SMART HOME SECURITY SYSTEM BERBASIS MIKROKONTROLER

Jalu Wardoyo
Fakultas Teknik, Program Studi Pendidikan Teknik Elektro
Universitas Negeri Semarang
Email: jaluwardoyo@gmail.com

Noor Hudallah
Jurusan Teknik Elektro, Fakultas Teknik
Universitas Negeri Semarang
Email: noorhudallah@mail.unnes.ac.id

Aryo Baskoro Utomo
Jurusan Teknik Elektro, Fakultas Teknik
Universitas Negeri Semarang
Email: aryobaskoro@mail.unnes.ac.id

ABSTRAK

Tingginya tindak kejahatan pencurian di rumah tangga perlu diantisipasi dengan penggunaan sistem keamanan rumah yang modern, salah satunya yaitu *smart home*. Salah satu penerapan *smart home* berupa *safety system.* Studi ini mengajukan perancangan sistem keamanan *smart home* berbasis mikrokontroler. Sistem keamanan *smart home* ini menggunakan kombinasi metode pengaman *biometric fingerprint* dan *password.* Metode perancangan sistem dengan metode *Research and Development (RnD)*. Proses RnD dibagi menjadi tiga tahap yaitu tahap studi, *research,* dan pengembangan. Tahap studi meliputi studi pustaka dan studi lapangan terkait sistem keamanan rumah, tahap *research* berupa pembuatan dan pengujian *prototype* sistem keamanan, dan tahap pengembangan berupa pengujian dan perbaikan terhadap kekurangan sistem keamanan. Penelitian ini menghasilkan *prototype* sistem keamanan *smart home* yang memiliki kemampuan memberikan akses terhadap pintu dengan metode autentifikasi *biometric fingerprint* dan *password* serta fitur tambahan *emergency backup supply* dan *emergency entry.* Akses pintu diberikan ketika autentifikasi berhasil dilakukan dan mikrokontroler akan memberikan perintah untuk menghidupkan *solenoid door lock* sebagai mekanisme penguncian pintu. Sistem ini bekerja menggunakan beberapa perangkat diantaranya: Arduino Mega, *modul fingerprint*, *keypad*, LCD, *power supply unit* (PSU), *magnetic switch*, *solenoid door lock,* dan buzzer.

Kata kunci: *smart home*; *safety system*; arduino mega; *fingerprint*; *password*; *solenoid door lock*.

ABSTRACT

The height of domestic crime can be anticipated by using a modern home security system, such as smart home. One of its implementation is safety system. This study proposes a design of microcontroller based smart home security system. This smart home security system use combination of biometric fingerprint and password method. System is developed by using Reseearch and development (RnD) method. RnD divided into 3 stages that is study, research, and development. Study phase consist of literature and field review about home security system. Research phase consist of building and testing security system prototype, and development phase consist of testing and fixing flaws of security system. This study resulted a smart home security system prototype which gives access to door using biometric fingerprint and password authentication method, also emergency backup supply and emergency entry features. Access to door given when authentication is done and microcontroller will give command to start solenoid door lock as door lock mechanism. This system works using hardware such as arduino mega, fingerprint module, keypad, LCD, power supply unit (PSU), magnetic switch, solenoid door lock, and buzzer.

Keywords: *smart home; safety system; arduino mega; fingerprint; password; solenoid door lock.*

1. PENDAHULUAN

Salah satu kebutuhan dasar manusia adalah rasa aman. Namun demikian kebutuhan akan rasa aman belum terpenuhi. Data Biro Pembinaan dan Operasional, Mabes Polri menunjukkan peningkatan jumlah

kejadian kejahatan (*crime total*) pada periode tahun 2014 hingga 2016 yaitu sebesar 325.317 pada tahun 2014, meningkat pada tahun 2015 dan 2016 menjadi 352.936 dan 357.197 [1]. Salah satu objek tindak kejahatan adalah di rumah tangga dimana jenis kejahatan tersebut dibedakan menjadi beberapa kategori seperti pencurian, penganiayaan, pencurian dengan kekerasan, pelecehan seksual, dan lain-lain. Pencurian menjadi tindak kejahatan paling dominan sebesar 87,19% dari total jumlah tindak kejahatan di rumah tangga [1]. Tingginya tindak pencurian di rumah tangga dapat diantisipasi dengan penggunaan sistem pengaman rumah yang lebih modern salah satunya yaitu *smart home.*

Smart home merupakan tempat tinggal yang didalamnya terdapat gabungan beberapa alat yang memiliki kemampuan atau kemahiran tertentu bergantung pada aplikasinya. Berdasarkan aplikasinya *smart home* dibagi menjadi beberapa 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 kejahatan di rumah tangga yaitu *safety system* [2]. Penerapan *safety system* dalam *smart home* dapat berupa deteksi asap, *Close Circuit Tele Vision* (CCTV), dan *smart door lock* [2]. *Safety system* terkait akses pintu melibatkan proses autentifikasi dan atau identifikasi pengguna.

Penelitian *safety system* terkait akses pintu telah dilakukan menggunakan identifikasi *biometric fingerprint* dan *password*. Identifikasi *biometric* lebih unggul dibandingkan identifikasi lain [3]. Perbandingan penggunaan berbagai metode *biometric* telah dilakukan dan diperoleh hasil bahwa *biometric fingerprint* memiliki keunggulan dalam tingkat akurasi, mudahnya penerapan pada sistem, dan bersifat permanen dibanding jenis *biometric* lainnya [4],[5]. Dalam implementasi identifikasi *biometric fingerprint* dan *password* digabungkan dengan beberapa teknologi lainnya. Modul *Global System of Mobile Communications* (GSM) digunakan mengirimkan pesan peringatan kesalahan [6] ataupun kombinasi PIN/*Password* untuk mengakses pintu [7]. Penelitian [8] menggunakan *password* sebagai metode pengamanan dan GSM sebagai media autentifikasi. Sistem keamanan tersebut bekerja ketika pengguna memasukan *password* maka modul GSM akan mengirimkan perintah *authorize* pada *mobile device* untuk memperoleh akses terhadap pintu. Pemanfaatkan kapasitas memori penyimpanan *Electrically Erasable Programmable Read-Only Memory* (EEPROM) pada modul mikrokontroler dapat digunakan sebagai *data loggger* sistem pengaman rumah [9].

Beberapa penelitian tersebut ([6]–[9]) masih memiliki kekurangan.. Penggunaan modul GSM memerlukan biaya tambahan dalam pengoperasiannya. Jeda waktu yang dibutuhkan untuk memperoleh akses pintu cukup lama. Kombinasi *password* tidak dapat disesuaikan dengan preferensi masing-masing pengguna. Penelitian lanjutan *safety system* terkait akses pintu perlu untuk dilakukan.

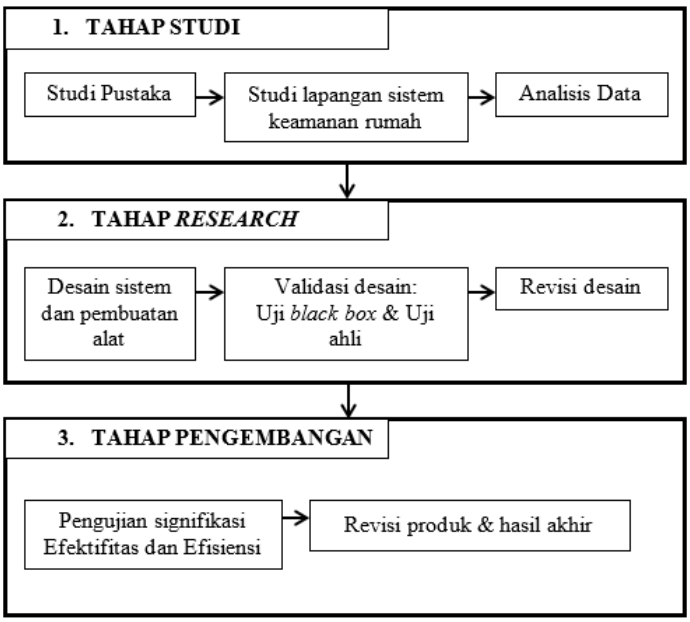
Dalam artikel ini diusulkan sistem keamanan *smart home* dengan penggunaan metode *biometric* dan *password* sebagai metode keamanan akses terhadap pintu, mikrokontroler sebagai pusat kontrol, memori EEPROM sebagai media penyimpanan, *relay* dan *solenoid door lock* sebagai mekanisme penguncian pintu. Mikrokontroler yang digunakan pada penelitian ini mengunakan Arduino Mega serta menambahkan fitur *magnetic switch* sebagai mekanisme keamanan pintu untuk deteksi pelanggaran hak akses pintu, *emergency backup supply* sebagai mekanisme keamanan sistem ketika sistem kehilangan daya sumber utama, dan *emergency entry* sebagai pembuka hak akses pintu secara darurat.

2. METODOLOGI PENELITIAN

Metode penelitian yang digunakan pada penelitian ini adalah *Reasearch and Development (RnD). Research and Development* adalah metode penelitian yang digunakan untuk menghasilkan produk tertentu, dan menguji keefektifan produk tersebut. Produk dalam penelitian ini berupa sistem keamanan *smart home* berbasis mikrokontroler. Untuk mewujudkan suatu sistem keamanan *smart home*, maka pada bagian ini akan dijelaskan tentang langkah dan alat yang digunakan dalam penelitian.

2.1 Langkah-langkah Penelitian

Langkah penelitian ini dibagi menjadi tiga tahapan yaitu tahap studi, tahap *research*, dan tahap pengembangan. Tahapan dalam penelitian ini dipaparkan pada diagram alir gambar 1.



Gambar 1. Langkah-langkah Penelitian

Tahap studi meliputi studi pustaka dan studi lapangan. Tahap studi pustaka dilakukan untuk mencari referensi terkait dengan penelitian yang akan dilakukan. Referensi yang dirujuk berkaitan dengan sistem keamanan rumah beserta metode-metodenya dan sistem kontrol menggunakan mikrokontroler. Studi lapangan dilakukan dengan teknik wawancara dan observasi. Hasil dari tahap studi tersebut kemudian dilakukan analisis. Hasil analisis digunakan sebagai acuan perancangan desain sistem keamanan *smart home*.

Tahap *research* meliputi perancangan desain dan pembuatan *prototype* sistem keamanan. Desain dan *prototype* dibuat berdasarkan hasil analisis pada tahap studi. Hasil *prototype* sistem dilakukan validasi desain untuk mengetahui kualitas desain sistem tersebut. Validasi desain meliputi uji ahli dan uji *black box*. Uji ahli dilakukan dengan mempresentasikan desain *prototype* kepada para ahli atau pakar yang memiliki kompetensi terkait dengan penelitian yang dilakukan sedangkan uji *black box* dilakukan untuk mengetahui kinerja fungsional perangkat lunak terhadap keluaran sistem. Pada tahap validasi desain akan ditemukan dari kekurangan pada desain sistem keamanan yang mengarah pada revisi desain. Revisi desain dilakukan berdasarkan saran dan komentar para ahli. Revisi desain lebih mengarah pada evaluasi terhadap proses, sehingga perbaikan lebih bersifat internal. Revisi desain ditujukan untuk meningkatkan mutu produk sebelum memasuki tahap selanjutnya yaitu tahap pengembangan.

Tahap pengembangan dilakukan dengan melakukan uji coba sistem. Uji coba sistem dilakukan untuk mengetahui apakah sistem yang telah dibuat memenuhi aspek fungsionalitas, signifikasi, efektifitas, dan efisiensi. Uji coba yang dilakukan berupa uji pengguna. Uji pengguna dilakukan dengan demonstrasi penggunaan sistem keamanan dan memberikan kuesioner sebagai media pengumpulan data. Analisis dilakukan pada hasil uji pengguna untuk kemudian hasil tersebut digunakan sebagai acuan untuk melakukan revisi produk. Revisi produk bersifat perbaikan internal dengan uji coba yang lebih luas serta revisi produk didasarkan pada evaluasi hasil dan efektifitas. Hasil dari revisi produk pada tahap ini dapat dikatakan sebagai hasil akhir atau produk akhir.

2.2 Alat dan Bahan

Proses membuat *prototype* sistem keamanan dibutuhkan beberapa perangkat keras dan perangkat lunak. Perangkat keras yang digunakan dalam pembuatan *prototype* sistem keamanan ini adalah Arduino Mega

a) *Module fingerprint ZM-20*
b) *Keypad 3 x 4*
c) *Liquid Crystal Display (LCD)*
d) Adaptor 12V 3A
e) *Relay*
f) *Solenoid*
g) *Magnetic switch*

h) *Bluetooth* HC-05
i) *Button*
j) Regulator DC-DC 12V-5V
k) *Buzzer*
l) *Power Supply Unit* (PSU)

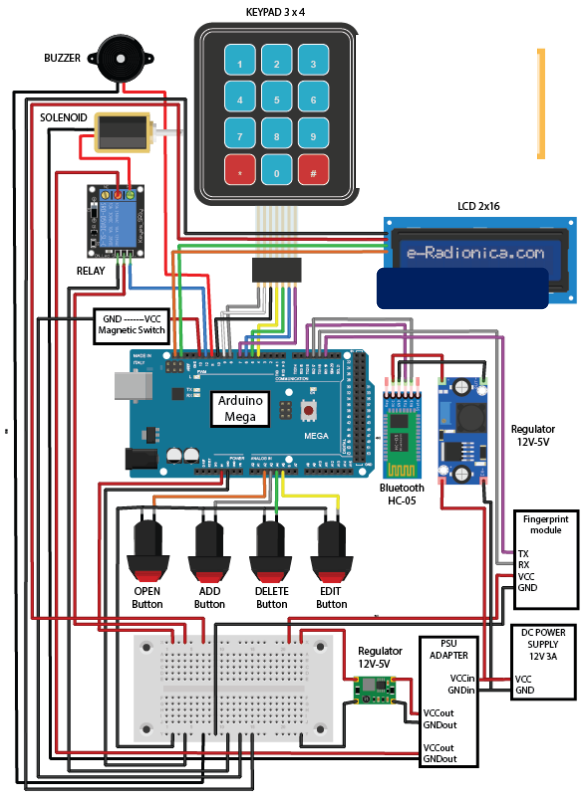
Sedangkan perangkat lunak yang digunakan dalam pembuatan *prototype* sistem keamanan ini adalah:

a) Fritzing merupakan aplikasi yang digunakan untuk membuat skema rangkaian sistem keamanan.
b) Sketch Arduino merupakan aplikasi yang digunakan untuk compile dan upload program kedalam Arduino Mega.

2.3 Alur Kerja System

Alur kerja sistem pada penelitian ini terdiri dari tiga bagian, antara lain perangkat keras (*hardware*), perangkat lunak (*software*), dan pengguna (*user*). Perangkat keras adalah rangkaian elektronis yang disusun sedemikian rupa sehingga dapat mengolah data dan menghasilkan informasi [10]. Perangkat lunak yaitu sistem dan aplikasi yang digunakan untuk memproses masukan (*input*) untuk menjadi informasi [11]. Pengguna adalah manusia yang terlibat dalam pengoperaian serta mengatur sistem [12]. Ketiga bagian tersebut bekerja secara terintegrasi pada sistem keamanan *smart home.*

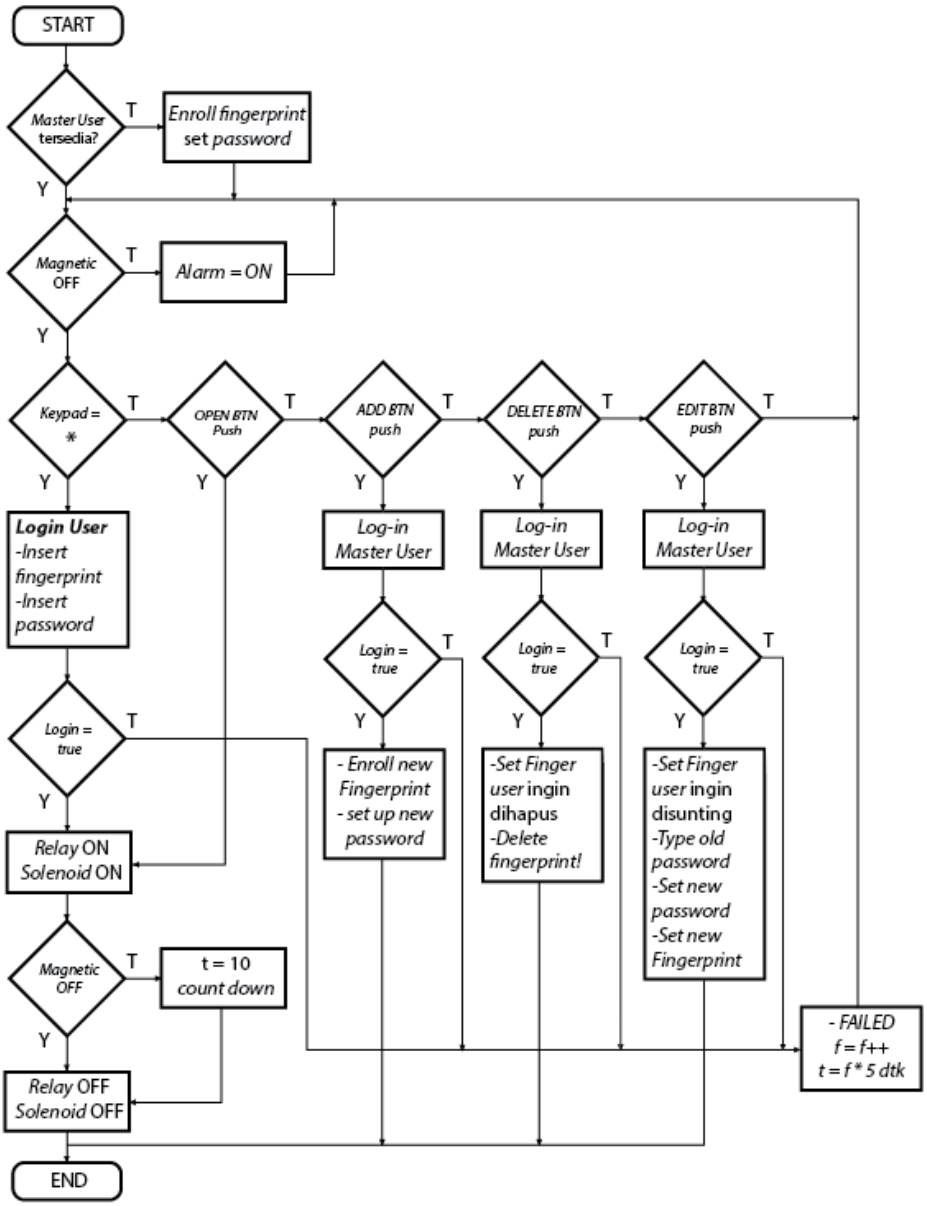
Perangkat keras dalam penelitian ini terdari dari beberapa komponen seperti yang disebutkan dalam alat dan bahan. Komponen tersebut dirangkai berdasarkan skema komponen, untuk lebih jelasnya skema komponen dapat dilihat pada gambar 2. Gambar 2 menunjukan rangkain komponen yang terhubung pada mikrokontroler Arduino Mega sebagai kontrol utama. Komponen tersebut dibagi menjadi beberapa bagian yaitu kompnen daya, pengaman pintu, mekanisme penguncian pintu, dan komponen keluaran. Komponen daya sebagai sumber tegangan utama berasal dari DC adaptor 12V 3A yang terhubung dengan PSU sebagai fitur tambahan *emergency backup supply* apabila sumber utama terputus. Sebelum digunakan tegangan utama akan melewati regulator yang berfungsi untuk menyesuaikan tegangan yang dibutuhkan masing-masing komponen. Komponen pengaman pintu terdiri *module fingerprint ZM-20*, *keypad*, *Bluetooth HC-05*, *magnetic switch*, dan *button.* Komponen mekanisme penguncian pintu terdiri atas *relay*, *buzzer*, dan *solenoid* sedangkan komponen keluaran (*output*) berupa LCD untuk menampilkan *user interface.*



Gambar 2. Skema Komponen

Perangkat lunak pada sistem keamanan *smart home* merupakan sebuah program dengan bahas pemprograman C++ yang di-*compile* melalui Arduino Sketch. Program tersebut bekerja berdasarkan diagram alur program pada gambar 3. Program tersebut akan memberikan akses terhadap pintu apabila proses autentifikasi berhasil dilakukan. Proses autentifikasi tersebut terdiri dari autentifikasi *biometric fingerprint* dan *password*. Program akan menolak akses terhadap pintu dan memberikan *delay* apabila terjadi kesalahan pada prosedur autentifikasi. *Delay* pada program akan bertambah lama ketika terjadi kesalahan secara berturut-turut. Program tersebut didesain agar memberikan peringatan apabila terjadi upaya akses terhadap pintu secara paksa. Program ini memiliki fitur untuk mengubah data pengguna yang tersimpan pada sistem keamanan.

Pengguna sistem keamanan *smart home* dibagi menjadi dua yaitu pengguna *master* dan pengguna biasa. Pengguna *master* merupakan pengguna yang didaftarkan pertama kali pada sistem keamanan. Pengguna master memiliki kewenangan umum berupa akses terhadap pintu dan kewenangan khusus untuk menambah pengguna, menghapus pengguna, dan menyunting pengguna. Pengguna biasa merupakan pengguna yang didaftarkan oleh pengguna *master*, pengguna biasa hanya memiliki kewenangan umum untuk mengakses pintu. Pengguna merupakan orang yang mengoperasikan sistem keamanan dan memperoleh manfaat dari sistem keamanan tersebut.



Gambar 3. Diagram Alur Program

3. HASIL DAN PEMBAHASAN

Hasil penelitian berupa sebuah sistem pengaman pintu menggunakan kombinasi metode *biometric fingerprint* dan *password*. Sistem pengaman ini diterapkan pada pintu yang terdapat di rumah. Sistem keamanan ini memiliki fitur tambahan berupa *emergency backup* dimana fitur ini bekerja ketika terjadi pemadaman listrik dan *emergency entry* ketika terjadi kerusakan pada panel luar. Fitur *emergency backup* ini bekerja dengan menggunakan baterai *rechargeable*. *Emergency entry* berkerja dengan menggunakan perintah dari *mobile device* yang terkoneksi *bluetooth* modul HC-05. Hasil perancangan sistem keamanan *smart home* dapat dilihat pada gambar 4.

Gambar 4. Hasil Perancangan Desain Alat

Sistem keamanan yang telah dibuat bekerja dengan mengautentifikasi dan membandingkan sidik jari dan *password* yang dimasukan melalui *module Fingerprint ZM-20* dan *keypad.* Akses terhadap pintu diberikan ketika sidik jari dan *password* yang dimasukan sesuai yang terdaftar pada EEPROM Arduino Mega. Ketika kombinasi sidik jari dan *password* yang dimasukan tidak sesuai maka sistem akan menolak akses terhadap pintu dan dilakukan hitung mundur sebelum dapat melakukan autentifikasi kembali, hitung mundur akan bertambah setiap kali pengguna memasukan kombinasi yang salah secara berturut-turut. *Alarm* akan berbunyi ketika terjadi pelanggaran terhadap akses rumah yang dideteksi oleh *magnetic switch* pada pintu. PSU akan bekerja ketika terjadi pemutusan aliran listrik dari sumber utama.

Uji ahli dilakukan dengan memberikan angket kepada para ahli dan pakar pada bidang sistem keamanan. Ahli mengisi angket dan memberikan saran maupun masukan dalam pengembangan sistem keamanan. Desain sistem keamanan dinyatakan baik ketika memperoleh persentase lebih dari 62,5%. Uji *black box* dilakukan dengan menguji tingkat fungsionalitas perangkat lunak dengan metode *task testing* dan *error trapping.* Hasil uji ahli dapat dilihat pada tabel 1.

Tabel 1. Tabulasi hasil uji ahli

	Aspek Kelayakan			
	Desain	***Penggunaan***	***Teknis***	***Keamanan***
Jumlah	18	20	32	27
Jumlah Maksimal	24	24	40	32
Persentase	75%	83,33%	80%	84,25%
Total Skor		97		
Total Persentase		80,83%		

Pada tabel 1 diketahui bahwa desain perancangan sistem keamanan mendapat skor 97 dengan persentase 80,83%, dengan demikian desain rancangan sistem dinyatakan lulus uji ahli. Dalam pengujian *black box* baik dengan metode *task testing* maupun *error trapping output* keluaran sistem sesuai dengan desain rancangan dan dinyatakan *valid*. Hasil uji *black box* dapat dilihat pada tabel 2.

Pengujian selanjutnya berupa uji pengguna, pengujian dilakukan dengan sampel penelitian 10 orang dengan kriteria umur lebih dari 12 tahun. Terdapat 3 aspek penilaian masing-masing aspek terdiri atas 5 pertanyaan dengan total 15 pertanyaan angket dan 5 pertanyaan esai tambahan. Berdasarkan data dapat diketahui jumlah skor yang diperoleh sebesar 506 dengan persentase 84,33%. Lebih lengkap hasil uji pengguna dapat dilihat pada tabel 3.

Tabel 2. Hasil uji *black box*

No	*Kelas Uji*	*Butir Uji*	*Hasil*
		Task Testing	
	Panel luar	Autentifikasi sidik jari	Valid
1		Entri *password*	Valid
		Akses pintu	Valid
	Panel dalam	Tambah *pengguna*	Valid
2		Hapus pengguna	Valid
		Sunting pengguna	Valid
3	Panel pintu	*Relock*	Valid
		Emergency Entry	Valid
		Error Trapping	
1	*Keypad*	Entri *password* salah	Valid
2	*Fingerprint*	Entri *fingerprint* salah	Valid
3	*Emergency switch*	Memutus aliran listrik	Valid
4	*Magnetic switch*	Membuka paksa pintu	Valid

Tabel 3. Tabulasi hasil uji pengguna

	Aspek Kelayakan		
	Tampilan Alat	***Kemudahan Pengoperasian***	***Fungsi Alat***
Jumlah	165	167	174
Jumlah Maksimal	200	200	200
Persentase	82,25%	83,5%	87%
Total Skor		506	
Total Persentase		84,33%	

Sistem keamanan yang dibuat menggunakan ATmega 2560 sebagai pusat kontrol. Modul *fingerprint* yang digunakan memiliki *False Acceptance Rate* (FAR) kurang dari 0,001% (*security level* 3) dan *False Reject Rate* (FRR) kurang dari 1,0% (security level 3) serta *fingerprint imaging time* kurang dari 1 detik [13]. Dengan demikian penggunaan modul *fingerprint* Adafruit ZM-20 sudah memenuhi syarat *performace* sebagai metode sistem keamanan rumah.

Biometric fingerprint bila dibandingkan dengan metode *biometric* lain memperoleh nilai yang tinggi pada aspek *ease of use*, *accuracy*, *security*, dan *performance* [3]–[5]. Berdasarkan hasil perbandingan tersebut metode *biometric* yang digunakan pada penelitian ini berupa metode *biometric fingerprint*. Penelitian [6] dan [7] menggunakan modul GSM untuk mengirimkan pesan peringatan kesalahan ataupun kombinasi PIN/*Password* untuk mengakses pintu. Pengoperasian modul GSM membutuhkan biaya tambahan berupa pulsa untuk menggunakan jasa provider GSM, sedangkan pada penelitian ini *password* tidak dikirimkan melalui modul GSM namun *password* yang digunakan menyesuaikan dengan *fingerprint* yang didaftarkan. Hal ini menjadikan sistem keamanan *smart home* memiliki kecepatan akses yang lebih baik karena tidak perlu menunggu pesan yang berisikan *password* dan tidak adanya biaya tambahan dalam pengoperasian layaknya penggunaan modul GSM. Waktu yang dibutuhkan untuk mengakses pintu pada penelitian [8] bergantung kepada kecepatan *authorize* oleh pengguna *mobile device* sedangkan pada penelitian ini akses terhadap pintu diberikan sesaat setelah proses autentifikasi selesai tanpa menunggu *authorize* dari pengguna *master*. Tanpa adanya proses *authorize* maka efektifitas kerja sistem keamanan lebih cepat karena akses terhadap pintu diberikan hampir tanpa jeda setelah pengguna berhasil terautentifikasi oleh sistem keamanan. Penelitian [9] menggunakan memori penyimpanan EEPROM pada modul mikrokontroler sebagai *data logger* sedangkan pada penelitian ini digunakan untuk menyimpan *password* yang telah didaftarkan. *Password* tersebut telah terintegrasi sesuai dengan sidik jari yang telah didaftarkan. Hal ini memungkinkan pengguna mendaftarkan *password* sesuai dengan preferensi masing-masing, dengan demikian metode *password* pada sistem keamanan *smart home* tidak dapat ditebak dengan mudah karena berbeda-beda pada setiap pengguna yang mendorong meningkatnya performa metode *password*. Berdasarkan uraian tersebut, sistem keamanan *smart home* yang diusulkan memiliki keunggulan pada kecepatan akses pintu, performa *password*, dan bebas biaya tambahan.

Selain keunggulan tersebut sistem keamanan *smart home* yang diusulkan juga memiliki fitur tambahan berupa *emergency backup supply* dan *emergency entry*. *Emergency backup supply* memungkinkan pengguna tetap dapat mengakses pintu ketika terjadi gangguan *supply* dari sumber utama (PLN). *Emergency entry* memungkinkan akses terhadap pintu dapat dilakukan ketika terjadi kerusakan

pada panel luar dengan menghubungkan *smartphone* yang telah terinstal aplikasi mengunakan koneksi *bluetooth* yang telah tersedia dalam *smart home security system* berbasis mikrokontroler.

4. KESIMPULAN

Sistem keamanan *smart home* yang diusulkan mengkombinasikan dua metode yaitu *biometric fingerprint* dan *password* sebagai metode keamanan akses terhadap pintu. Sistem bekerja dengan menggunakan modul Arduino Mega dengan IC 2560 sebagai sistem kontrol. Mekanisme penguncian pintu menggunakan *solenoid door lock.* Sistem keamanan *smart home* memiliki fitur tambahan berupa sistem pengaman dengan *magnetic switch, emergency backup supply,* dan *emergency entry* dengan modul bluetooth HC-05. Kinerja dari sistem keamanan *smart home* telah melalui proses pengujian seperti uji *black box* setiap komponen mampu bekerja sesuai desain perangkat lunak yang telah direncanakan, uji ahli berhasil mendapat skor 80,83% dengan kategori "baik",dan uji pengguna mendapat skor 84,33% dengan kategori "sangat baik". Berdasarkan hasil tersebut sistem keamanan *smart home* dapat dikatakan layak digunakan sebagai sistem keamanan di rumah tangga.

DAFTAR PUSTAKA

[1] BPS, *Statistik Kriminal 2017*. Jakarta-Indonesia: Badan Pusat Statistika, 2017.
[2] C. Lee, L. Zappaterra, K. Choi, and H. Choi, "Securing Smart Home : Technologies , Security Challenges , and Security Requirements," *Work. Secur. Priv. Mach. Commun.*, pp. 67–72, 2014.
[3] S. Liu and M. Silverman, "A Practical Guide to Biometric Security Technology," pp. 27–32, 2001.
[4] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, 2004.
[5] M. Faundez-zanuy, "Biometric Security Technology," *IEEE A&E Syst. Mag.*, vol. 21, no. 6, pp. 15–26, 2006.
[6] R. Hasan, M. M. Khan, and A. Ashek, "Microcontroller Based Home Security System with GSM Technology," *Open J. Saf. Sci. Technol.*, vol. 5, no. June, pp. 55–62, 2015.
[7] M. Gayathri, P. Selvakumari, and R. Brindha, "Fingerprint and GSM based security system," *Int. J. Eng. Sci. Res. Technol.*, vol. 3, no. 4, pp. 4024–4029, 2014.
[8] S. Rajadurai, P. P. Nehru, and R. Selvarasu, "Android mobile based home security and device control using GSM," *ICIIECS 2015 - 2015 IEEE Int. Conf. Innov. Information, Embed. Commun. Syst.*, 2015.
[9] S. Ardhi and Savitri, "Perencanaan dan Pembuatan Sistem Pengaman Rumah dengan Teknologi Pengenal Sidik Jari," *Konf. Nas. "Inovasi dalam Desain dan Teknol.*, pp. 398–406, 2011.
[10] J. Andriana and B. E. Purnama, "Pembuatan Animasi Film Kartun dengan Komputer Multimedia," *J. Speed - Sentra Penelit. Eng. dan Edukasi*, vol. 1, no. 3, pp. 11–19, 2009.
[11] D. D. R. Rahadi, "Peranan teknologi informasi dalam peningkatan pelayanan di sektor publik," *Semin. Nas. Teknol. 2007 (SNT 2007)*, vol. 2007, no. November, pp. 1–13, 2007.
[12] R. Sidh, "Peranan Brainware Dalam Sistem Informasi Manajemen," *J. Comput. Bisnis*, vol. 7, no. 1, pp. 19 – 29, 2013.
[13] Ladyada, "Adafruit Optical Fingerprint Sensor," *Adafruit.com*, p. 25, 2014.