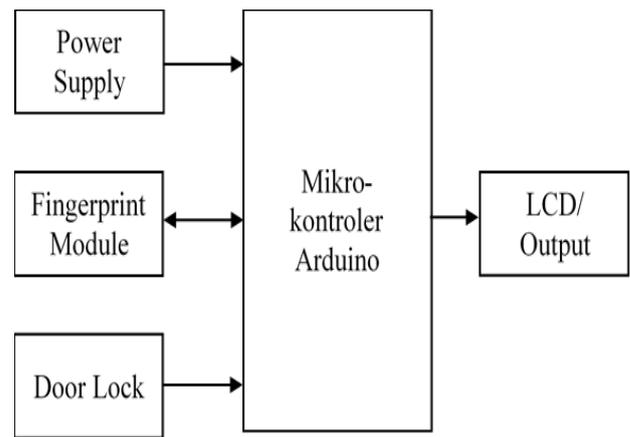
prototipe yang benar dan baik. Secara umum metodologi penelitian dapat dilihat pada gambar 5 di bawah ini.



Gambar 5. Metodologi Penelitian

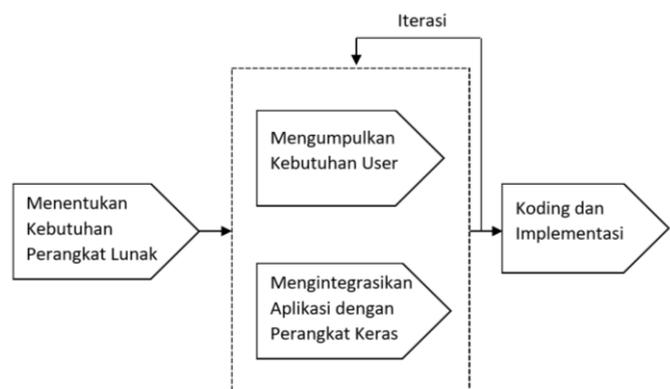
Desain Rancangan Perangkat Keras

Pada model rancangan penelitian ini akan dibuat desain *hardware* yang terdiri dari Arduino sebagai mikrokontroler dan untuk penyediaan *input/output*. Selain itu ada juga *scanner fingerprint*, komponen ini digunakan untuk menangkap sidik jari dari pengguna. Ketika digunakan pada saat pertama, pengguna akan menempatkan jarinya pada perangkat ini, dan perangkat akan menangkap sidik jarinya serta menyimpan dalam *database*. Untuk tahap otentikasi, pengguna akan menempatkan jarinya, dan perangkat akan menangkap gambar dan membandingkan data dengan yang disimpan dalam *database*. Selanjutnya direncanakan juga dalam model rancangan terdapat LCD untuk menampilkan akses data di terima dan yang ditolak.



Gambar 6. Blok Diagram Rancangan

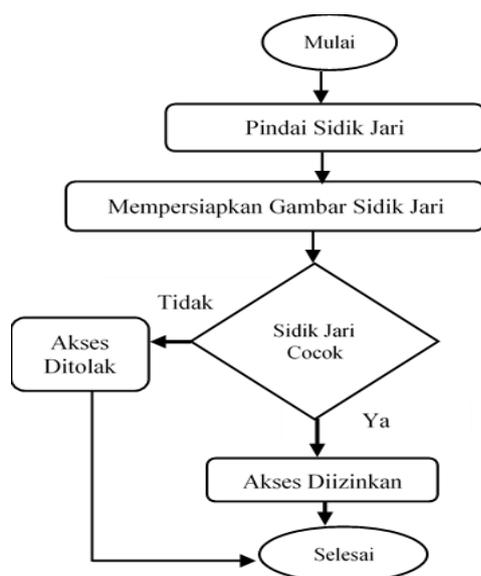
Adapun tahapan dari perancangan perangkat lunak adalah yang pertama menentukan kebutuhan perangkat lunak dari aplikasi yang akan dibangun, kemudian mengumpulkan dan menganalisa kebutuhan user. Bersamaan dengan itu juga mengintegrasikan aplikasi dengan perangkat keras. Kemudian tahapan berikutnya adalah koding dan implementasi. Tahapan ini juga dapat kembali pada tahapan tengah karena aplikasi dibangun dengan metode perulangan program atau iterasi. Seperti yang ditunjukkan pada gambar 7 di bawah ini.



Gambar 7. Tahapan Rancangan perangkat Lunak

HASIL DAN PEMBAHASAN

Penelitian ini bertujuan untuk menerapkan sensor sidik jari untuk kendali di pintu utama rumah dan garasi. Saat sistem ini diimplementasikan di rumah, penghuni yang berwenang diminta untuk mendaftarkan data sidik jari mereka dengan aplikasi sederhana dan data akan disimpan di memori mikrokontroler Arduino. Penghuni memindai sidik jari mereka dengan menggunakan sensor sidik jari. Hasil pemindaian disimpan dalam format digital di memori Arduino. Setelah itu, catatan sidik jari diproses dengan memproduksi daftar fitur corak yang unik. Fitur pola sidik jari disimpan dalam *database*. Saat penghuni memindai jari mereka, pola yang dihasilkan dari sidik jari akan disesuaikan dengan yang tersimpan dalam *database*. Jika kedua data cocok, maka memori Arduino mengirimkan sinyal persetujuan ke mikrokontroler untuk membuka pintu dan memberikan akses ke penghuninya. Diagram alir pada Gambar 8 menunjukkan aliran proses sistem kendali pintu yang telah dirancang.



Gambar 8. Diagram alir proses pendaftaran dan otentikasi

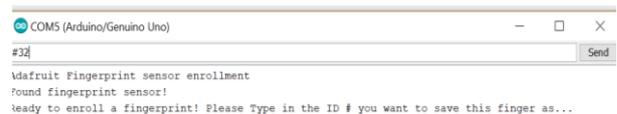
Adapun hasil rancangan prototipe yang telah dibuat adalah sebagai berikut :



Gambar 9. Hasil Rancangan Prototipe

Proses Pendaftaran dan Otentikasi

Dalam proses pendaftaran *user* sidik jari, disini dibuat koding sederhana dari Arduino IDE. Seorang *user* harus mendaftarkan sidik jarinya agar dapat dikenali di dalam basis data mikrokontroler Arduino. Setelah terdaftar maka *user* akanizinkan untuk akses ke dalam prototipe rumah yang sudah dirancang. Berikut ini adalah gambar dari proses pendaftaran dan otentikasi sidik jari untuk pengaman pintu rumah cerdas.



Gambar 10. Kode Program Pendaftaran Sidik Jari

Pada gambar 10 di atas, pertama user harus mendaftarkan salah satu sidik jari, langkah pertama adalah perekaman data digital, kemudian verifikasi untuk memastikan bahwa proses

perekaman selesai dan juga proses pengubahan sidik jari menjadi *template* berhasil. Setelah berhasil direkam ke dalam *database*, maka *template* sidik jari yang terdaftar akan diizinkan untuk mengakses lingkungan rumah. Pada koding juga disediakan penanganan untuk menghapus *user* yang diinginkan oleh pemilik rumah.



Gambar 11. Proses pendaftaran dan otentikasi yang benar

Sedangkan untuk *user* yang tidak terdaftar dalam *database* maka sistem secara otomatis akan menolak untuk dapat akses ke pintu rumah. Inilah salah satu keunggulan dari sistem biometrik dimana tidak ada alasan lupa *password* atau kunci karena semuanya dapat dilakukan dengan teknologi biometrik baik pada kategori fisik tubuh atau perilaku manusia. Untuk keterangan mengenai sidik jari yang ditolak oleh sistem keamanan pintu dengan menggunakan mikrokontroler Arduino dapat dilihat pada gambar 11.

Berdasarkan pengujian yang dilakukan dengan beberapa sidik jari peneliti, maka prototipe ini mampu bekerja dengan baik dalam merekam data dan mengotentikasi pengguna yang terdaftar dalam *database*.



Gambar 12. Sidik jari yang ditolak

Tabel 1. Pengujian prototipe sidik jari

Sidik Jari	Pendaftaran	Otentikasi
Jempol	Berhasil	Berhasil
Telunjuk	Berhasil	Berhasil
Jari Tengah	Berhasil	Berhasil
Jari Manis	Berhasil	Berhasil
Kelingking	Berhasil	Berhasil

Sistem sidik jari biometrik memberikan solusi yang baik untuk keamanan pintu rumah. Sebuah prototipe baru dari sidik jari biometrik hemat biaya teknologi yang diusulkan dalam makalah ini. Ini memberi ide dasar bagaimana mengintegrasikan kunci pintu, sensor sidik jari, mikrokontroler Arduino dan *door lock* dengan aplikasi sederhana. Sebagai tren pada sistem keamanan biometrik, arsitektur ini akan membutuhkan implementasi dalam sistem nyata sehingga sistem ini dapat memberikan manfaat yang lebih baik. Kedepannya akan tercipta untuk perancangan perangkat keras dan perangkat lunak untuk melihat kemampuan sistem ini dalam mengamankan rumah. Penulis memprediksikan arsitektur ini sangat ekonomis.

PENUTUP

Penggunaan sidik jari biometrik untuk sistem keamanan pintu rumah menggunakan mikrokontroler Arduino bisa menjadi salah satu alternatif untuk keamanan rumah yang andal dan rendah biaya. Semua komponen yang digunakan relatif murah dan banyak tersedia di pasaran. Diharapkan sistem ini dapat menyediakan fungsi yang serupa dengan sistem riil untuk pengaman rumah.

UCAPAN TERIMA KASIH

Penelitian ini didukung oleh Direktorat Riset dan Pengabdian Masyarakat, Direktorat Jenderal Penguatan Riset dan Pengembangan Kementerian Riset, Teknologi, dan Pendidikan Tinggi (RISTEKDIKTI) dengan Skema Hibah Penelitian Dosen Pemula (Kontrak Penelitian Nomor: 130/KONTRAK/LP-UIR/4-2017)

DAFTAR PUSTAKA

- Adriansyah, A., & Dani, A. W. (2014). *Design of small smart home system based on Arduino*. Paper presented at the Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS), 2014.
- Bell, C. (2014). *Beginning sensor networks with Arduino and Raspberry Pi*: Apress.
- Demiris, G., & Hensel, B. K. (2008). Technologies for an aging society: a systematic review of "smart home" applications. *Yearb Med Inform*, 3, 33-40.
- Evans, M., Noble, J. J., & Hochenbaum, J. (2013). *Arduino in action*: Manning New York.
- Ishengoma, F. R. (2014). Authentication System for Smart Homes Based on ARM7TDMI-S and IRIS-Fingerprint Recognition Technologies. *arXiv preprint arXiv:1410.0534*.
- Krivokuca, V. (2015). *Fingerprint Template Protection using Compact Minutiae Patterns*. ResearchSpace@ Auckland.
- Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., & Jain, A. K. (2002). FVC2000: Fingerprint verification competition. *IEEE transactions on pattern analysis and machine intelligence*, 24(3), 402-412.
- Maltoni, D., Maio, D., Jain, A., & Prabhakar, S. (2009a). *Handbook of fingerprint recognition*: Springer Science & Business Media.
- Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009b). Securing Fingerprint Systems. *Handbook of Fingerprint Recognition*, 371-416.
- Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: Security and privacy concerns. *IEEE security & privacy*, 99(2), 33-42.
- Ross, S. M., & Morrison, G. R. Experimental research methods.
- Shankar, A. A., Sastry, P., Ram, A. V., & Vamsidhar, A. (2015). Finger Print Based Door Locking System. *International Journal Of Engineering And Computer Science*, 4(3), 10810-10814.
- Siswanto, A., Katuk, N., & Ku-Mahamud, K. R. (2016). Biometric fingerprint architecture for home security system.
- Tobing, S. L. (2014). Rancang Bangun Pengaman Pintu Menggunakan Sidik Jari (Fingerprint) Dan Smartphone Android Berbasis Mikrokontroler Atmega8. *Jurnal Teknik Elektro Universitas Tanjungpura*, 1(1).