



***SMART HOME SECURITY SYSTEM***  
**BERBASIS ARDUINO**

**Skripsi**

**diajukan sebagai salah satu persyaratan untuk memperoleh gelar  
Sarjana Pendidikan Program Studi Pendidikan Teknik Elektro**

**Oleh**

**Jalu Wardoyo**

**NIM.5301412026**

**PENDIDIKAN TEKNIK ELEKTRO  
JURUSAN TEKNIK ELEKTRO  
FAKULTAS TEKNIK  
UNIVERSITAS NEGERI SEMARANG  
2018**

## PENGESAHAN

Skripsi dengan judul *Smart Home Security System* Berbasis Arduino telah dipertahan di depan sidang Panitia Ujian Skripsi Fakultas Teknik UNNES pada tanggal 24 bulan Oktober tahun 2018

Nama : Jalu Wardoyo  
NIM : 5301412026  
Program Studi : Pendidikan Teknik Elektro

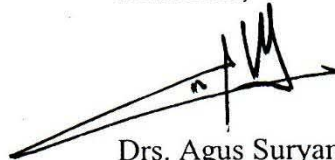
Panitia,

Ketua Panitia,



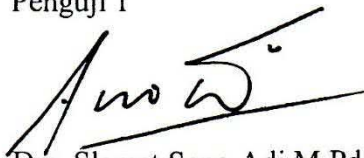
Dr. -Ing. Dhidik Prastiyanto, S.T.,M.T  
NIP. 197805312005011002

Sekretaris,



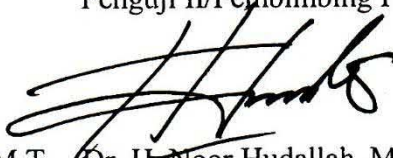
Drs. Agus Suryanto M.T.  
NIP. 196708181992031004

Penguji I



Drs. Slamet Seno Adi M.Pd., M.T  
NIP. 195812181985031004

Penguji II/Pembimbing I



Dr. H. Noor Hudallah, M.T.  
NIP. 196410161989011001

Penguji III/Pembimbing



Aryo Baskoro Utomo, S  
NIP. 198409092012121

Mengetahui;

Decan Fakultas Teknik UNNES



Dr. Nur Qudus, M.T

NIP. 196911301994031001

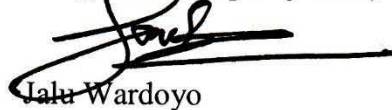
## PERNYATAAN KEASLIAN

Dengan ini saya menyatakan bahwa:

1. Skripsi ini, adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (sarjana, magister, dan/atau doktor), baik di Universitas Negeri Semarang (UNNES) maupun di perguruan tinggi lain.
2. Karya tulis ini adalah murni gagasan, rumusan, dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan Pembimbing dan masukan Tim Penguji.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya ini, serta sanksi lainnya sesuai dengan norma yang berlaku di perguruan tinggi ini.

Semarang, 20 Oktober 2018

Yang membuat pernyataan,



Jala Wardoyo

NIM, 5301412026

## ABSTRAK

Jalu Wardoyo. 2018. *Smart Home Security System Berbasis Arduino*. Skripsi, Pendidikan Teknik Elektro, Fakultas Teknik, Universitas Negeri Semarang. Pembimbing: Dr. H. Noor Hudallah, M.T., Aryo Baskoro Utomo, S.T., M.T.

Penelitian ini dilatarbelakangi oleh tingginya tindak kejahatan di rumah tangga terutama tindak pencurian. Tingginya tindak pencurian di rumah tangga dapat diantisipasi dengan penggunaan sistem pengaman rumah yang lebih modern salah satunya yaitu *smart home*. Salah satu aplikasi sistem *smart home* adalah *safety system*. *Safety system* merupakan sebuah sistem yang terintegrasi baik *hardware* maupun *software* yang berfungsi sebagai pengaman untuk mencegah kerusakan maupun kerugian. Tujuan penelitian ini adalah mengembangkan dan menguji *safety system* menggunakan kombinasi *biometric fingerprint* dan *password* terhadap akses pintu.

Metode yang digunakan adalah *Research and Development (RnD)*. Proses penelitian *RnD* dibagi menjadi tiga tahap yaitu tahap studi, tahap *research*, dan pengembangan. Tahapan studi meliputi studi pustaka, studi lapangan terhadap sistem pengaman rumah, dan analisis data. Tahap *research* yang dilakukan adalah mendesain dan membuat *prototype* alat, melakukan pengujian dan revisi pada uji ahli dan *black box*. Pada tahap pengembangan dilakukan pengujian pengguna untuk mengetahui efektifitas dan efisiensi alat serta revisi apabila terdapat kekurangan sebelum dinyatakan sebagai hasil akhir.

Penelitian ini menghasilkan sistem keamanan dengan kombinasi metode pengaman *biometric fingerprint* dan *password* berbasis Arduino. Arduino yang digunakan berupa *board* Arduino Mega dengan IC 2560. Mekanisme penguncian pintu menggunakan solenoid *door lock*. Sistem keamanan ini memiliki fitur tambahan berupa *emergency backup supply* dan *emergency entry* dengan modul *bluetooth* HC-05. Sistem keamanan ini telah melalui beberapa pengujian seperti uji ahli, uji *black box*, dan uji pengguna. Analisa terhadap hasil uji ahli menunjukkan skor 80,8% dengan kategori “baik”, hasil uji *black box* menunjukkan *software* dapat bekerja sesuai desain rancangan, dan hasil uji pengguna memperoleh skor 84,33% dengan kategori “sangat baik”. Secara keseluruhan alat tersebut telah memenuhi berbagai kriteria uji dan dinyatakan layak digunakan sebagai sistem pengaman rumah.

**Kata kunci:** *smart home, safety system, biometric, fingerprint, password, research and development.*

## **KATA PENGANTAR**

Puji syukur Alhamdulillah peneliti panjatkan kehadiran Allah SWT yang telah melimpahkan nikmat, rahmat, taufik, dan hidayah-Nya, sehingga penulisan skripsi ini dapat diselesaikan dengan baik.

Laporan skripsi ini disusun guna memenuhi salah satu syarat untuk menyelesaikan Program Studi Pendidikan Teknik Elektro Jurusan Teknik Elektro Fakultas Teknik Universitas Negeri Semarang. Keberhasilan peneliti dalam menyusun skripsi ini tidak terlepas dari bantuan, dorongan, serta doa dari berbagai pihak baik secara langsung maupun tidak langsung. Pada kesempatan ini, dengan segala kerendahan hati peneliti menyampaikan terima kasih yang setulus-tulusnya kepada :

1. Kedua Orangtua tercinta, Bapak dan Ibu yang selalu memberikan doa, semangat, serta dorongan yang tiada hentinya.
2. Bapak Dr. H. Noor Hudallah, M.T. sebagai dosen pembimbing utama yang telah memberikan arahan, bimbingan, dan saran kepada peneliti.
3. Bapak Aryo Baskoro Utomo, S.T., M.T. sebagai dosen pembimbing kedua yang telah memberikan arahan, bimbingan, dan saran kepada peneliti.
4. Bapak Dr. Nur Qudus, M.T. sebagai Dekan Fakultas Teknik Universitas Negeri Semarang.
5. Bapak Dr. –Ing. Dhidik Prastiyanto, S.T.,M.T. sebagai Ketua Jurusan Teknik Elektro dan Ketua Program Studi Pendidikan Teknik Elektro.
6. Seluruh Dosen dan staff karyawan Jurusan Teknik Elektro.

7. Rekan-rekan PTE 2012 yang selalu memberikan bantuan serta semangat dalam penyusunan skripsi ini.
  8. Serta pihak-pihak yang tidak dapat disebutkan satu persatu dalam tulisan ini.
- Semoga laporan skripsi ini dapat bermanfaat bagi semua pihak sebagaimana yang diharapkan. Amin.

Peneliti,

Jalu Wardoyo

## DAFTAR ISI

<b>PENGESAHAN</b> .....	<b>ii</b>
<b>PERNYATAAN KEASLIAN</b> .....	<b>iii</b>
<b>ABSTRAK</b> .....	<b>iv</b>
<b>KATA PENGANTAR</b> .....	<b>v</b>
<b>DAFTAR ISI</b> .....	<b>vii</b>
<b>DAFTAR GAMBAR</b> .....	<b>x</b>
<b>DAFTAR TABEL</b> .....	<b>xii</b>
<b>DAFTAR LAMPIRAN</b> .....	<b>xiii</b>
<b>BAB I PENDAHULUAN</b> .....	<b>1</b>
1.1. Latar Belakang .....	1
1.2. Rumusan Masalah .....	7
1.3. Batasan Masalah.....	7
1.4. Tujuan Penelitian .....	8
1.5. Manfaat Penelitian .....	8
1.6. Sistematika Penulisan .....	9
<b>BAB II LANDASAN TEORI</b> .....	<b>11</b>
2.1. Kajian Pustaka.....	11
2.2. Landasan Teori.....	13
2.2.1. <i>Smart Home Security</i> .....	13
2.2.2. <i>Safety System Smart Home</i> .....	15
2.2.3. <i>Magnetic Door Lock</i> .....	15
2.2.4. <i>Password</i> .....	18
2.2.5. <i>Biometric</i> .....	20

2.2.6. Sidik Jari .....	22
2.2.7. Modul Sensor Sidik Jari .....	28
2.2.8. Mikrokontroler .....	29
2.2.9. <i>Liquid Cristal Display</i> (LCD) .....	37
2.2.10. <i>Magnetic Switch</i> .....	38
<b>BAB III METODOLOGI PENELITIAN .....</b>	<b>40</b>
3.1. Metode Penelitian.....	40
3.2. Prosedur Pengembangan .....	41
3.3. Tahap Studi .....	42
3.3.1. Studi Pustaka .....	42
3.3.2. Studi Lapangan.....	42
3.3.3. Analisis Data .....	43
3.4. Tahapan <i>Research</i> .....	43
3.4.1. Desain Produk .....	43
3.4.2. Pembuatan Alat .....	44
3.4.3. Validasi Desain .....	52
3.4.4. Revisi Desain .....	55
3.5. Tahap Pengembangan .....	56
3.5.1. Uji Coba Sistem .....	56
3.1.6. Revisi Produk dan Hasil Akhir .....	61
<b>BAB IV HASIL DAN PEMBAHASAN .....</b>	<b>63</b>
4.1. Hasil Penelitian .....	63
4.1.1. Deskripsi Alat Perancangan .....	63
4.1.2. Hasil Pengujian Alat .....	69
4.1.3. Hasil Revisi Alat .....	77



4.2.	Pembahasan.....	83
4.2.1.	Pembahasan Uji Ahli.....	83
4.2.2.	Pembahasan Uji <i>Black Box</i> .....	85
4.2.3.	Pembahasan Uji Pengguna.....	86
4.2.4.	Perbandingan dengan Penelitian yang Relevan .....	87
<b>BAB V</b>	<b>PENUTUP.....</b>	<b>90</b>
5.1.	Kesimpulan .....	90
5.2.	Saran.....	91
<b>DAFTAR PUSTAKA</b>	<b>.....</b>	<b>92</b>
<b>LAMPIRAN</b>	<b>.....</b>	<b>94</b>

## DAFTAR GAMBAR

Gambar 1. Contoh konsep <i>smart home</i> .....	14
Gambar 2. Diagram <i>magnetic door lock</i> .....	16
Gambar 3. Skema <i>keypad</i> 3 x 4.....	19
Gambar 4. Bentuk fisik <i>keypad</i> 3x4.....	19
Gambar 5. Klasifikasi teknologi <i>biometric</i> .....	20
Gambar 6. Sidik jari diambil melalui <i>ink technique</i> dan <i>scanner</i> sidik jari.....	23
Gambar 7. <i>Singular legion</i> .....	25
Gambar 8. Proses ekstraksi <i>minutiae</i> .....	26
Gambar 9. Proses <i>matching</i> dengan metode <i>minutiae-based methods</i> : a) dan b) <i>minutiae</i> diekstaksi dari <i>template</i> dan input, c) <i>minutiae</i> ditandai dengan lingkaran, d) tiap lingkaran menunjukkan <i>minutiae</i> yang dicocokkan oleh algoritma.....	27
Gambar 10. Modul sensor sidik jari Adafruit .....	28
Gambar 11. Chip mikrokontroler.....	30
Gambar 12. Diagram blok ATmega328.....	31
Gambar 13. Arduino Uno dan Arduino Mega .....	33
Gambar 14. Modul LCD 16 x 2 .....	37
Gambar 15. <i>Magnetic switch</i> .....	38
Gambar 16. Langkah-langkah metode penelitian <i>research and development</i> (R&D) .....	40
Gambar 17. Tahap kegiatan penelitian dan pengembangan produk .....	41
Gambar 18. Perancangan alat.....	43
Gambar 19. Desain rangkaian elektronik.....	46
Gambar 20. Desain panel luar .....	48
Gambar 21. Desain panel dalam .....	49
Gambar 22. Desain panel pintu.....	50
Gambar 23. <i>Flowchart</i> program.....	51
Gambar 24. Hasil desain elektronik.....	65

Gambar 25. <i>Smart home security system berbasis Arduino</i> .....	66
Gambar 26. Revisi penggantian <i>box</i> .....	78
Gambar 27. <i>Flowchart software</i> dan skema komponen <i>emergency entry</i> .....	79
Gambar 28. <i>Bluetooth HC-05</i> .....	80
Gambar 29. Skema indikator baterai.....	83

## DAFTAR TABEL

Tabel 1 Rekapitulasi Tindak Kejahatan tahun 2014-2016.....	2
Tabel 2 Persentase Korban Kejahatan menurut Jenis Kejahatan.....	3
Tabel 3 Komparasi Variasi Teknologi <i>Biometric</i> .....	21
Tabel 4 Perbandingan Spesifikasi Arduino Uno dan Mega.....	34
Tabel 5 Konfigurasi <i>Pin</i> LCD 16 x 2.....	38
Tabel 6 Keterhubungan <i>Pin</i> Arduino Uno .....	46
Tabel 7 Kisi-kisi Angket Ahli Sistem .....	52
Tabel 8 Skenario Pengujian <i>Task Testing</i> .....	55
Tabel 9 Skenario Pengujian <i>Error Trapping</i> .....	55
Tabel 10 Sampel Penelitian Uji Pengguna.....	57
Tabel 11 Kisi-kisi Uji Pengguna.....	57
Tabel 12 Interval Pengkategoriaan Skor .....	61
Tabel 13 Hasil Tabulasi Uji Ahli .....	69
Tabel 14 Hasil Uji <i>Task Testing</i> .....	71
Tabel 15 Hasil Uji <i>Error Trapping</i> .....	74
Tabel 16 Hasil Tabulasi Uji Pengguna.....	76
Tabel 17 Konfigurasi <i>Pin</i> Modul Bluetooth HC-05.....	80
Tabel 18 Hasil Uji <i>Black Box Emergency Entry</i> .....	81
Tabel 19 Hasil Perhitungan Aspek Uji Ahli .....	83
Tabel 20 Hasil Perhitungan Aspek Uji Pengguna.....	86

## DAFTAR LAMPIRAN

Lampiran 1. Formulir usulan topik skripsi.....	94
Lampiran 2. Surat usulan dosen pembimbing.....	95
Lampiran 3. Surat tugas dosen pembimbing.....	96
Lampiran 4. <i>Source code smart home security system berbasis Arduino</i> .....	97
Lampiran 5. Dokumentasi penelitian .....	107
Lampiran 6. Tabulasi hasil uji pengguna .....	108
Lampiran 7. Kuesioner uji ahli .....	109
Lampiran 8. Kuesioner uji pengguna .....	112

# **BAB I**

## **PENDAHULUAN**

### **1.1. Latar Belakang**

Kebutuhan fundamental setiap manusia terdiri dari kebutuhan biologis (seperti makan, minum, serta tidur) dan kebutuhan sosial (seperti status sosial, peranan sosial, aktualisasi diri, dan rasa aman). Saat ini dapat dikatakan bahwa rasa aman merupakan salah satu kebutuhan dasar manusia dalam menjalankan aktivitas sehari-harinya (BPS, 2017: 3). Hal ini menunjukkan bahwa rasa aman merupakan kebutuhan manusia yang mendasar.

Dalam katalog yang diterbitkan oleh Badan Pusat Statistika (2017), selama periode tahun 2014-2016 jumlah kejadian kejahatan atau tindakan kriminallitas di Indonesia cenderung meningkat. Data Biro Pembinaan dan Operasional, Mabes Polri memperlihatkan jumlah kejadian kejahatan (*crime total*) pada tahun 2014 sebanyak 325.317 kasus, meningkat pada tahun 2015 menjadi sebanyak 352.936 kasus, dan meningkat kembali menjadi 357.197 kasus pada tahun 2016. Jumlah kejahatan berdasarkan jenis kejahatan secara lengkap bisa dilihat pada tabel 1.

Sedangkan berdasarkan jenis kejahatan yang dialami dapat dilihat pada tabel 2. Mayoritas kejahatan yang terjadi pada tahun 2016 berupa kejahatan pencurian sebesar 87,19%, kejahatan lainnya sebesar 10,48%, penganiayaan sebesar 3,45%, pencurian dengan kekerasan sebesar 3,02%, dan pelecehan seksual sebesar 1,15%. Jika dibandingkan periode sebelumnya, kejadian kejahatan pencurian memiliki pola dengan kecenderungan meningkat.

Tabel 1  
Rekapitulasi Tindak Kejahatan tahun 2014-2016

Kelompok/Jenis Kejahatan	Tahun		
	2014	2015	2016
Pembunuhan	1.277	1.491	1.292
Penganiayaan Berat	13.996	14.664	14.468
Penganiayaan Ringan	22.984	22.981	21.55
Kekerasan dalam Rumah Tangga	9.386	9.483	11.083
Perkosaaan	1.715	1.739	1.594
Pencabulan	3.784	3.312	3.652
Penculikan	336	380	374
Memperkerjakan Anak Dibawah Umur	1.618	1.832	2.511
Pencurian dengan Kekerasan	10.414	10.759	10.726
Pencurian dengan Kekerasan Senjata Api	331	312	272
Pencurian dengan Kekerasan Senjata Tajam	1.012	785	1.097
Pencurian	24.538	26.298	26.636
Pencurian dengan Pemberatan	42.699	41.100	46.277
Pencurian Kendaraan Bermotor	42.166	38.389	37.871
Pengrusakan/Penghancuran Barang	7.207	6.968	7.926
Pembakaran dengan Sengaja	788	712	650
Penadahan	354	537	666
Narkoba dan Psikotropika	19.280	36.874	39.171
Penipuan/Perbuatan Curang	26.390	30.689	27.421
Penggelapan	21.404	21.646	20.459
Korupsi	814	1.780	1.318
Kejahatan Terhadap Ketertiban Umum	4.519	4.227	4.297
<b>JUMLAH</b>	<b>325.317</b>	<b>352.936</b>	<b>357.197</b>

Sumber: Biro Pembinaan dan Operasional, Mabes Polri. Statistik Kriminal 2016, katalog: 4401002, Badan Pusat Statstistika

Tabel 2  
 Persentase Korban Kejahatan menurut Jenis Kejahatan  
 tahun 2015-2016

Kategori	Tahun	
	2015	2016
Pencurian	84,19	87,19
Penganiayaan	3,15	3,45
Pencurian dengan kekerasan	2,55	3,02
Pelecehan seksual	0,8	1,15
Lain-lain	11,82	10,48
Lebih dari 1 kali jenis kejahatan	2,51	5,29

Sumber : Diolah dari susenas 2015-2016

Pencurian berdasarkan KUHP pasal 362 adalah suatu tindakan mengambil barang atau sesuatu yang seluruhnya atau sebagiannya adalah kepunyaan orang lain dengan maksud untuk memiliki secara melawan hukum. Salah satu bentuk kejahatan pencurian yang banyak mendapatkan perhatian adalah kasus pencurian di rumah tangga. Rumah tangga selayaknya merupakan suatu tempat yang aman, termasuk aman dari berbagai gangguan kejahatan. Pada kenyataannya data tabel 2 menunjukkan bahwa kasus tindak kejahatan pencurian semakin meningkat.

Menurut O'Block dalam Rara Fitri (2009: 68), kejahatan terjadi di lingkungan tempat tinggal umumnya berbentuk pencurian rumah kosong, pencurian kendaraan bermotor, pencurian dengan penipuan, perampokan, dan pembobolan rumah. O'Block berpendapat, dalam beberapa kasus di lingkungan tempat tinggal merupakan kombinasi antara niat dan kesempatan. Dengan demikian salah satu cara untuk mengurangi tingkat kejahatan di lingkungan tempat tinggal



adalah dengan menghilangkan kesempatan yang dapat menimbulkan niat untuk mencuri.

Lebih lanjut O'Block (Rara Fitri, 2009: 68) berpendapat terdapat beberapa variabel yang turut andil menjadikan tempat tinggal sebagai daerah rawan kejahatan. Variabel tersebut antara lain: (1) Kondisi dan karakteristik lingkungan, terkait status sosial, ekonomi, dan integritas warga, (2) Personil pengamanan, berwujud satuan pengamanan, (3) Karakteristik warga, usia, dan penempatan rumah, (4) Karakteristik rumah, misal rumah dengan pagar rendah, (5) Desain lingkungan, berhubungan erat dengan instrumen pengaman misalnya kunci, *alarm*, jendela, teralis dan lain-lain, (6) Pola dan karakteristik pelaku, jam sering terjadinya pencurian dan target pencurian. Salah satu upaya meningkatkan variable desain lingkungan adalah penerapan *smart home*.

*Smart home* atau rumah pintar merupakan gabungan dari dua kata yaitu rumah yang bermakna tempat untuk tinggal dan pintar yang bermakna mahir dalam sesuatu (KBBI Daring). Dengan demikian rumah pintar merupakan tempat tinggal yang didalamnya terdapat gabungan beberapa alat yang memiliki kemampuan atau kemahiran tertentu bergantung pada aplikasinya. Alat-alat tersebut memiliki karakteristik tersendiri baik *hardware*, *software*, dan dukungan sistem komunikasi yang berbeda. Konsep *smart home* berdasarkan aplikasinya antara lain: (1) *Light control*, (2) *Appliance control*, (3) *Entertainment*, (4) *Safety system*, (5) *Climate control*, dan (6) *Assisted living*. Salah satu aplikasi *smart home* yang dapat diterapkan untuk menanggulangi upaya kejahatan di lingkungan tempat tinggal

yaitu *safety system* (Changmin Lee, 2014: 67). Aplikasi *safety system* dalam *smart home* adalah deteksi asap, CCTV, dan *smart door lock*.

*Smart door lock* menjadi bagian utama pada *safety system* karena pintu merupakan jalan masuk utama untuk memperoleh hak akses rumah. Secara umum sistem keamanan yang digunakan pada pintu berupa kunci konvensional atau kunci fisik. Kunci fisik memiliki beberapa kekurangan seperti mudah hilang, dicuri maupun rusak (Nur Adila, 2014: 1). Penerapan *smart door lock* menggunakan solenoid *door lock* sebagai mekanisme penguncian pintu. Beberapa metode operasi solenoid *door lock* antara lain menggunakan *password*, *Radio Frequency Identification* (RFID), dan identifikasi *biometric*. Dengan demikian untuk mengatasi kekurangan pada penggunaan kunci fisik maka digantikan dengan kunci non-fisik seperti *password* dan identifikasi *biometric*.

Anil K. Jain (2008: 3) Identifikasi *biometric* adalah metode identifikasi seseorang berdasarkan fisik dan kebiasaan seperti wajah, sidik jari, suara, dan iris. Pemanfaatan metode *biometric* dengan sidik jari memiliki beberapa keunggulan dibandingkan dengan metode *biometric* yang lain. *Biometric* dengan sidik jari memiliki keunggulan dalam tingkat akurasi, mudahnya penerapan pada sistem, dan bersifat permanen dimana karakter *biometric* tidak berubah selama periode waktu tertentu. Salah satu modul identifikasi sidik jari yang beredar di pasaran saat ini adalah keluaran dari Adafriut ZM-20 dengan *False Acceptance Rate* kurang dari 0,001% dan *False Rejection Rate* kurang dari 1%. Sistem ini sangat cocok sebagai salah satu instrumen sistem keamanan tempat tinggal.

Beberapa penelitian telah dilakukan terkait *safety system* menggunakan identifikasi *biometric* sidik jari diantaranya Setya Ardhi (2011: 398-409) melakukan perancangan dan pembuatan sistem pengaman rumah dengan teknologi pengenalan sidik jari. Dalam penelitiannya dinyatakan bahwa *Integrated Fingerprint Verification Sensor* merupakan modul yang cocok digunakan untuk pembuatan aplikasi yang membutuhkan kemampuan mendeteksi sidik jari, serta masih dapat dikembangkan lebih lanjut aplikasi-aplikasi lainnya. Penelitian lain dilakukan oleh M. Gayathri (2014) dengan judul “*Fingerprint and GSM based Security System*” menjelaskan teknik sidik jari mempunyai kemampuan keamanan yang tinggi baik untuk rumah, kantor, bank dll. Penelitian ini mengidentifikasi untuk meningkatkan sistem keamanan yang ada dapat dilakukan pengembangan dengan mengkombinasikan metode sidik jari dan *Personal Identification Number (PIN)/Password*.

Berdasarkan uraian terkait tindak kejahatan di rumah tangga dan *safety system* menggunakan identifikasi *biometric* dan *password*, peneliti tertarik untuk membangun sebuah sistem keamanan rumah dengan mengkombinasikan antara metode *password* dan sidik jari. Penelitian yang akan dilakukan dengan judul “*Smart home Security System Berbasis Arduino*”. Penelitian ini diharapkan mampu memenuhi kebutuhan terkait sistem keamanan rumah terhadap akses pintu.

## 1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan maka dapat ditentukan permasalahan dalam skripsi ini yaitu:

1. Bagaimana merancang dan membuat sistem keamanan hak akses rumah dengan kombinasi metode *biometric fingerprint* dan *password* berbasis Arduino?
2. Bagaimana unjuk kerja *smart home security system* berbasis Arduino?

## 1.3. Batasan Masalah

Penelitian rancang bangun *smart home security system* ini menitikberatkan pengkajian pada:

1. Mikrokontroler yang digunakan berupa *board* Arduino.
2. Metode *biometric* yang digunakan adalah sidik jari (*fingerprint*).
3. Kombinasi metode pengamanan yang digunakan adalah *password* dan sidik jari.
4. Simulasi *alarm* dilakukan dengan *buzzer*.
5. Penggunaan solenoid sebagai piranti penguncian magnet pada pintu.
6. Sensor “Adafriut Fingerprint ZM-20” sebagai sensor identifikasi sidik jari, memiliki kemampuan *enroll* sistem secara otomatis.
7. *Keypad* sebagai *input* kode pengaman menggunakan *keypad* jenis 3 x 4.
8. Penelitian berfokus pada mekanisme pengamanan pintu.

#### **1.4. Tujuan Penelitian**

Tujuan dari penelitian ini adalah mendesain rancang bangun *smart home security system* berbasis Arduino dengan metode *biometric fingerprint* dan *password*, adapun tujuan khusus sebagai berikut :

1. Mengembangkan sistem keamanan hak akses rumah dengan kombinasi metode *biometric fingerprint* dan *password* berbasis Arduino.
2. Mengetahui unjuk kerja sistem keamanan hak akses rumah dengan kombinasi metode *biometric fingerprint* dan *password* berbasis Arduino.

#### **1.5. Manfaat Penelitian**

Manfaat dari penelitian ini adalah untuk mendesain sistem keamanan akses rumah dengan tingkat keamanan tinggi dengan memanfaatkan identifikasi *biometric fingerprint* dan *password* untuk menutupi kekurangan dari sistem keamanan konvensional kunci maupun identifikasi RFID (kartu ID) hilang atau dicuri. Dengan penerapan *smart home security system* berbasis Arduino ini dapat memenuhi kebutuhan keamanan bagi personal maupun keluarga di rumah.

Hasil penelitian rancang bangun *smart home security system* berbasis Arduino ini diharapkan dapat bermanfaat bagi :

1. Peneliti
  - a. Sebagai sarana untuk menambah dan menerapkan ilmu pengetahuan yang diperoleh di perkuliahan, sumber ide untuk melakukan pembuatan alat dan pengembangan rancangan yang lebih baik.

- b. Sebagai persyaratan guna memperoleh gelar sarjana di Fakultas Teknik Universitas Negeri Semarang.

## 2. Masyarakat

- a. Mendapatkan sistem keamanan dengan tingkat keamanan yang tinggi.
- b. Memberikan ide untuk pengembangan sistem keamanan lain.
- c. Meminimalisir aksi tindak kriminal dengan adanya sistem keamanan akses rumah.

## 3. Industri

- a. Dapat dilakukan pengembangan pada alat ini untuk meningkatkan nilai kemudian diproduksi secara massal untuk menekan biaya produksi.
- b. Menumbuhkan pangsa pasar baru akan kebutuhan sistem keamanan di masyarakat.

## 4. Pendidikan

Menjadi salah satu rujukan penerapan dan pengembangan sistem keamanan dengan identifikasi *biometric fingerprint* dan *password*.

### **1.6. Sistematika Penulisan**

Sistematika penulisan pada penelitian ini adalah :

#### 1. Bab I Pendahuluan

Berisi latar belakang masalah, rumusan masalah, pembatasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan penelitian.

## 2. Bab II Landasan Teori

Berisi penjabaran teori dan kajian pustaka berdasarkan teori yang relevan untuk digunakan sebagai bahan acuan dalam penelitian.

## 3. Bab III Metode Penelitian

Bab ini menjabarkan model pengembangan sistem yang akan dibuat, serta sistematika perancangan dan pembuatan *smart home security system* berbasis Arduino.

## 4. Bab IV Hasil dan Pembahasan

Bab ini akan membahas mengenai hasil dari model pengembangan yang digunakan dalam perancangan dan pembuatan *smart home security system* berbasis Arduino serta menjelaskan pembahasan hasil pengujian terhadap alat dan kesesuaian dengan tujuan yang telah dijelaskan sebelumnya.

## 5. Bab V Penutup

Berisi tentang kesimpulan dan saran berdasarkan hasil pengembangan *smart home security system* berbasis Arduino.

## BAB II

### LANDASAN TEORI

#### 2.1. Kajian Pustaka

Dalam penulisan skripsi ini peneliti menggali informasi dari penelitian-penelitian sebelumnya sebagai bahan perbandingan, baik mengenai kekurangan atau kelebihan yang sudah ada. Selain itu, peneliti juga menggali informasi dari artikel, buku-buku, dan skripsi dalam rangka mendapat informasi tentang teori yang berkaitan dengan *smart home security system* berbasis Arduino untuk memperoleh landasan teori ilmiah.

Tugas akhir Idris Setyawan (2015), mahasiswa Universitas Negeri Semarang, dengan judul “Sistem Pengaman Pintu Menggunakan Sensor Sidik Jari (*fingerprint*)”. Pada penelitian tersebut *fingerprint* digunakan sebagai sistem pengaman dengan menggunakan sensor *fingerprint*. Alat ini memeriksa apakah terdapat kecocokan antara data yang diperoleh dari proses verifikasi dengan data yang tersimpan pada sistem untuk membuka akses pintu. Penelitian tersebut juga menggunakan sistem *relay* dan solenoid sebagai mekanisme pengunci pintu.

M. Gayatri, dkk (2014) dalam Artikel IJESRT *Department of Electronics and Communication, Communication systems*, Sri Shakthi Institute Of Engineering And Technology, Coimbatore, India dengan judul “*Fingerprint and GSM based Security System*”. Pada artikel tersebut dijelaskan mengenai penerapan sistem keamanan loker berdasarkan teknologi sidik jari dan *password* yang dikirimkan secara acak melalui modul GSM. Sistem penguncian loker dapat mengautentifikasi,



memvalidasi pengguna, dan membuka kunci pintu secara *real time* untuk akses loker. Apabila sidik jari telah terverifikasi maka pengguna akan mendapatkan notifikasi dari modul GSM berupa *password* secara acak setiap kali sistem digunakan untuk membuka loker. *Buzzer* akan berbunyi sebagai *alarm* apabila sidik jari tidak terverifikasi.

Penelitian yang dilakukan oleh Rajadurai (2015) dengan judul “*Android Mobile Based Home Security and Device Control Using GSM.*” Menggunakan *password* sebagai metode pengaman rumah dan GSM sebagai media autentifikasi. Alat yang dirancang oleh Rajadurai bekerja dengan cara ketika pengguna memasukan *password* maka modul GSM akan mengirimkan perintah *authorize* pada *mobile device* yang terhubung dengan sistem pengaman. Akses terhadap pintu diberikan ketika *password* yang dimasukan sesuai dan telah mendapat *authorized*. Rajadurai menggunakan mikrokontroler yang berbasis arsitektur *Reduced Instruction Set Computer* (RISC) yang dikembangkan oleh *Advanced RISC Machines* (ARM) sebagai pusat kendali alat.

Penelitian yang dilakukan Setya Ardhi (2011: 398-409) mahasiswa Sekolah Tinggi Teknik Surabaya dengan judul “Perencanaan dan Pembuatan Sistem Pengaman Rumah dengan Teknologi Pengenal Sidik Jari”. Pada penelitian tersebut selain memanfaatkan metode pengamanan dengan *biometric fingerprint*, alat yang dirancang Setya Ardi juga memanfaatkan kapasitas memori penyimpanan EEPROM pada modul mikrokontroler yang digunakan. EEPROM tersebut dimanfaatkan sebagai wadah penyimpanan daftar pengguna sidik jari yang telah didaftarkan.

Dalam artikel penelitian yang dibuat oleh Marcos Faundez Zanuy (2006) Escola Universitaria Politecnica de Mataro, Faundez membandingkan berbagai macam metode pengamanan *biometric* dalam beberapa aspek seperti *Ease of use*, *Accuracy*, *Acceptability*, *security*, *Performance*. Dari penelitian tersebut diketahui *biometric fingerprint* memiliki skor rata-rata tertinggi pada masing-masing aspek yang diujikan. Sehingga metode *biometric fingerprint* sangat cocok untuk digunakan dalam sistem pengamanan.

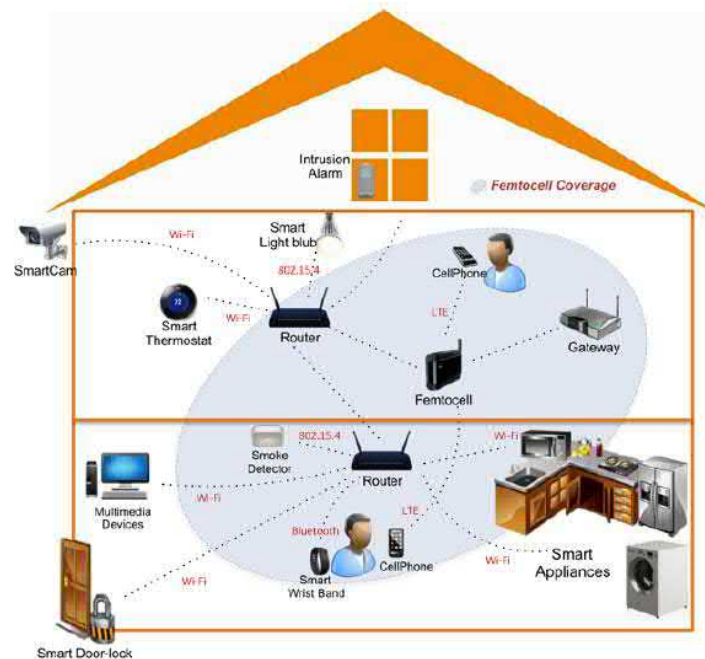
Hasil dari beberapa penelitian tersebut berupa *fingerprint* sebagai penggunaan metode *biometric* dan *password* sebagai metode pengaman akses terhadap pintu, penggunaan mikrokontroler sebagai pusat kontrol, pemanfaatan memori EEPROM sebagai media penyimpanan, penggunaan *relay* dan solenoid *door lock* sebagai mekanisme penguncian pintu, dan pemanfaatan *buzzer* sebagai indikasi *alarm*. Sedangkan pada penelitian ini berupa *smart home security system* berbasis Arduino yang dirancang berdasarkan beberapa penelitian tersebut dengan menambahkan fitur *magnetic switch* sebagai mekanisme pengaman pintu untuk deteksi pelanggaran terhadap akses pintu dan *emergency backup supply* sebagai mekanisme pengaman sistem ketika kehilangan sumber daya utama.

## **2.2. Landasan Teori**

### **2.2.1. Smart Home Security**

*Smart home* merupakan sebuah rumah yang terdiri dari banyak perangkat yang saling terhubung dan memiliki daerah aplikasi yang berbeda. Perangkat-perangkat ini ditandai dengan *hardware* yang heterogen, *software resource*, dan

memiliki teknologi komunikasi yang berbeda-beda (Changmin Lee, 2014: 67). Dengan demikian *smart home* dapat dikatakan merupakan sebuah hunian tempat tinggal yang didalamnya terdapat gabungan beberapa alat yang memiliki kemampuan atau kemahiran tertentu bergantung pada aplikasinya. Contoh konsep penerapan aplikasi *smart home* dapat dilihat pada gambar 1.



Gambar 1. Contoh konsep *smart home*

Konsep dari penerapan *smart home* berdasarkan aplikasinya. antara lain: (1) *Light control*, (2) *Appliance control*, (3) *Entertainment*, (4) *Safety system*, (5) *Climate control*, dan (6) *Assisted living*. Salah satu aplikasi *smart home* yang dapat diterapkan untuk menanggulangi upaya tindak kejahatan di lingkungan tempat tinggal yaitu *safety system*.

### **2.2.2. Safety System Smart Home**

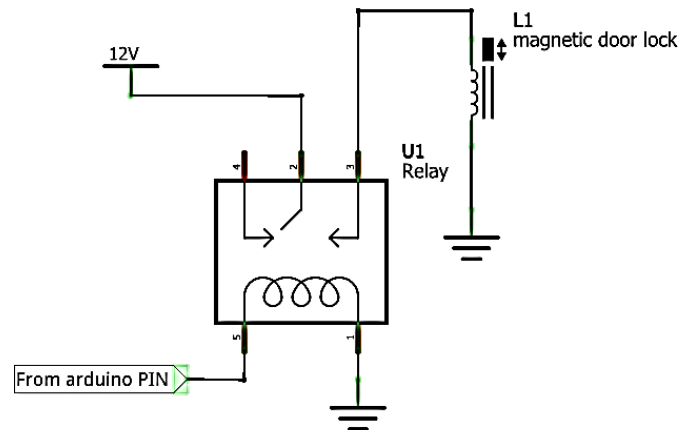
*Safety system* pada *smart home* dalam pengaplikasiannya terdiri dari deteksi asap, deteksi zona intrusi untuk mendeteksi aktifitas yang mencurigakan dalam rumah, *alarm* pencuri, dan kamera pengintai. Penerapan tersebut saling terintegrasi. Bentuk *alarm* yang digunakan bisa disampaikan kepada warga sekitar atau pihak kepolisian (Changmin Lee, 2014: 68). *Alarm* juga harus disampaikan saat itu juga sebagai tindakan antisipasi sistem dan meminimalisir kerugian akibat aktivitas yang dianggap merugikan.

Dalam *safety system smart home* pintu menjadi poin utama untuk menjaga privasi dan keamanan rumah. Pintu dalam sebuah bangunan merupakan sebuah alat penghubung untuk keluar masuk bangunan. Pintu berfungsi untuk menghubungkan dua ruangan yang terpisah secara permanen, selain itu pintu juga berfungsi untuk menjaga privasi serta keamanan sebuah rumah. Dalam pengamanan pintu menggunakan banyak sistem penguncian, salah satunya menggunakan *magnetic door lock*.

### **2.2.3. Magnetic Door Lock**

*Magnetic door lock* adalah peralatan dengan sifat kemagnetan sangat kuat yang dibangkitkan secara elektromagnetik dan bekerja sebagai pengunci pintu. Sistem kerja *magnetic door lock* memanfaatkan induksi listrik yang dihasilkan dari kawat melingkar pada inti besi untuk menghasilkan medan magnet. Ketika arus melewati kawat ini maka akan menghasilkan medan magnet atau kekuatan magnet

yang digunakan untuk menarik inti besi. Pintu akan tetap terkunci selama *magnetic door lock* tidak diberikan tegangan untuk dapat bekerja menarik inti besi. Sehingga kinerja penguncian akan mengamankan pintu. Untuk lebih jelas skema *magnetic door lock* dapat dilihat pada gambar 2.



Gambar 2. Diagram *magnetic door lock*

Operasi *magnetic door lock* pada penelitian ini menggunakan solenoid. Solenoid adalah sebuah aktuator yang mampu melakukan gerak linier. Solenoid berkerja dengan menggunakan konsep elektromekanis, hidrolis, pneumatik atau didorong dengan prinsip yang sama. Solenoid menghasilkan gerak linier ketika diberikan tegangan. Solenoid DC beroperasi sesuai dengan prinsip motor DC, hanya saja yang membedakan solenoid merupakan motor yang tidak dapat berputar.

Metode operasi solenoid *magnetic door lock* dapat menggunakan tiga operasi yaitu sistem *keypad*, sistem kartu pintar, dan sistem *biometric*.

#### a. Sistem *Keypad*

Sistem *keypad* merupakan salah satu sistem keamanan yang paling umum digunakan dalam identifikasi dan kontrol akses. Sistem bekerja dengan mengenali

kode *password* yang dimasukan pengguna dan dicocokkan dengan kode *password* pengguna yang sudah terdaftar. Pengguna dapat mengganti *password* secara berkala agar tidak mudah ditebak dan tetap menjaga kerahasiaan *password*.

Kekurangan dari sistem *keypad* adalah mudahnya lupa atau diretas. Keunggulan *password* adalah mudah digunakan dan diterima pengguna serta pengguna tidak perlu membawa kunci fisik. Jadi, untuk tingkat sistem keamanan yang tinggi sebaiknya sistem *keypad* dapat dikombinasikan dengan sistem keamanan yang lain.

#### **b. Sistem Kartu Pintar**

Kartu pintar merupakan sebuah kartu yang telah dibenamkan sirkuit terpadu didalamnya. Terdapat dua jenis kartu pintar yaitu kartu pintar sentuh dan *non-sentuh*. Kartu pintar sentuh memiliki *chip* keemasan dihubungkan melalui pembaca kartu, *chip* terhubung langsung dengan elektronik yang dapat membaca informasi atau menuliskannya kembali. Kartu pintar *non-sentuh* dihubungkan dengan pembaca kartu dengan cara induksi RFID. Kartu ini hanya perlu didekatkan dengan pembaca kartu untuk menyelesaikan transaksi data.

Kartu pintar dalam penerapan *smart home security system* mengizinkan pemilik kartu untuk mengakses ruang. Kartu pintar dapat diprogram untuk memperoleh akses ke pintu tertentu dalam sebuah gedung. Kartu pintar menyimpan informasi dan data pemilik kartu. Terdapat dua tipe kartu pintar yaitu menggunakan identitas dan tanpa identitas. Kartu pintar tanpa identitas menggunakan sinyal elektronik untuk mentransfer data ketika terjadi kontak dengan alat penerima.

Sistem kartu pintar memiliki beberapa kekurangan seperti mudah hilang, dicuri, maupun rusak karena terkena medan magnet kuat.

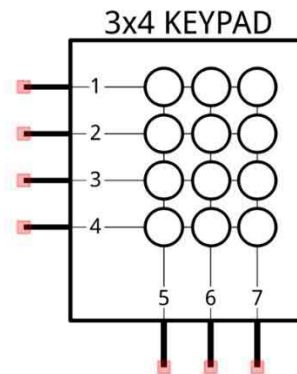
### c. **Sistem *Biometric***

Sistem *biometric* memungkinkan penggunaan ciri khusus yang dimiliki seperti sidik jari, suara, dan wajah dimana individu memiliki keunikan masing-masing. Sistem ini memanfaatkan karakteristik yang berbeda pada masing-masing individu sehingga tidak dapat ditiru oleh orang lain.

Beberapa jenis metode *biometric* yang dapat digunakan pada sistem hak akses rumah seperti sidik jari, pengenalan suara, dan pengenalan wajah. Masing-masing metode dapat dikategorikan pada penggunaan dan tingkat keamanan yang memiliki karakteristik masing-masing

#### **2.2.4. *Password***

*Password* adalah sistem identifikasi yang unik dengan kombinasi huruf, angka dan/atau simbol yang digunakan untuk mengidentifikasi individu (Tom Wayteg, 2013: 146-148). *Password* merupakan suatu bentuk dari data otentikasi rahasia yang digunakan untuk mengontrol akses ke dalam suatu sumber. *Password* kadang digunakan dalam bentuk *Personal Identification Number* (PIN) yang hanya terdiri dari angka. Dalam penerapannya pada sistem keamanan *password* menggunakan *keypad* sebagai *input*. Beberapa tipe *keypad* yang umum digunakan adalah *keypad* modul 3 x 4. *Keypad* 3 x 4 memanfaatkan skema *matric* untuk mengurangi penggunaan kabel. Lebih jelasnya dapat dilihat pada gambar 3.



Gambar 3. Skema *keypad* 3 x 4

*Keypad* 3 x 4 merupakan suatu modul *keypad* berukuran 3 kolom x 4 baris. Modul ini dapat difungsikan sebagai *input* dalam aplikasi seperti pengaman digital, data *logger*, absensi, pengendali kecepatan motor, robotik, dan sebagainya. Susunan tombol-tombol yang ditempatkan seperti matriks, yakni terdiri dari barisan dan kolom. Terdapat 3 kolom tombol dan 4 baris tombol berupa matriks 3 x 4. Penggunaan *keypad* jenis ini menghemat penggunaan kabel dikarenakan pada *keypad* terdapat hubungan saklar antara baris dan kolom. Adapun bentuk fisik dari *keypad* 3 x 4 seperti gambar 4.

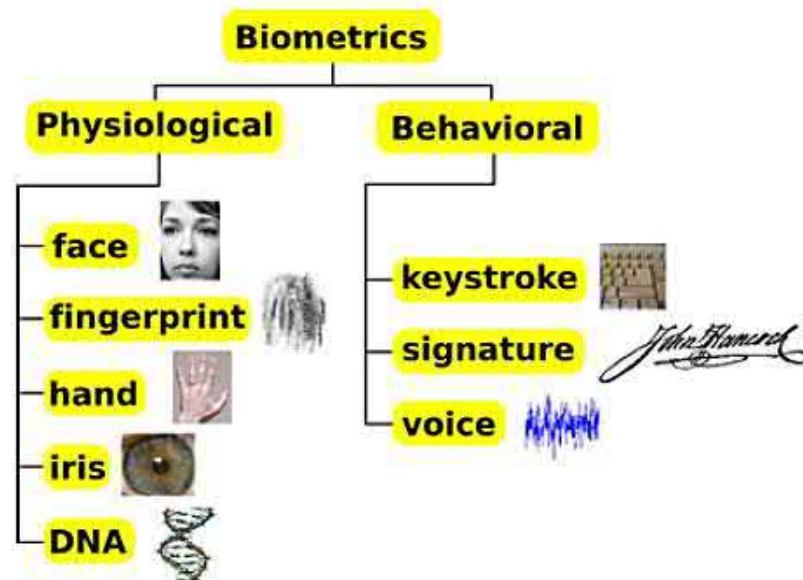


Gambar 4. Bentuk fisik *keypad* 3x4



### 2.2.5. *Biometric*

Penerapan teknologi *biometric* dalam sistem keamanan sangat luas, metode ini mengidentifikasi dan memverifikasi berdasarkan karakteristik seseorang. *Biometric* dapat dibagi menjadi dua kategori yaitu karakter fisik dan kebiasaan. Karakteristik fisik meliputi wajah, sidik jari, tangan, iris, dan DNA. Sedangkan karakteristik kebiasaan berdasarkan suara, *keystone*, dan tandatangan. Klasifikasi teknologi *biometric* dapat dilihat pada gambar 5.



Gambar 5. Klasifikasi teknologi *biometric*

Penggunaan teknologi *biometric* pada sebuah sistem keamanan sangat dianjurkan, karena setiap orang mempunyai keunikan masing-masing yang tidak dapat ditiru. Simon Liu dan Silverman (2001 : 27) menyatakan *biometric* adalah metode autentifikasi paling aman dan mudah, tidak bisa dipinjam, dicuri dan terlupa. Selain itu penggunaan metode *biometric* dapat dengan mudah mengenali seseorang dengan mengetahui kesamaan karakteristik.

Menurut Anil K. Jain, dkk (2004: 4-20) melakukan komparasi dari variasi metode *biometric* berdasarkan tujuh faktor yaitu: (1) *Universality*, semua orang dapat menggunakan metode tersebut, (2) *Distinctiveness*, setiap individu memiliki perbedaan karakter yang jelas, (3) *Permanence*, karakter *biometric* tidak berubah selama periode waktu, (4) *Collectability*, kemudahan pengumpulan data, (5) *Performance*, akurasi *biometric*, (6) *Acceptability*, individu dalam populasi dapat menerima aplikasi *biometric*, (7) *Circumvention*, *biometric* tidak mudah dipalsukan. Penilaian dibagi menjadi tiga kategori *low* (L), *medium* (M), dan *high* (H). Semakin tinggi penilaian mengindikasikan semakin baik performa, sebaliknya semakin rendah penilaian mengindikasikan kurangnya performa. Komparasi variasi teknologi *biometric* dapat dilihat pada tabel 3.

Tabel 3  
Komparasi Variasi Teknologi *Biometric*

Identifikasi	Faktor						
	<i>Universality</i>	<i>Distinctiveness</i>	<i>Permanence</i>	<i>Collectability</i>	<i>Performance</i>	<i>Acceptability</i>	<i>Circumvention</i>
Wajah	H	L	M	H	L	H	H
Sidik jari	M	H	H	M	H	M	M
Tanda tangan	L	L	L	H	L	H	H
Suara	M	L	L	M	L	H	H

Keterangan: H= *High*, M= *Medium*, L= *Low*

Sumber: *Face Recognition Security System for Access Control* 2004

Dalam penerapan teknologi *biometric* pada sistem keamanan harus memiliki penilaian tinggi pada *universality*, *distinctiveness*, *permanence*, dan *performance*. (M. Faundez-Zanuy, 2006: 15-26). Sidik jari memiliki penilaian *high* pada *distinctiveness*, *permanence*, dan *performance*. Selain itu sidik jari juga mendapat penilaian *medium* pada faktor *universality*. Sehingga, berdasarkan pandangan tersebut, metode sidik jari dipilih untuk diterapkan dan dikembangkan dalam *smart home security system* pada penelitian ini.

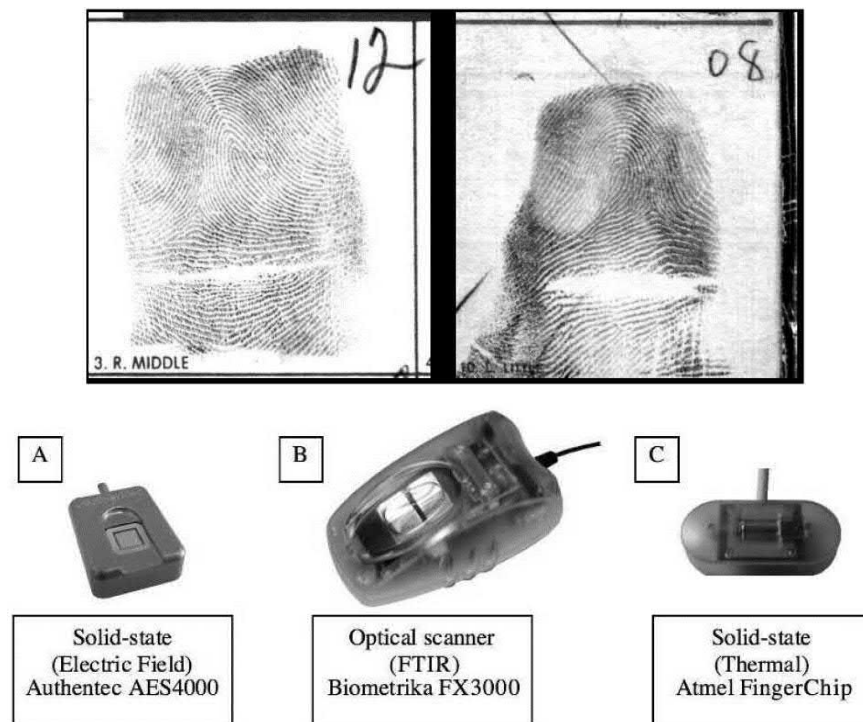
#### **2.2.6. Sidik Jari**

Sidik jari merupakan representasi dari jaringan epidermis pada jari, bentuk pola tonjolan, dan lekukan. Seperti semua bagian dalam tubuh, sidik jari merupakan perkembangan dari genetik dan faktor lingkungan. Kode genetik dalam DNA memberikan perintah umum kepada jaringan kulit untuk membuat aliran darah dan secara spesifik menjadi acak. Sidik jari sangat stabil digunakan sebagai metode identifikasi, sidik jari tidak akan berubah selama hidup seseorang kecuali karena kecelakaan seperti terpotong pada sidik jari (Anil K, 2008: 23).

Metode sidik jari berdasarkan sistem *biometric* dibagi menjadi tiga bagian yaitu *sensing*, *extraction*, dan *matching*. *Sensing* mengenai bagaimana sidik jari diperoleh secara digital menjadi *file* mentah. *Extraction* terkait *file* mentah sidik jari diekstraksi untuk mengetahui nilai karakteristik sidik jari. *Matching* merupakan proses mencocokkan karakteristik sidik jari dengan karakteristik sidik jari yang sudah ada.

### a. Sensing

Dalam sejarahnya pengenalan sidik jari dilakukan dengan “*ink technique*” dimana jari diberikan tinta hitam dan ditekan pada sebuah kertas untuk kemudian menggunakan kertas *scanner* untuk menghasilkan gambar digital. Saat ini pengenalan sidik jari menggunakan metode *live-scan* dimana gambar digital diperoleh dengan menempatkan permukaan sidik jari pada *scanner* sidik jari elektronik. Pada metode *live-scan* tidak menggunakan tinta, hanya perlu meletakkan jari pada bidang datar tertentu.



Gambar 6. Sidik jari diambil melalui *ink technique* dan *scanner* sidik jari

Bagian terpenting dari *scanner* sidik jari adalah sensor, komponen dimana gambar sidik jari dibuat. Tiga jenis sensor yang umum digunakan yaitu *optical*, *solid state*, dan *ultrasound*.

*Optical Sensors* mempunyai jantung bernama *Charge Couple Device* (CCD) yaitu sebuah *chip* silikon yang terbentuk dari dioda fotosensitif yang disebut photosites atau *pixel* yang dapat menghasilkan sinyal listrik. Photosites akan menangkap satu titik objek yang kemudian dirangkai bersama photosites lain menjadi sebuah bentuk gambar. *Frustrated Total Internal Reflection* (FTIR) salah satu metode tertua dan paling banyak digunakan dalam operasi identifikasi sidik jari. Permukaan jari diletakan pada permukaan kaca dimana terdapat sensor *optical* didalamnya. Tonjolan akan menyentuh permukaan kaca dan cekungan akan memberikan jarak dengan permukaan kaca. Pada salah satu bagian sisi kaca prisma akan memancarkan cahaya. Cahaya yang memasuki kaca prisma akan memantulkan cekungan dan menyerap tonjolan. Sehingga antara pantulan cekungan dan tojolan terpisah. Cahaya keluar pada sisi lain dari kaca prisma akan difokuskan pada *Complementary Metal Oxide Semikonduktor* (CMOS) sebagai sensor yang sensitif terhadap cahaya dan berfungsi mengubah cahaya menjadi elektron, yang kemudian dikirimkan ke sebuah *chip* dan konverter *analog* ke digital.

*Solid-state sensor* atau lebih sering dikenal sebagai sensor silikon sering digunakan sejak tahun 1990. Semua bagian dasar sensor silikon terdiri dari *array pixel*, masing-masing *pixel* menjadi sebuah sensor kecil tersendiri. Pengguna secara langsung menyentuh permukaan silikon. Informasi fisik yang diterima berupa *capasitive*, suhu, medan listrik, dan *piezoelectric* yang kemudian dijadikan sinyal elektrik.

*Ultrasound Sensors* secara umum merupakan pemanfaatan prinsip *echography*. Salah satu karakteristik dari gelombang suara adalah kemampuan

untuk menembus materi, memberikan pantulan yang masing memiliki impedansi yang berbeda. Teknik ini tidak digunakan secara luas untuk skala produksi.

#### **b. *Feature Extraction***

*Feature extraction* merupakan suatu pengambilan ciri dari suatu bentuk yang nantinya nilai yang didapatkan akan dianalisis untuk proses selanjutnya. *Feature extraction* dilakukan dengan menghitung jumlah titik atau *pixels* yang ditemui dalam setiap pengecekan, dimana pengecekan dilakukan dalam berbagai arah *tracing*. Pengecekan pada koordinat kartesian dari citra digital yang dianalisis yaitu vertikal, horizontal, diagonal kanan, dan diagonal kiri.

Dalam identifikasi sidik jari *feature extraction* berdasarkan citra sidik jari yang diterima oleh sensor. Alur tonjolan (*ridge line*) digambarkan berwarna gelap, sedangkan cekungan pada sidik jari digambarkan berwarna terang. Pada *feature extraction ridge line* dianalisis menjadi beberapa bagian, bagian tersebut bisa berupa *singularities* atau *singular region* yang diklasifikasikan menjadi *arch*, *loop*, dan *whorl*. Untuk lebih jelasnya klasifikasi *ridge line* dapat dilihat pada gambar 7.

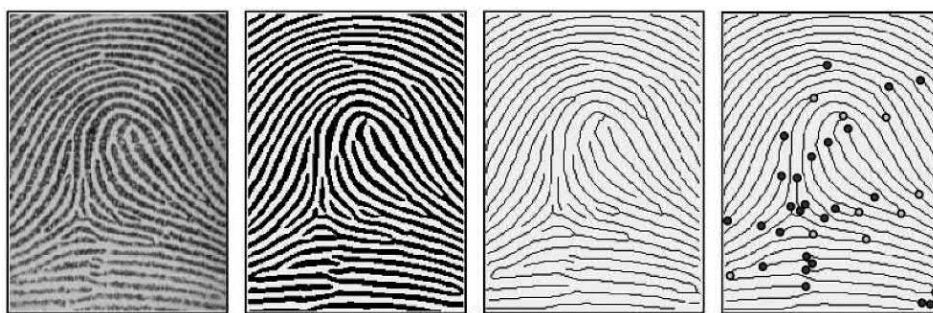


Gambar 7. *Singular legion*

*Loop* adalah bentuk pokok sidik jari dimana satu garis atau lebih datang dari satu sisi lukisan, melereng, menyentuh atau melintasi suatu garis bayangan yang

ditarik antara *delta* dan *core*, berhenti atau cenderung berhenti ke arah sisi semula. *Arch* merupakan bentuk pokok sidik jari yang semua garis-garisnya datang dari satu sisi lukisan, mengalir atau cenderung mengalir ke sisi yang lain dari lukisan itu, dengan bergelombang naik ditengah-tengah. *Whorl* adalah bentuk pokok sidik jari, mempunyai 2 *delta* dan sedikitnya satu garis melingkar di dalam *pattern area*, berjalan didepan kedua *delta*.

Dilihat secara khusus sidik jari memiliki bagian penting yang disebut *minutiae* yang dapat ditemui pada pola sidik jari. *Minutiae* merupakan variasi jalan dimana *ridge line* terputus atau tersambung (Anil K, 2008: 28). Selain klasifikasi pada gambar 7 identifikasi sidik jari juga menggunakan metode *minutiae extraction*. Metode yang sering digunakan dalam *minutiae extraction* adalah menggunakan gambar *gray-scale* sidik jari yang dikonversikan menjadi gambar binari. Proses ini menipiskan *ridge line* menjadi satu pixel. Kemudian dengan mudah gambar sederhana dari struktur sidik jari dapat dianalisis untuk memperoleh titik-titik *minutiae*. Proses ekstraksi *minutiae* dapat dilihat pada gambar 8.



Gambar 8. Proses ekstraksi *minutiae*

### c. *Matching*

*Matching* merupakan sebuah proses perbandingan hasil *feature extraction* dalam identifikasi *biometric*. *Matching* gambar sidik jari dengan kualitas tinggi dan variasi ringan sangat mudah dengan algoritma yang ada. Masalah utama dari *matching* adalah luas dan lebar permukaan sidik jari, sudut perputaran sidik jari, *non-linier* distorsi, perbedaan tekanan dan kondisi permukaan, serta *error extraction*.

*Minutiae-based methods* merupakan metode yang paling umum dan sering digunakan dan menjadi *basic* dari identifikasi sidik jari. Algoritma dari *minutiae matching* dengan membandingkan triplet  $m = \{x, y, \theta\}$  dimana  $x, y$  menunjukkan koordinat *minutiae* dan  $\theta$  menunjukkan sudut. *Minutiae-based Methods* bekerja berdasarkan algoritma *Hough Transform* berupa teknik transformasi citra untuk mendapatkan fitur dari sebuah citra. Algoritma *Hough transform* mengkonversi pola titik dan mendeteksi jarak antara puncak dari parameter transformasi. Proses *matching* dengan metode *minutiae-based methods* dapat dilihat pada gambar 9.

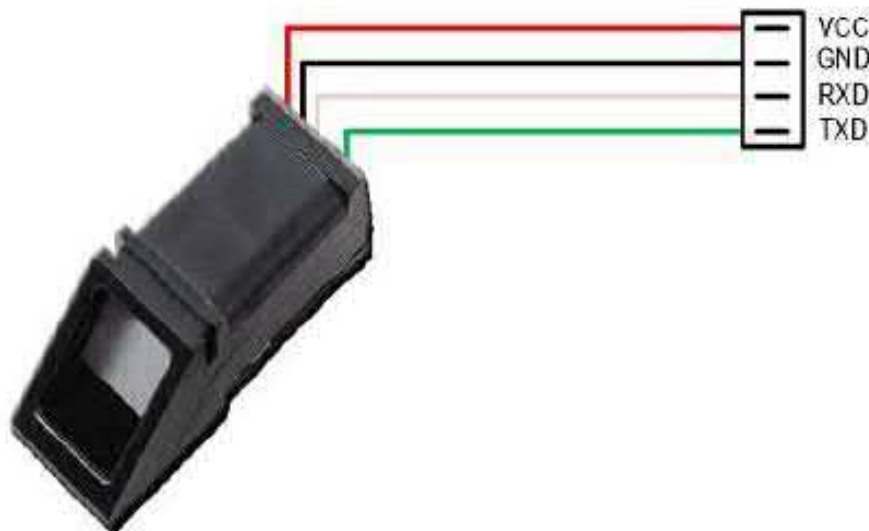


Gambar 9. Proses *matching* dengan metode *minutiae-based methods*: a) dan b) *minutiae* diekstraksi dari *template* dan input, c) *minutiae* ditandai dengan lingkaran, d) tiap lingkaran menunjukkan *minutiae* yang dicocokkan oleh algoritma.



### 2.2.7. Modul Sensor Sidik Jari

Modul sensor sidik jari telah banyak beredar di pasaran, salah satu modul sidik jari yang murah dan memiliki kinerja yang baik adalah modul sensor sidik jari dari perusahaan Adafruit. Modul ini sudah memiliki kemampuan *enrolling* data sidik jari secara otomatis, kita hanya perlu melakukan pemrograman ulang dengan memanggil *library* yang telah disediakan oleh Adafruit. Modul sensor Adafruit termasuk jenis *optical sensor* dengan kemampuan ekstraksi secara otomatis dan kemampuan *matching* dengan metode *minutiae-based method*. Bentuk fisik modul Adafruit ZM-20 dapat dilihat pada gambar 10.



Gambar 10. Modul sensor sidik jari Adafruit

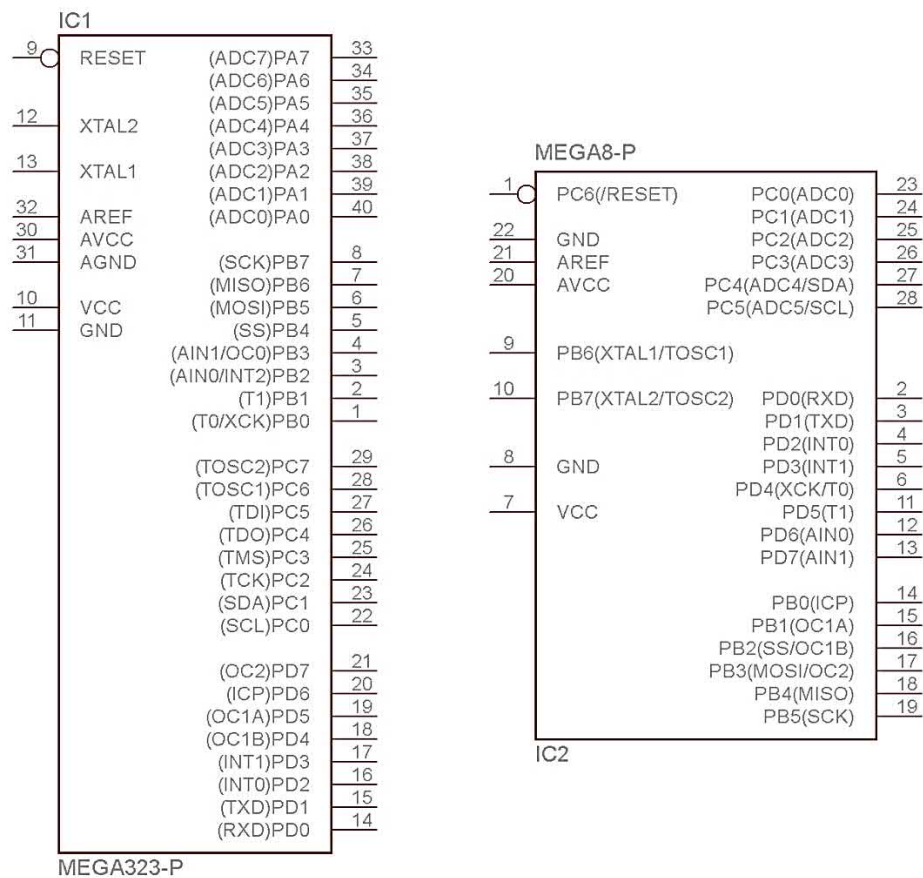
Spesifikasi modul sidik jari Adafruit ZM-20:

- *Supply voltage : 3,6-6,0 VDC*
- *Operating current : 120mA max*
- *Peak current : 150mA max*
- *Fingerprint imaging time : < 1,0 Secon*
- *Window Area : 14 mm x 18 mm*
- *Signature file : 256 byte*

- *Template file : 512 byte*
- *Storage capacity : 162 template*
- *Safety rating : (1 – 5 low to high safety)*
- *False Acceptance Rate : < 0,001% (security level 3)*
- *False Reject Rate : < 1,0% (security level 3)*
- *Interface : TTL series*
- *Baud Rate : 9600, 19200, 28800, 38400, 57600, (default 57600)*
- *Working temperature rating : -20C to +50C*
- *Working humidity : 40%-80% RH*
- *Full dimensions : 56 x 20 x 21,5 mm*
- *Exposed dimensions : (when place in the box) 12 x 12 x 12 mm triangular*
- *Wight : 20 grams*

### **2.2.8. Mikrokontroler**

Mikrokontroler terdiri atas ribuan transistor dan terdapat berbagai macam fungsi logika, memori, dan bahkan beberapa mikrokontroler tertentu memiliki *operational amplifier* dan fungsi-fungsi khusus seperti *Analog to Digital Converter* (ADC) (Andi, 2012: 53). Mikrokontroler bisa disebut juga sentral pemrosesan (CPU). CPU juga dapat mengakses memori, melakukan kalkulasi, pengontrolan, dan penanganan interupsi. Ini dilakukan menggunakan arsitektur Harvard (bus untuk memori, program, dan data terpisah) sehingga dihasilkan performa yang tinggi. Hal ini dikarenakan instruksi pada memori program dieksekusi dengan *single level pipelining*. Dengan demikian, pada saat sebuah instruksi dieksekusi, instruksi berikutnya dapat diakses dari memori program. Konsep ini memungkinkan instruksi dieksekusi pada setiap siklus *clock* (Widodo, 2009: 10). Contoh IC mikrokontroler dapat dilihat pada gambar 11.

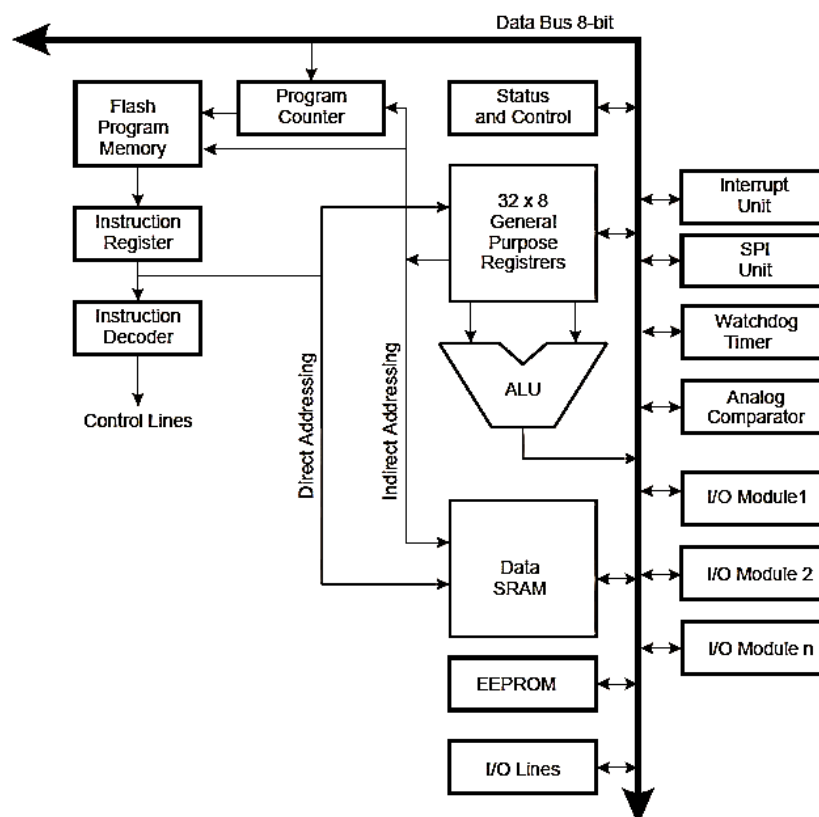


Gambar 11. *Chip* mikrokontroler

Ada beberapa macam bahasa pemrograman untuk mikrokontroler, seperti assembly, C dan Basic. Namun, *file* yang diunduh adalah *file* heksa dengan ekstensi HEX. Bahasa pemrograman berfungsi untuk mempermudah manusia dalam memprogram *mikrokontroler* dengan bahasa-bahasa yang lebih manusiawi, sedangkan *file* heksa yang biasa disebut program *object* dibuat agar mikrokontroler dapat membaca perintah-perintah yang kita programkan. Konversi dari *file* yang dibuat dalam bahasa pemrograman ke bentuk program *object* dilanjutkan dengan proses kompilasi atau *compile* (Andi, 2012: 54).

### 2.2.8.1. Mikrokontroler AT-mega

ATMega adalah mikrokontroler keluaran dari Atmel yang mempunyai arsitektur *Reduce Instruction Set Computer* (RISC) dimana setiap proses eksekusi data lebih cepat dari pada arsitektur *Completed Instruction Set Computer* (CISC). Mikrokontroler ATmega memiliki arsitektur Harvard seperti ATmega 2560 dan 328P, yaitu memisahkan memori untuk kode program dan memori untuk data sehingga dapat memaksimalkan kerja secara paralel. Instruksi-instruksi dalam memori program dieksekusi dalam satu alur tunggal, dimana pada saat satu instruksi dikerjakan instruksi berikutnya sudah diambil dari memori program. Mikrokontroler ATmega 2560 dan 328P beroperasi pada frekuensi *clock* sampai 16 Mhz. Alur instruksi pada ATmega 328 dapat dilihat pada gambar 12.



Gambar 12. Diagram blok ATmega328

ATmega 2560 dan 328P memiliki dua *Power Saving Mode* yang dapat dikontrol melalui *software*, yaitu *Active Mode* dan *Power Down Mode*. Pada *Active Mode*, CPU tidak aktif sedangkan isi RAM tetap dipertahankan dengan *timer/counter*, *serial port*, dan *interrupt system* tetap berfungsi. Pada *Power Down Mode*, isi RAM akan disimpan tetapi osilatornya tidak akan berfungsi sehingga semua fungsi dari *chip* akan berhenti sampai mendapat *reset* secara *hardware*. Salah satu mikrokontroler yang menggunakan ATmega 2560 adalah mikrokontroler keluaran Arduino yaitu Arduino mega. Sedangkan mikrokontroler yang menggunakan ATmega 328P adalah Arduino Uno.

#### **2.2.8.2. Memori ATmega**

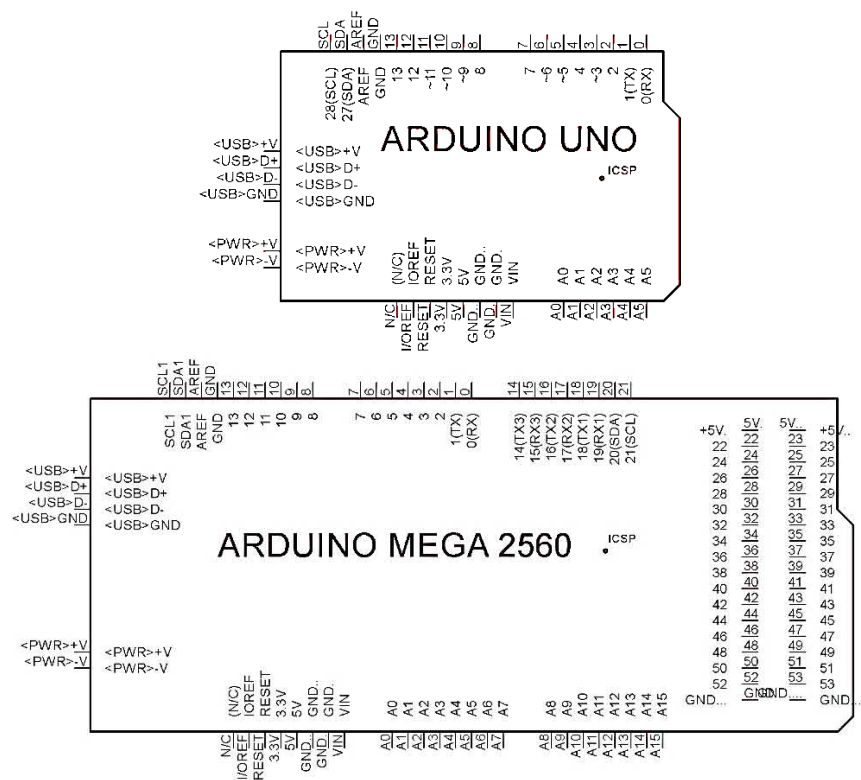
Mikrokontroler ATmega memiliki 3 jenis memori, yaitu *flash memory*, *Static Random Access Memory* (SRAM) dan memori *Electrically Erasable Programmable Read Only Memory* (EEPROM). Ketiganya memiliki ruang tersendiri dan terpisah. *Flash memory* dan EEPROM masuk dalam kategori memori *non-volatile*. Artinya, sekalipun ATmega kehilangan catu daya, data atau program pada kedua memori tersebut tidak akan hilang. Sedangkan SRAM masuk dalam kategori memori *volatile*, yang datanya akan hilang ketika ATmega kehilangan catu daya.

*Flash memory* atau memori program berfungsi untuk menyimpan program dimana sebagian memori tersebut digunakan untuk program *bootloader*. SRAM merupakan memori yang digunakan untuk menyimpan data-data variabel sementara. Sedangkan EEPROM merupakan memori yang digunakan untuk

menyimpan data dalam waktu lama. Setiap ATmega memiliki spesifikasi memori yang berbeda-beda sesuai dengan kegunaannya. Contoh untuk ATmega 328P memiliki *flash memory* sebesar 32 KB sedangkan ATmega 2560 memiliki *flash memory* sebesar 256 KB.

### 2.2.8.3.Arduino

Arduino adalah suatu papan (*board*) yang berisi mikrokontroler. Arduino adalah papan elektronik bersifat *open source* yang didalamnya terdapat komponen utama yaitu sebuah *chip* mikrokontroler dengan jenis AVR dari perusahaan Atmel. Modul Mikrokontroler Arduino diciptakan oleh Massimo Banzi, David Cuartiles, Tom Gianluca, David A. Mellis, dan Nicholas Zambetti pada tahun 2005. Arduino Mega merupakan salah satu produk berlabel Arduino. Contoh *board* Arduino dapat dilihat pada gambar 13.



Gambar 13. Arduino Uno dan Arduino Mega

Beberapa *board* Arduino yang dikenal menggunakan ATmega seperti Arduino Uno dengan ATmega 328P dan Arduino Mega dengan ATmega 2560. Arduino Uno memiliki memori dan konektifitas lebih sedikit dibandingkan dengan Arduino Mega. Di sisi lain penggunaan Arduino Uno memiliki keuntungan dengan ukuran modul yang lebih kecil. Untuk lebih jelas perbedaan spesifikasi dapat dilihat pada tabel 4.

Tabel 4  
Perbandingan Spesifikasi Arduino Uno dan Mega

NO	Spesifikasi	Arduino Uno	Arduino Mega
1	<i>Microcontroller</i>	ATmega 328P	Atmega 2560
2	<i>Operating Voltage</i>	5 V	5 V
3	<i>Input Voltage (Recommendad)</i>	7-12 V	7-12 V
4	<i>Digital I/O pins</i>	14 & 6 PWM <i>out</i>	54 & 6 PWM <i>out</i>
5	<i>Analog Input Pins</i>	6	16
6	<i>DC Current per I/O pin</i>	40 mA	20 mA
7	<i>DC Current for 3.3 Volt Pin</i>	50 mA	50 mA
8	<i>Flash Memory</i>	32 KB, 5 KB <i>bootloader</i>	256 KB, 8KB <i>bootloader</i>
9	SRAM	2 Kb	8 Kb
10	EEPROM	1 Kb	4 Kb
11	<i>Clock Speed</i>	16 MHz	16 MHz

Arduino Mega 2560 memiliki jumlah *pin* terbanyak dari semua *board* Arduino. Arduino Mega 2560 memiliki 54 buah digital *pin* yang dapat digunakan sebagai *input* atau *output*, dengan menggunakan fungsi *pinMode()*, *digitalWrite()*, dan *digitalRead()*. Sedangkan Arduino Uno hanya memiliki 14 buah *digital pin*. Masing-masing *pin* tersebut bekerja pada tegangan 5 V. Masing-masing *pin*

tersebut dapat bekerja dengan arus sebesar 20 mA pada Arduino Mega dan 40 mA pada Arduino Uno, serta memiliki tahanan *pull-up* antara 20-50 Kohm (secara *default* dalam posisi *disconnect*). Untuk menghindari kerusakan pada *chip* mikrokontroler penggunaan arus maksimal 40 mA sebisa mungkin dihindari.

Kapasitas memori pada Arduino Uno dan Arduino Mega memiliki perbedaan yang signifikan. *Flash memory* pada Arduino Uno sebesar 32 KB dengan 5 KB digunakan sebagai *bootloader* sedangkan Arduino Mega sebesar 256 KB dengan 8 KB digunakan sebagai *bootloader*. SRAM pada Arduino Uno sebesar 2 Kb dan pada Arduino Mega sebesar 8 Kb. Pada memori EEPROM Arduino Uno memiliki kapasitas penyimpanan sebesar 1 Kb sedangkan Arduino Mega sebesar 4 Kb. Namun demikian kedua Arduino tersebut berjalan pada *clock speed* yang sama yakni 16 MHz.

Beberapa *pin* memiliki fungsi khusus yaitu:

- *Serial*, Arduino Mega memiliki 4 serial yang masing-masing terdiri dari 2 *pin*.  
*Serial 0*: *pin* 0 (RX) dan *pin* 1 (TX). *Serial 1*: *pin* 19 (RX) dan *pin* 18 (TX).  
*Serial 2*: *pin* 17 (RX) dan *pin* 16 (TX). *Serial 3*: *pin* 15 (RX) dan *pin* 14 (TX).  
 Sedangkan Arduino Uno memiliki sepasang *serial* pada *pin* 0 (RX) dan *pin* 1 (TX). RX digunakan untuk menerima dan TX untuk transmit data *serial* TTL.  
*Pin* 0 dan *pin* 1 adalah *pin* yang digunakan oleh *chip* USB-to-TTL ATmega16U2.
- *External Interrupts*, yaitu *pin* 2 (untuk *interrupt* 0), *pin* 3 (*interrupt* 1), *pin* 18 (*interrupt* 5), *pin* 19 (*interrupt* 4), *pin* 20 (*interrupt* 3), dan *pin* 21 (*interrupt* 2). Dengan demikian Arduino Mega 2560 memiliki jumlah *interrupt* yang



cukup melimpah: 6 buah. Gunakan fungsi *attachInterrupt()* untuk mengatur *interrupt* tersebut. Sedangkan Arduino Uno hanya memiliki 2 yaitu *pin 2 (interrupt 0)*, *pin 3 (interrupt 1)*,

- PWM: Pada Arduino Mega *Pin 2* hingga *13* dan *44* hingga *46*, yang menyediakan *output* PWM 8-bit dengan menggunakan fungsi *analogWrite()*. Sedangkan pada Arduino Uno tersedia dalam *pin 3*, *5*, *6*, *9*, *10*, dan *11*.
- SPI: Pada Arduino Mega *Pin 50 (MISO)*, *51 (MOSI)*, *52 (SCK)*, dan *53 (SS)* mendukung komunikasi SPI dengan menggunakan *SPI Library*. Sedangkan pada Arduino Uno tersedia pada *pin 10 (SS)*, *11 (MOSI)*, *12 (MISO)*, *13 (SCK)*.
- LED : antara Arduino Mega dan Arduino Uno memiliki *pin* LED yang sama yaitu *Pin 13*. Pada *pin 13* terhubung *built-in* LED yang dikendalikan oleh digital *pin 13*. Set *HIGH* untuk menyalakan led, *LOW* untuk mematikan.
- TWI: pada Arduino Mega *Pin 20 (SDA)* dan *pin 21 (SCL)* yang mendukung komunikasi TWI dengan menggunakan *Wire Library*. Pada Arduino Uno terdapat pada *pin A4* atau *SDA* dan *pin A5* atau *SCL*.

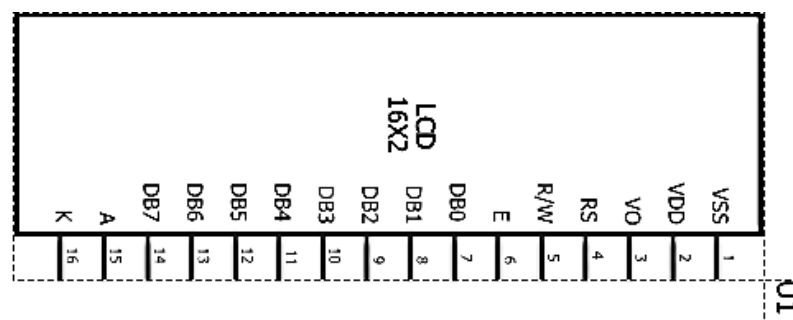
Arduino Uno memiliki 6 buah *input analog*, yang diberi tanda dengan *A0*, *A1*, *A2*, *A3*, *A4*, dan *A5*. Sedangkan Arduino Mega memiliki 16 *pin* dari *A0-A15*. Secara *default*, *pin-pin* tersebut diukur dari *ground* ke *pin 5V*, namun bisa juga menggunakan *pin AREF* dengan menggunakan fungsi *analogReference()*. Beberapa *pin* lainnya pada kedua *board* ini adalah :

- AREF. Sebagai referensi tegangan untuk *input analog*.

- *Reset*. Hubungkan ke LOW untuk melakukan *reset* terhadap Arduino. Sama dengan penggunaan tombol *reset* yang tersedia.

### 2.2.9. *Liquid Cristal Display (LCD)*

LCD adalah salah satu komponen elektronika yang berfungsi sebagai tampilan suatu data, baik karakter, huruf ataupun grafik. LCD terdiri dari dua bagian. Bagian pertama merupakan panel LCD sebagai media penampil informasi dalam bentuk huruf/angka dua baris. Bagian kedua merupakan sebuah sistem yang dibentuk dengan mikrokontroler yang ditempel dibalik pada panel LCD yang berfungsi mengatur tampilan LCD. Ada banyak jenis LCD yang beredar di pasaran. Namun ada standarisasi yang cukup populer digunakan yaitu LCD dengan tampilan 2 x 16 (2 baris x 16 kolom) dengan konsumsi daya rendah. Adapun letak *pin* pada Modul LCD 16 x 2 dapat dilihat pada gambar 14.



Gambar 14. Modul LCD 16 x 2

Urutan *pin* (1) dimulai dari sebelah kanan (terletak di pojok kanan bawah) dan untuk LCD yang memiliki 16 *pin*, 2 *pin* terakhir (15 dan 16) adalah anoda dan katoda untuk *back-lighting*. Keterangan masing-masing *pin* pada LCD 16 x 2 dapat dilihat pada tabel 5.

Tabel 5  
Konfigurasi *Pin* LCD 16 x 2

<i>Pin</i>	Deskripsi
1	<i>Ground</i>
2	VCC 5 Volt DC
3	Pengatur kontraks
4	“RS” Instruction/Regoster Select
5	“R/W” Read/Write LCD Registers
6	“EN” Enable clock
7-16	Data I/O <i>Pin</i> ss

### 2.2.10. *Magnetic Switch*

*Magnetic switch* merupakan saklar yang dapat merespon medan magnet yang berada disekitarnya. *Magnetic switch* ini seperti halnya sensor limit *switch* yang diberikan tambahan plat logam yang dapat merespon adanya magnet. Untuk lebih jelas bentuk fisik dan skema *magnetic switch* dapat dilihat pada gambar 15.



Gambar 15. *Magnetic switch*

*Magnetic switch* tersebut biasa digunakan sebagai deteksi pengamanan pada pintu dan jendela. Dalam pemasangannya *magnetic switch* ini dapat dipasang dengan cara ditanam di bagian pintu atau hanya ditempelkan saja di jendela. Pemasangan dapat dipasang pada pintu atau jendela yang terbuat dari kayu atau dari logam, seperti aluminium. *Magnetic switch* yang digunakan pada penelitian ini adalah type PE-905, dapat digunakan pada suatu perangkat pengendalian otomatis sampai tegangan maksimal 4V dan arus sampai 100-500mA.

## **BAB V**

### **PENUTUP**

#### **5.1. Kesimpulan**

*Smart home security system* berbasis Arduino ini dirancang dengan mengkombinasikan dua metode yaitu *biometric fingerprint* dan *password*. Sistem ini bekerja dengan menggunakan modul Arduino Mega dengan IC 2560 sebagai sistem kontrol. Mekanisme penguncian pintu menggunakan solenoid *door lock*. *Smart home security sistem* berbasis Arduino juga memiliki fitur tambahan berupa sistem pengaman dengan *magnetic switch*, *emergency backup supply*, *emergency entry* dengan modul bluetooth HC-05, dan indikator baterai.

*Smart home security system* berbasis Arduino telah melalui beberapa tahap pengujian. Pada uji *black box* setiap komponen mampu bekerja sesuai desain *software* yang telah direncanakan. Pada uji ahli *smart home security system* berbasis Arduino berhasil mendapat skor 80,83% dengan kategori “baik”. Pada tahap uji pengguna *smart home security system* berbasis Arduino mendapatkan skor 84,33% dengan kategori “sangat baik”.

Dengan demikian berdasarkan analisis data *smart home security system* berbasis Arduino telah memenuhi kriteria dalam berbagai pengujian yang telah dilakukan. *Smart home security system* berbasis Arduino telah layak untuk digunakan sebagai sistem pengaman akses pintu di lingkungan rumah tangga.

## 5.2. Saran

Berdasarkan kesimpulan dan proses pengembangan *smart home security system* berbasis Arduino, maka peneliti dapat memberikan saran guna pengembangan sistem keamanan lebih lanjut. Proses pengembangan selanjutnya masih terdapat beberapa aspek yang bisa ditingkatkan, seperti penggunaan modul *wifi* sebagai media konektivitas dengan sistem perangkat *home automation* lain sehingga *smart home security system* berbasis Arduino dapat bekerja terintegrasi. Dari aspek mekanik pembuka pintu dapat ditambahkan sistem pembuka otomatis dengan servo maupun mekanisme pembuka pintu yang lain. Pada proses instalasi apabila alat digunakan pengunci pintu dengan daya yang besar maka dibutuhkan *interface* tambahan sebagai penghubung.

## DAFTAR PUSTAKA

- Andi Nalwa. 2012. *Teknik Rancang Bangun Robot: Tingkat Dasar*. Yogyakarta: CV.ANDI.
- Anil K. Jain, Patrick J. Flynn, dkk. 2008. *Handbook of Biometrics*. New York: Springer Science+Business Media. ISBN-13: 978-0-387-71040-2.
- Anil K. Jain., Ross, dkk. 2004. *An Introduction to Biometric Recognition*. IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 4–20.
- Badan Pusat Statistik. 2017. *Statistika Kriminal 2017*. Jakarta:BPS.
- Changmin Lee, Luca Zappaterra, dkk. 2014. *Securing Smart Home : Technologies, Security Challenges, and Security Requirement*. Seoul: Workshop on Security and Privacy in Machine-to-Machine Communications.
- Emzir, 2008. *Metodologi Penelitian Pendidikan : Kuantitatif dan Kuantitatif*. PT Rajagafindo Persada. Jakarta.
- KBBI Daring. <https://kbbi.web.id>. (03/10/2018).
- M. Faundez-Zanuy. 2006. *Biometric Security Technology*. IEEE A&E Syst. Mag., vol. 21, no. 6, pp. 15–26.
- M. Gayathri, P. Selvakumari, dkk. 2014. *Fingerprint and GSM based Security System*. Int. J. Eng. Sci. Res. Technol., vol. 3, no. 4, pp. 4024–4029.
- Nur Adila. 2014. *Face Recognition Security System for Access Control*. Malaysia: Universiti Teknologi Malaysia.
- Rara Fitri. 2009. *Analisis Determinan Penyebab Terjadinya Fear of Crime pada Kasus Pencurian di Kalangan Ibu Rumah Tangga*. Universitas Indonesia: Jurnal Kriminologi Indonesia Vol. 5.
- Rajadurai. 2015. *Android Mobile Based Home Security and Device Control Using GSM*. International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS) 2015.
- Setiawan Idris. 2015. *Sistem Pengaman Pintu Menggunakan Sensor Sidik Jari (fingerprint)*. Indonesia: Universitas Negeri Semarang.

- Setya Ardhi, Savitri. 2011. *Perencanaan dan Pembuatan Sistem Pengaman Rumah dengan Teknologi Pengenalan Sidik Jari*. IDeaTech 2011. Pp. 398-406. ISSN: 2089-1121.
- Simon Liu, M Silverman. 2001. *A Practical Guide to Biometric Security Technology*. PP. 27-32.
- Singgih Santoso. 2009. *Panduan Lengkap Menguasai Statistik dengan SPSS 17*. Jakarta: PT, Elex Media Komputindo.
- Sugiyono. 2008. *Metode Penelitian Kuantitatif, Kualitatif dan R & D*. Cetakan keempat. Bandung. Alfabeta.
- Suharsimi Arikunto. 2010. *Prosedur Penelitian: Suatu Pendekatan Praktik*. Edisi revisi 2010. Cetakan 14. Rineka Cipta. Jakarta.
- Tom Wayteg. 2003. *Kamus Internet, Cara Cepat Praktis Masuk Dunia Cyber*. Surabaya: liris cetakan 1.
- Trianto. 2011. *Panduan Lengkap Penelitian Tindakan Kelas [Classroom Action Research] Teori & Praktik*. Jakarta: Prestasi Pustakarya.
- Widodo Budiharto, Sigit Firmansyah. 2009. *Elektronika Digital dan Mikroprosesor*. Jakarta: PT Elex Media Komputindo.