Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN: 2548-964X
Vol. 3, No. 10, Oktober 2019, hlm. 9386-9394 http://j-ptiik.ub.ac.id

Implementasi Wireless Sensor Network pada Sistem Keamanan Rumah menggunakan Sensor PIR dan *Fingerprint*

Crisandolin Desman Rumahorbo[1], Mochammad Hannats Hanafi Ichsan[2], Agung Setia Budi[3]

Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]crisandolin007@gmail.com, [2]hanas.hanafi@ub.ac.id, [3]agungsetiabudi@ub.ac.id

Abstrak

Dewasa ini keamanan rumah saat ditinggalkan oleh pemiliknya menjadi salah satu masalah yang serius. Mekanisme keamanan pintu berbasis RFID atau kata sandi dapat dengan mudah dimanipulasi ketika kartu RFID atau kata sandi dibagikan atau dicuri, sehingga diperlukan sistem keamanan berbasis biometrik. *Monitoring* kondisi ruangan yang luas pada pengimplementasiannya memiliki kelemahan yaitu mekanisme *single-hop*. Mekanisme yang digunakan untuk menjangkau area yang lebih luas adalah mekanisme *multi-hop.* Berdasarkan kebutuhan akan keamanan dan pemantauan rumah dari jarak yang jauh diperlukan sistem yang menggunakan *fingerprint* sebagai orisinalitas pemilik, sensor PIR sebagai pemantau dan mekanisme *multi-hop* untuk menjangkau area luas yang terhubung dengan internet yang dapat diakses dengan *smartphone* sehingga keadaan rumah dapat diakses dimana saja. Hasil pengujian *single-hop* dengan 100 percobaan pengiriman data tanpa penghalang jarak 3-15 meter memiliki *packet loss* 0%, 18-20 meter 2%, 22-25 meter 5%, 28-33 meter 8%, 38 meter 9%, 45 meter 47%, 50 meter 98% dengan total rata-rata *delay* sebesar 46.1 ms. *Single-hop* dengan penghalang jarak 3-12 meter memiliki *packet loss* 0%, 15 meter 12%, 18 meter 25%, 20 meter 58%, 22 meter 99%, dengan total rata-rata *delay* sebesar 38.1 ms. Hasil pengujian mekanisme *multi-hop* dengan 100 percobaan pengiriman data 1 *hop* dengan penghalang jarak 3-12 meter memiliki *packet loss* 0%, 15 meter 19%, 18 meter 53%, 20 meter 98%, dengan total rata-rata *delay* sebesar 118.31 ms. *Multi-hop* dengan 2 *hop* dengan penghalang jarak 3-9 meter memiliki *packet loss* 0%, 12 meter 8%, 15 meter 54%, 18 meter 74%, dengan total rata-rata *delay* sebesar 105.13 ms.

Kata kunci: *Fingerprint, PIR, Multi-hop, Smartphone, Keamanan Rumah*

Abstract

Today home security is left behind by its owner to be one serious problem. The security mechanisms of the RFID or password-based doors can be easily manipulated when the RFID card or password is shared or stolen, so a biometric based security system is required. Monitoring The wide space of the condition in its implementation has a weakness that is single-hop mechanism. The mechanism used to reach a wider area is a multi-hop mechanism. Based on the need for security and home monitoring from a far distance required system that uses fingerprints as the originality of the owner, PIR sensors as monitors and implements multi-hop to reach a wide area that Connected to the Internet that can be accessed by smartphone so the state of the house can be accessed anywhere. The results of single-hop testing with 100 tests of data delivery without a barrier distance of 3-15 meters has a packet loss 0%, 18-20 meters 2%, 22-25 meters 5%, 28-33 meters 8%, 38 meters 9%, 45 meters 47%, 50 meters 98% with an average total delay of 46.1 ms. Single-hop 3-12 meters distance barrier has 0% packet loss, 15 meters 12%, 18 meters 25%, 20 meters 58%, 22 meters 99%, with a total average delay of 38.1 ms. Multi-hop mechanism test results with 100 data delivery test with 1 hop distance barrier 3-12 meters have a packet loss 0%, 15 meters 19%, 18 meters 53%, 20 meters 98%, with a total average delay of 118.31 ms. Multi-hop with 2 hops with a barrier of 3-9 meters distance has a packet loss 0%, 12 meters 8%, 15 meters 54%, 18 meters 74%, with an average total delay of 105.13 ms.

Keywords: *Fingerprint, PIR, Multi-Hop, Smartphone, home security*

1. PENDAHULUAN

Dewasa ini keamanan rumah saat ditinggalkan oleh pemiliknya menjadi salah satu masalah yang serius. Jenis kriminal yang paling besar setiap tahunnya adalah kejadian kejahatan kriminal tapi tanpa adanya kekerasan.

Upaya seperti menggunakan jasa seseorang untuk mengamankan rumah digunakan untuk mengatasi masalah ini, tetapi upaya tersebut kurang efektif selain biaya yang besar, pemilik rumah juga tidak dapat memberikan keamanan rumahnya atau barang berharganya kepada orang lain begitu saja (Badya,et.al, 2017). Mekanisme keamanan pintu berbasis RFID atau kata sandi dapat dengan mudah dimanipulasi ketika kartu RFID atau kata sandi dibagikan atau dicuri, sehingga diperlukan sistem keamanan berbasis biometrik (Badya,et.al, 2017).

Salah satu keamanan berbasis biometrik adalah keamanan dengan menggunakan *fingerprint*. Sampai saat ini, ada banyak penelitian yang telah dilakukan berbasis *fingerprint* untuk mengamankan rumah. Afolabi dan Alice (2014) mengusulkan desain sistem keamanan sistem dengan menggunakan sensor *Fingerprint* SN_FOR_UART dan mikrokontroler PIC16F648A untuk membuka pintu dengan menggunakan motor. Tobing (2014) membuat sistem keamanan *fingerprint* yang hampir sama penelitian yang dilakukan Afolabi dan Alice, tetapi menggunakan *smartphone* sebagai *user interface*. Siswanto (2016) membuat sistem keamanan *fingerprint* dengan menggunakan *fingerprint sensors*, sebuah mikrokontroler, Wireless Network Router, sebuah server, koneksi dengan internet, dan dikontrol oleh *smartphone*. Morsalin (2016) membuat sistem keamanan dengan tiga proteksi, dimulai dari NFC Tag, *password* menggunakan Keypad, dan *fingerprint* untuk membuka pintu yang dengan aktuator Servo. Baidya (2017) membuat sistem keamanan *fingerprint* yang hampir sama dengan sebelumnya, peneliti membuat sistem *fingerprint* pada *doorlock* dengan *elektronic lock*.

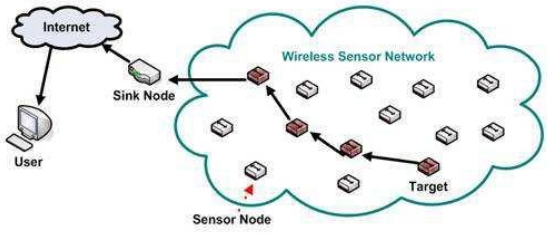
Berdasarkan kebutuhan akan keamanan dan pemantauan rumah dari jarak yang jauh diperlukan sistem yang akan dikembang dalam skripsi ini. Pada penelitian ini, peneliti akan merancang sistem dengan menggunakan *fingerprint* sebagai orisinalitas pemilik dan sensor PIR sebagai pemantau yang terhubung dengan internet yang dapat diakses dengan *smartphone* sehingga keadaan rumah dapat diakses dimana saja. Untuk menjangkau area yang lebih luas, peneliti mengimplementasikan *multi-hop* pada *Wireless Sensor Network* karena mengurangi penggunaan energi (Ergen,et.al, 2005) dan lebih murah dibanding dengan penggunaan CCTV.

2. DASAR TEORI

Terdapat beberapa teori yang menopang penyusunan penelitian berupa arti, cara kerja produk, dan spesifikasi sehingga memudahkan pembaca memahami isi penelitian.

2.1 W*ireless Sensor Network*

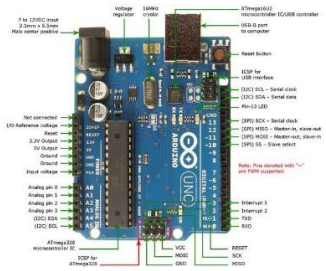
Wireless sensor network adalah jaringan yang bertanggung jawab untuk mengumpulkan, memproses dan mendistribusikan data *wireless* ke *database* penyimpanan yang terpusat (Pinar,et.al,2016). WSN dibangun dari beberapa *node* yang terdiri dari *transceiver radio*, mikrokontroler dan sensor. Aplikasi WSN dapat diklasifikasi menjadi dua kategori yaitu monitoring dan *tracking*. Monitoring termasuk lingkungan *indoor* atau *outdoor*. Sedangkan *tracking* termasuk pelacakan benda mati maupun benda hidup (Zhang,et.al, 2012). Fitur utama dari WSN adalah dapat mengatur diri sendiri, *rute multi-hop*, topologi jaringan yang dinamis, sumber *node* yang tidak terbatas, data sentris dan masalah keamanan.



Gambar 1. Gambar Wireless Sensor Network

2.2 Arduino Uno

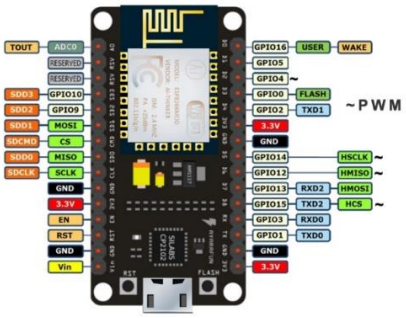
Arduino Uno adalah sebuah mikrokontroler yang berbasis pada ATmega328. Arduino Uno terdiri dari 14 pin sebagai *input* atau *output* dan 6 diantaranya dapat digunakan sebagai pin PWM, 6 pin analog *input*, 16MHz *ceramic resonator*, USB untuk konektitivitas, sebuah *power jack*, sebuah ICSP *header* dan tombol reset.



Gambar 2. Arduino Uno

2.3 *Node*MCU

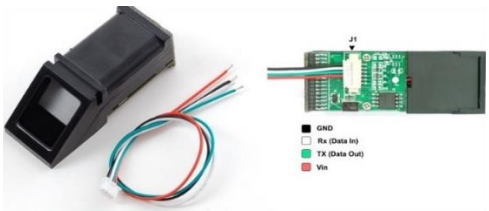
*Node*MCU adalah *sebuah firmware open-source* dan *kit development* yang digunakan untuk membantu membangun produk IoT atau *Internet of Things*. *Node*MCU dikembangkan untuk mempermudah pengguna API lanjutan untuk perangkat keras IO. API dapat mengurangi kerja yang berlebihan pada konfigurasi dan manipulasi *hardware*.



Gambar 3 *Node*MCU

2.4 Fingerprint FPM10A

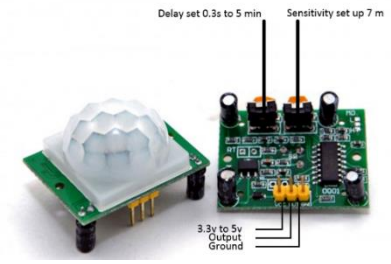
Fingerprint sensor menggunakan optik untuk menangkap data sidik jari dan melakukan verifikasi dengan simpel. Modul ini merupakan tipe yang dipakai untuk keamanan, pada module ini terdapat DSP bertenaga tinggi yang bertujuan untuk melakukan rendering gambar, perhitungan, pencarian fitur dan pencarian data sidik jari yang tersimpan. Pada modul ini dapat menambahkan sidik jari sampai 162 buah yang tersimpan pada memori Flash (Adafruit, 2019).



Gambar 4. FPM10A

2.5 Passive Infrared (PIR)

Passive Infrared (PIR) sensor terbuat dari lapisan Pyroelectric yang dapat mendeteksi tingkat radiasi *infrared*. Sensor akan tetap pada kondisi *idle* apabila sensor menerima jumlah infrared yang sama. Namun, ketika ada bagian yang hangat seperti manusia atau seekor binatang melewati wilayah sensor menyebabkan perubahan difrensial positif pada kedua bagian. Ketika bagian hangat tersebut meninggalkan area sensor, sebaliknya akan terjadi perubahan diferensial negatif.



Gambar 5. Sensor PIR

2.6 NRF24L01

NRF24L01 adalah sebuah *chip* tunggal dengan 2.4GHz *transceiver* yang didesain untuk pengaplikasian daya *ultralow*. nRF24l01 memiliki empat mode operasi. Kecepatan maksimum data rate dari nRF24L01 adalah 2Mbps. Fungsi pin pada nRF24L01 adalah sebagai berikut:

- CE untuk mengaktifkan transmisi atau penerimaan,
- CSN, SCK, MOSI, MISO untuk pin SPI, digunakan untuk konfigurasi dan operasi melalui pin SPI;
- IRQ adalah interupsi yang digunakan untuk memberi tahu mikrokontroler apakah modul berhasil dikirim atau diterima (Wang,et.al, 2014).

Gambar 6. NRF24L01

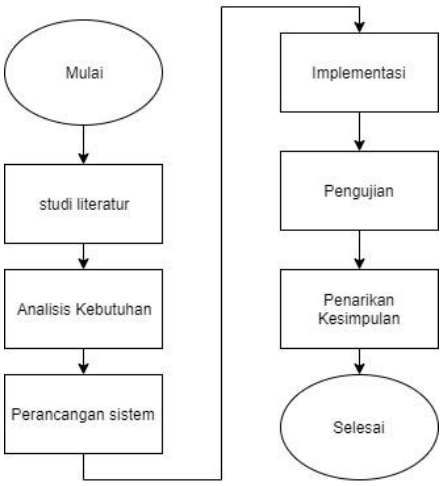
2.7 Realtime Firebase

Firebase adalah salah satu database Nosql.

NoSQL tidak menggunakan hubungan tabular sehingga memungkinkan perubahan nilai yang sering. Database NoSQL melihat skema dinamis, yang berarti bahwa struktur basis data dapat diubah tanpa skema yang telah ditentukan. Firebase merupakan database yang host-nya berada di cloud. Data yang tersimpan pada database, berbentuk JSON dan tersinkronisasi secara realtime pada setiap device yang terhubung.

3. METODOLOGI PENELITIAN

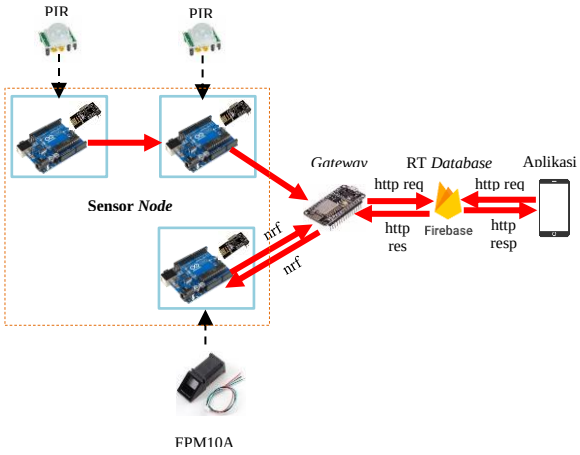
Metode penelitian digunakan untuk menjelaskan langkah-langkah yang diambil dalam pelaksanaan penelitian. Penelitian ini bertipe penelitian implementatif, sedangkan pendekatan yang dipakai adalah pengembangan. Sehingga penelitian ini menerapkan prinsip-prinsip seperti gambar berikut:



Gambar 7. Alur Metode Penelitian

4. GAMBARAN UMUM SISTEM

Monitoring rumah saat keadaan kosong adalah sistem yang akan dibuat pada penelitian ini dengan mengimplementasikan *multi-hop* pada Wireless Sensor Network. Penelitian ini menggunakan dua jenis modul komunikasi yaitu NRF24L01 sebagai komunikasi antara *node* dengan *gateway* dan ESP8266 sebagai komunikasi antara *gateway* dengan *real time database*. Sensor *node* yang digunakan adalah sebanyak tiga *node*, dua *node* yang terpasang sensor PIR dan satu *node* yang terpasang FPM10A. Data sensor yang diterima akan diproses oleh mikrontroler Arduino Uno. Data yang telah diolah akan dikirim menuju *gateway* dengan menggunakan modul komunikasi NRF24L01. Data yang diterima oleh *gateway* akan diteruskan menuju real time *database* menggunakan modul komunikasi ESP8266. Perancangan arsitektur sistem terdapat pada Gambar 8.

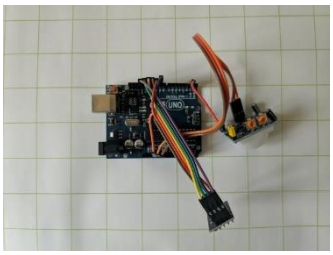


Gambar 8. Gambaran Umum

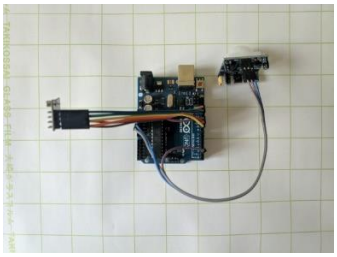
5. IMPLEMENTASI

Implementasi perangkat keras dan implementasi perangkat lunak akan ditampilkan pada bagian ini.

5.1 Implementasi *Node* Sensor PIR *Multi-hop* dan *Node* Sensor PIR



Gambar 9 *Node* Sensor PIR *Multi-hop*



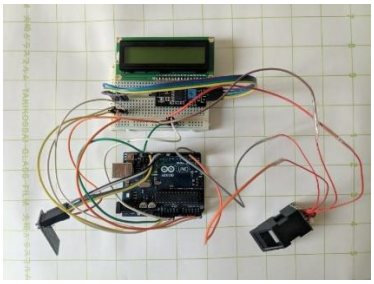
Gambar 10 *Node* Sensor PIR

Node sensor PIR *Multi-hop* dan *node* sensor menggunakan mikrokontroler Arduino, sebuah modul komunikasi NRF24L01 dan sebuah sensor PIR. Setelah semua komponen yang tersedia dihubungkan sesuai dengan

perancangan yang sudah ditentukan sebelumnya maka hasil dari rancangan *node* sensor dapat dilihat pada Gambar 9 dan Gambar 10.

5.2 Implementasi *Node* Sensor FPM10A

Node sensor FPM10 menggunakan mikrokontroler Arduino Uno, sebuah modul komunikasi NRF24L01, menggunakan LCD 16x2 yang terhubung dengan modul I2C dan sensor FPM10A. Setelah semua komponen yang diperlukan dihubungkan sesuai dengan perancangan yang sudah ditentukan sebelumnya, maka hasil dari rancangan *node* sensor dapat dilihat pada Gambar 11.



Gambar 11 *Node* Sensor FPM10A

5.3 Implementasi Gateway

Gateway menggunakan mikrokontroler *Node*MCU yang dilengkapi dengan modul komunikasi ESP822 dan sebuah modul komunikasi NRF24L01 yang digunakan untuk berkomunikasi dengan *node* sensor. Setelah semua komponen yang diperlukan dihubungkan sesuai dengan perancangan yang sudah ditentukan sebelumnya, maka hasil dari rancangan *gateway* dapat dilihat pada Gambar 12.

Gambar 12 Gateway

6. PENGUJIAN

Pengujian bertujuan untuk memastikan dan menguji sistem sehingga sesuai dengan kebutuhan. Pengujian yang dilakukan adalah pengujian fungsionalitas dan pengujian kinerja sistem.

6.1 Pengujian Fungsional

Menguji kebutuhan fungsional adalah tujuan utama pada pengujian ini, yang sudah didefenisikan. Pengujian fungsional dilakukan setelah perancangan dan implementasi dilakukan sehingga pengujiaannya menjadi akurat.

Tabel 1 Hasil Pengujian Fungsional

Kode Uji	Hasil Harapan	Hasil Pengujian	Kesimpulan
SF-01	Dapat menerima data sensor yang berasal dari sensor PIR oleh sensor *node*	Dapat menerima data sensor yang berasal dari sensor PIR oleh sensor *node*	valid
SF-02	Dapat menerima data sensor yang berasal dari sensor FPM10A oleh sensor *node*	Dapat menerima data sensor yang berasal dari sensor FPM10A oleh sensor *node*	valid
SF-03	Dapat mengirim data sensor yang didapat menuju *gateway* menggunakan modul NRF24L01 oleh *node* PIR	Dapat mengirim data sensor yang didapat menuju *gateway* menggunakan modul NRF24L01 oleh *node* PIR	valid
SF-04	Dapat mengirim data sensor yang didapat ke *gateway* dengan modul NRF24L01 oleh *node* FPM10A	Dapat mengirim data sensor yang didapat ke *gateway* dengan modul NRF24L01 oleh *node* FPM10A	valid
SF-05	Dapat melakukan mekanisme *multi-hop* untuk meneruskan data sensor menuju *gateway oleh node* PIR *multi-hop*	Dapat melakukan mekanisme *multi-hop* untuk meneruskan data sensor menuju *gateway oleh node* PIR *multi-hop*	valid
SF-06	Dapat mendapat data dan melanjutkan	Dapat mendapat data dan melanjutkan data dari sensor	valid

	data dari sensor *node* ke *database* oleh *gateway*	*node* ke *database* oleh *gateway*	
SF-07	*Gateway* mampu melakukan *get* data dari *database* dan meneruskan sensor *node* FPM10A	*Gateway* mampu melakukan *get* data dari *database* dan meneruskan sensor *node* FPM10A	valid
SF-08	Aplikasi Android dapat menampilkan data sensor yang didapat dari *database*	Aplikasi Android dapat menampilkan data sensor yang didapat dari *database*	valid
SF-09	Aplikasi Android dapat melakukan *push notification* saat keadaan rumah sedang tidak aman	Aplikasi Android dapat melakukan *push notification* saat keadaan rumah sedang tidak aman	valid
SF-10	Admin mampu menambahkan penghuni rumah melalui Aplikasi Android	Admin mampu menambahkan penghuni rumah melalui Aplikasi Android	valid

6.2 Pengujian Kinerja

Pengujian kinerja akan menghitung *packet loss* dan RTD pengiriman data dengan menggunakan parameter jarak antar *node* dan penghalang antar *node* dengan jarak yang ditentukan.

6.2.1 Pengujian *Single-hop* tanpa Penghalang

Pengujian ini dilakukan dengan melakukan mekanisme *single-hop* tanpa ada penghalang antar kedua *node*. Sistem dapat melakukan mekanisme *single-hop* dengan *packet loss* bernilai 0 mulai dari jarak 3 meter sampai pada jarak 15 meter. Sedangkan sistem tidak dapat lagi menerima data pada jarak 55 meter.

Tabel 2 Hasil Pengujian *Single-hop* dengan Penghalang

Jarak *Node* 1-*Node* 2	Packet loss	RTD Average
3 meter	0%	2 ms
6 meter	0%	2.05 ms
9 meter	0%	2.13 ms
12 meter	0%	2.09 ms
15 meter	0%	2.1 ms
18 meter	2%	2.2 ms
20 meter	2%	2.2 ms
22 meter	5%	2.5 ms
25 meter	5%	2.3 ms
28 meter	8%	2.7 ms
33 meter	8%	2.08 ms
38 meter	9%	2.3 ms
45 meter	47%	5.95 ms
50 meter	98%	13.5 ms
55 meter	100%	0 ms
60 meter	100%	0 ms

6.2.2 Pengujian *Single-hop* dengan Penghalang

Pengujian ini dilakukan dengan melakukan mekanisme *single-hop* dengan penghalang antar kedua *node.* Sistem dapat melakukan mekanisme *single-hop* dengan *packet loss* bernilai 0 mulai dari jarak 3 meter sampai pada jarak 12 meter. Sedangkan sistem tidak dapat lagi menerima data pada jarak 25 meter.

Tabel 3 Hasil Pengujian *Single-hop* dengan Penghalang

Jarak *Node* 1-*Node* 2	Packet loss	RTD Average
3 meter	0%	2 ms
6 meter	0%	2.01 ms
9 meter	0%	2.4 ms
12 meter	0%	2.4 ms
15 meter	12%	2.5 ms
18 meter	25%	2.7 ms
20 meter	58%	6.2 ms
22 meter	99%	18 ms
25 meter	100%	0 ms
28 meter	100%	0 ms

6.2.3 Pengujian *Multi-hop* 1 Penghalang

Pengujian ini dilakukan dengan melakukan mekanisme *multi-hop* dengan penghalang antara *Node* 2 dengan *Node* 3, sedangkan *Node* 1 dengan *Node* 2 tidak terdapat penghalang. Jarak yang digunakan untuk jarak antara *Node* 1 dan *Node* 2 adalah 15 meter. Jarak ini dipilih dikarenakan pada pengujian *single-hop* tanpa penghalang, jarak 15 meter menjadi jarak maksimal sistem untuk dapat menerima data dengan *packet loss* 0%. Jarak maksimal ini dipilih untuk menghitung jarak maksimal sistem untuk melakukan mekanisme *multi-hop*. Sistem dapat melakukan mekanisme *multi-hop* dengan *packet loss* bernilai 0 mulai dari jarak 3 meter sampai pada jarak 12 meter. Sedangkan sistem tidak dapat lagi menerima data pada jarak 22

meter.

Tabel 4 Hasil Pengujian *Multi-hop* dengan *Node*1-*Node*2 terdapat Penghalang

Jarak *Node* 1-*Node* 2	Jarak *Node* 2-*Node* 3	Packet loss	RTD Average
15 meter	3 meter	0%	10.61 ms
	6 meter	0%	11.52 ms
	9 meter	0%	11.83 ms
	12 meter	0%	12.01 ms
	15 meter	19%	13.74 ms
	18 meter	53%	26.1 ms
	20 meter	98%	32.5 ms
	22 meter	100%	0 ms
	25 meter	100%	0 ms

6.2.4 Pengujian *Multi-hop* 2 Penghalang

Pengujian ini dilakukan dengan melakukan mekanisme *multi-hop* dengan penghalang antara *Node* 1 dengan *Node* 2 dan *Node* 2 dengan *Node* 3. Jarak yang digunakan untuk jarak antara *Node* 1 dan *Node* 2 adalah 15 meter. Jarak ini dipilih dikarenakan pada pengujian *single-hop* tanpa penghalang, jarak 12 meter menjadi jarak maksimal sistem untuk dapat menerima data dengan *packet loss* 0%. Jarak maksimal ini dipilih untuk menghitung jarak maksimal sistem untuk melakukan mekanisme *multi-hop*. Sistem dapat melakukan mekanisme *multi-hop* dengan *packet loss* bernilai 0 mulai dari jarak 3 meter sampai pada jarak 9 meter. Sedangkan sistem tidak dapat lagi menerima data pada jarak 20 meter.

Tabel 5 Hasil Pengujian *Multi-hop* dengan *Node*1-*Node*2-*Node*3 terdapat Penghalang

Jarak *Node* 1-*Node* 2	Jarak *Node* 2-*Node* 3	Packet loss	RTD Average
12 meter	3 meter	0%	10.56 ms
	6 meter	0%	11.62 ms
	9 meter	0%	12.54 ms
	12 meter	8%	13.19 ms
	15 meter	54%	26.1 ms
	18 meter	74%	31.12 ms
	20 meter	100%	0 ms
	22 meter	100%	0 ms
	25 meter	100%	0 ms

7. KESIMPULAN DAN SARAN

Bab Kesimpulan dan saran adalah bab terakhir pada penelitian ini yang akan menjelaskan kesimpulan atau jawaban yang merujuk pada rumusan masalah yang ditetapkan sebelumnya dan menjelaskan saran bagi pengembang sistem berikutnya.

7.1 Kesimpulan

Berdasarkan implementasi dan pengujian yang dilaksanakan sebelumnya pada penelitian ini, hasilnya dapat menjawab rumusan masalah yang disimpulkan menjadi beberapa kesimpulan, seperti dibawah ini.

1. Sensor *Node* terdiri atas sensor, mikrokontroler, dan modul komunikasi NRF24L01. Sensor yang digunakan adalah sensor Passive Infrared (PIR) bertujuan untuk menangkap gerakan di dalam rumah. Data yang didapat akan diproses oleh mikrokontroler Arduino Uno untuk dikirimkan ke *gateway* melalui NRF24L01. *Gateway* adalah perangkat yang memiliki fungsi menghubungkan sensor *node* dengan *database*. *Gateway* akan menerima data sensor yang dikirim oleh sensor dan mengirim ke *database*. Salah satu sensor *node* tidak terhubung langsung dengan *gateway*, melainkan terhubung dengan sensor *node* yang lain. Sistem akan menerapkan mekanisme *multi-hop*e sehingga sensor *node* yang tidak terhubung langsung dengan *gateway* dapat mengirim data ke *gateway*. *Database* pada penelitian ini adalah Realtime *Database* Firebase dan menggunakan HTTP sebagai protokol yang bertanggung jawab untuk melakukan request dan response oleh pengguna melalui Android API. Android API digunakan sebagai interface pengguna dengan pengguna. Fitur yang diterapkan adalah keadaan rumah saat ini, penghuni yang sedang di rumah, dan menambahkan penghuni rumah. Android akan melakukan *push notification* apabila rumah pengguna sedang tidak aman.
2. Pada pengujian *single-hop*, terbagi atas *single-hop* tanpa penghalang dan *single-hop* dengan penghalang. Dari hasil pengujian tersebut didapat *packet loss* dan Round Time *Delay* didapat sebagai berikut:
   - Tanpa penghalang jarak 3-15 meter memiliki *packet loss* 0%, jarak 18-20 meter memiliki *packet loss* 2%, jarak 22-25 meter memiliki *packet loss* 5%, jarak 28-33 meter memiliki *packet loss* 8%, jarak 38 meter dengan *packet loss* 9%, jarak 45 meter dengan *packet loss* 47%, jarak 50 meter dengan *packet loss* 98% dengan total rata-rata *delay* sebesar 46.1 ms.

- Dengan penghalang jarak 3-12 meter memiliki *packet loss* 0%, jarak 15 meter memiliki *packet loss* 12%, jarak 18 meter memiliki *packet loss* 25%, jarak 20 meter memiliki *packet loss* 58%, jarak 22 meter dengan *packet loss* 99%, dengan total rata-rata *delay* sebesar 38.1 ms.

3. Pada pengujian *multi-hop*, terbagi atas *multi-hop* dengan 1 penghalang dan *multi-hop* dengan 2 penghalang. Dari hasil pengujian tersebut didapat *packet loss* dan Round Time *Delay* didapat sebagai berikut:
   - *Multi-hop* dengan 1 penghalang jarak 3-12 meter memiliki *packet loss* 0%, jarak 15 meter memiliki *packet loss* 19%, jarak 18 meter memiliki *packet loss* 53%, jarak 20 meter memiliki *packet loss* 98%, dengan total rata-rata *delay* sebesar 118.31 ms
   - *Multi-hop* dengan 2 penghalang jarak 3-9 meter memiliki *packet loss* 0%, jarak 12 meter memiliki *packet loss* 8%, jarak 15 meter memiliki *packet loss* 54%, jarak 18 meter memiliki *packet loss* 74%, dengan total rata-rata *delay* sebesar 105.13 ms

7.2 Saran

Berdasarkan kesimpulan yang telah dirangkum, terdapat beberapa hal yang perlu dikembangkan pada penelitian berikutnya. Adapun saran dari peneliti untuk penelitian berikutnya adalah sebagai berikut.

1. Sensor *node* pemantau yang digunakan pada penelitian ini adalah satu buah. Diharapkan pada penelitian berikutnya ditambah dengan beberapa *node* pemantau agar semua sudut rumah terjangkau.
2. Pada penelitian, tidak terdapat mekanisme membuka rumah dengan motor atau aktuator. Diharapkan penelitian berikutnya dapat menggunakan motor sebagai pelengkap sistem.

8. DAFTAR PUSTAKA

Adafruit, 2019. *Fingerprint Sensor*. [online] Tersedia di: <https://www.adafruit.com/product/751> [Diakses 20 Agustus 2019]

Afolabi, A., Alice, O., 2014. On Securing a Door with Finger Print Biometrik Technique. *Transactions on Machine Learning and Artificial Intelligence*, 2(2), pp.86-96.

Arduino, 2019. *Arduino Uno SMD*. [online] Tersedia di : < https://www.arduino.cc/en/Main/ArduinoBoardUnoSMD > [Diakses 20 Agustus 2019]

Badan Pusat Statistik, 2018. *Statistik Kriminal 2018*. [online] Badan Pusat Statistik. Tersedia di : <https://www.bps.go.id/publication/download.html?nrbvfeve=ODljMDZmNDY1Zjk0NGYzYmUzOTAwNmEx&xzmn=aHR0cHM6Ly93d3cuYnBzLmdvLmlkL3B1YmxpY2F0aW9uLzIwMTgvMTIvMjYvODljMDZmNDY1Zjk0NGYzYmUzOTAwNmExL3N0YXRpc3Rpay1rcmltaW5hbC0yMDE4Lmh0bWw%3D&twoadfnoarfeauf=MjAxOS0wOC0xOSAxNjo0Njo0NA%3D%3D> [Diakses 19 Agustus 2019]

Baidya, J., Saha, T., Moyashir, R., & Palit, R., 2017. Design and implementation of a *Fingerprint* based lock system for shared access. In: IEEE, *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*. Las Vegas, USA, 9-11 January 2017. IEEE Xplore :

Firebase, 2019. *Firebase Realtime Database*. [online] Tersedia di : <https://Firebase.google.com/docs/*database*?hl=id> [Diakses 20 Agustus 2019]

Handsontec, 2019. *ESP8266 Node*MCU *WiFi Devkit*. [pdf] Tersedia di : <https://www.handsontec.com/pdf_learn/esp8266-V10.pdf> [Diakses 20 Agustus 2019]

Morsalin, S., Islam, A. M. J., Rahat, G. R., Pidim, S. R. H., Rahman, A., Siddiqe, M. A. B., 2016. Machine-to-machine communication based smart home security system by NFC, *Fingerprint*, and PIR sensor with mobile android application. In: IEEE, *2016 3rd International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)*. Dhaka, Bangladesh, 22-24 September 2016. IEEE Xplore : IEEE.

Postech, 2013. *Research Area on WSN and Ad-hoc Networks*. [image online] Tersedia di:

< http://monet.postech.ac.kr/research.html > [Diakses 20 Agustus 2019]

Siswanto, A., Katuk, N., Ku-Mahamud, K.R., 2016. Biometrik *Fingerprint* Architecture for Home Security System. In: ResearchGate, *3rd Innovation and Analytics Conference & Exhibition (IACE) 2016*. Sintok, Malaysia, 31 Oktober-1 November 2016. researchgate.net : ResearchGate

Teachmemicro, 2019. *Node*MCU *Pinout Reference*. [image online] Tersedia di: <https://www.teachmemicro.com/*Node*MCU-pinout/> [Diakses 20 Agustus 2019]

TheoryCircuit, 2019. *Fingerprint sensor pinout*. [image online] Tersedia di: <http://www.theorycircuit.com/*Fingerprint*-sensor-scanner-arduino/*Fingerprint*-sensor-pinout/> [Diakses 20 Agustus 2019]

Tobing, Sandro Lumban. 2014. Rancang Bangun Pengaman Pintu Menggunakan Sidik Jari (*Fingerprint*) Dan *Smartphone* Android Berbasis Mikrokontroler Atmega8. *Jurnal Teknik Elektro UNTAN*, [e-journal] 1(1). Tersedia melalui: Jurnal Teknik Elektro Universitas Tanjungpura <http://jurnal.untan.ac.id> [Diakses 20 Agustus 2019]

Wang, Y., Hu, C., Feng, Z., Ren, Y., 2014. Wireless transmission module comparison. In: IEEE, *2014 IEEE International Conference on Information and Automation (ICIA)*. Hailar, China, 28-30 July 2014. IEEE Explore : IEEE.

Zhang, S., Zhang, H., 2012. A review of wireless sensor networks and its applications. In: IEEE, *2012 IEEE International Conference on Automation and Logistics*. Zhengzhou, China, 15-17 August 2012. IEEE Xplore : IEEE.