

**SKRIPSI**

**ANALISIS KINERJA SecWSN BERBASIS RSA 2048 DAN  
SHA-3 MENGGUNAKAN RASPBERRY PI**

***PERFORMANCE ANALYSIS OF SECWSN BASED ON RSA 2048  
AND SHA-3 USING RASPBERRY PI***



Disusun oleh

**AHMAD FAUZZAN MAGHRIBI  
17101044**

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI  
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO  
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

**2021**

**ANALISIS KINERJA SecWSN BERBASIS RSA 2048 DAN  
SHA-3 MENGGUNAKAN RASPBERRY PI**

***PERFORMANCE ANALYSIS OF SecWSN BASED ON RSA 2048  
AND SHA-3 USING RASPBERRY PI***

**Skripsi ini digunakan sebagai salah satu syarat untuk memperoleh  
Gelar Sarjana Teknik (S.T.)  
Di Institut Teknologi Telkom Purwokerto  
2021**

Disusun oleh

**AHMAD FAUZZAN MAGHRIBI  
17101044**

**DOSEN PEMBIMBING**

**Syariful Ikhwan, S.T., M.T.**

**Risa Farrid Christianti, S.T., M.T.**

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI  
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO  
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

**2021**

**HALAMAN PENGESAHAN**

**ANALISIS KINERJA SecWSN BERBASIS RSA 2048 DAN  
SHA-3 MENGGUNAKAN RASPBERRY PI**

***PERFORMANCE ANALYSIS OF SECWSN BASED ON RSA 2048  
AND SHA-3 USING RASPBERRY PI***

Disusun oleh  
**AHMAD FAUZZAN MAGHRIBI**  
17101044

Telah dipertanggungjawabkan di hadapan Tim Penguji pada tanggal 3 Maret 2021

**Susunan Tim Penguji**

Pembimbing Utama : Syariful Ikhwan, S.T., M.T. ( )  
NIDN. 0605048201

Pembimbing Pendamping : Risa Farrid Christianti, S.T., M.T. ( )  
NIDN. 0604027802

Penguji 1 : Khoirun Ni'amah, S.T., M.T. ( )  
NIDN. 0619129301

Penguji 2 : Mas Aly Afandi, S.T., M.T. ( )  
NIDN. 0617059302

**Mengetahui,**

Ketua Program Studi S1 Teknik Telekomunikasi  
Institut Teknologi Telkom Purwokerto

Herryawan Pujiharsono, S.T., M.Eng.  
NIDN. 0617068801

## HALAMAN PERNYATAAN ORISINALITAS

Dengan ini saya, **AHMAD FAUZZAN MAGHRIBI**, menyatakan bahwa skripsi dengan judul **“ANALISIS KINERJA SecWSN BERBASIS RSA 2048 DAN SHA-3 MENGGUNAKAN RASPBERRY PI”** adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan kecuali melalui pengutipan sesuai dengan etika keilmuan yang berlaku. Saya bersedia menanggung risiko ataupun sanksi yang dijatuhkan kepada saya apabila ditemukan pelanggaran terhadap etika keilmuan dalam skripsi saya ini.

Purwokerto, 22 Februari 2021

Yang menyatakan,



(Ahmad Fauzzan Maghribi)

## PRAKATA

Puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan kasih dan sayang-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul “**Analisis Kinerja SecWSN Berbasis RSA 2048 Dan SHA-3 Menggunakan Raspberry Pi**”.

Maksud dari penyusunan skripsi ini adalah untuk memenuhi salah satu syarat dalam menempuh ujian sarjana Teknik Telekomunikasi pada Fakultas Teknik Telekomunikasi dan Elektro Institut Teknologi Telkom Purwokerto.

Dalam penyusunan skripsi ini, banyak pihak yang sangat membantu penulis dalam berbagai hal. Oleh karena itu, penulis sampaikan rasa terima kasih yang sedalam-dalamnya kepada:

1. Ummi dan Abi yang selalu memberi dukungan sepenuh hati kepada saya.
2. Bapak Syariful Ikhwan, S.T., M.T. selaku pembimbing I.
3. Ibu Risa Farrid Christianti, S.T., M.T. selaku pembimbing II.
4. Pak Herryawan Pujiharsono, S.T., M.Eng. selaku Dosen Wali dan Ketua Program Studi S1 Teknik Telekomunikasi.
5. Bapak Dr. Ali Rohman., M.Si. selaku Rektor Institut Teknologi Telkom Purwokerto.
6. Seluruh dosen, staf dan karyawan Program studi S1 Teknik Telekomunikasi Institut Teknologi Telkom Purwokerto.
7. Serta seluruh rekan-rekan saya yang selalu mengingatkan dan memberi semangat sehingga saya bisa mengerjakan penelitian ini hingga selesai.

Purwokerto, 22 Februari 2021

(Ahmad Fauzzan Maghribi)

## DAFTAR ISI

HALAMAN JUDUL .....	I
HALAMAN PENGESAHAN .....	I
HALAMAN PERNYATAAN ORISINALITAS .....	III
PRAKATA.....	IV
ABSTRAK.....	V
<i>ABSTRACT</i> .....	VI
DAFTAR ISI.....	VII
DAFTAR GAMBAR.....	IX
DAFTAR TABEL.....	XI
BAB 1 PENDAHULUAN .....	1
1.1    LATAR BELAKANG.....	1
1.2    RUMUSAN MASALAH .....	2
1.3    BATASAN MASALAH.....	3
1.4    TUJUAN.....	3
1.5    MANFAAT .....	3
1.6    SISTEMATIKA PENULISAN .....	3
BAB 2 DASAR TEORI.....	5
2.1    KAJIAN PUSTAKA .....	5
2.2 <i>Wireless Sensor Network (WSN)</i> .....	7
2.3    LoRa ( <i>Long Range</i> ) .....	9
2.4    Algoritma RSA.....	10
2.5    Algoritma SHA-3 .....	11
2.6    Quality Of Service (QoS) .....	12
2.7    Raspberry Pi .....	13
BAB 3 METODE PENELITIAN .....	14
3.1    ALAT YANG DIGUNAKAN.....	14
3.2    ALUR PENELITIAN .....	14
3.3    SKENARIO PENELITIAN.....	15

3.4	ALUR PEMROGRAMAN.....	16
3.5	PROSES ENKRIPSI.....	20
3.6	PROSES DEKRIPSI.....	22
BAB 4 HASIL DAN PEMBAHASAN .....		25
4.1	PROSES PENGUJIAN.....	25
4.2	ANALISIS <i>DELAY</i> .....	26
4.4	ANALISIS KEAMANAN.....	31
BAB 5 PENUTUP .....		33
5.1	KESIMPULAN.....	33
5.2	SARAN.....	33
DAFTAR PUSTAKA .....		35
LAMPIRAN.....		38

## DAFTAR GAMBAR

Gambar 2.1 <i>Protocol layer</i> WSN [2] .....	8
Gambar 2.2 Alokasi frekuensi LoRa [14] .....	9
Gambar 2.3 Ilustrasi algoritma RSA .....	11
Gambar 2.4 Ilustrasi <i>Sponge Function</i> [13] .....	12
Gambar 2.5 Raspberry Pi dan arsitekturnya [22] .....	13
Gambar 3.1 Alur proses penelitian .....	14
Gambar 3.2 Topologi WSN yang digunakan .....	15
Gambar 3.3 Skenario pengujian .....	16
Gambar 3.4 Alur algoritma program pengirim .....	17
Gambar 3.5 Alur algoritma program penerima .....	18
Gambar 3.6 <i>Import</i> fungsi dari <i>library</i> pada program pengirim .....	19
Gambar 3.7 <i>Import</i> fungsi dari <i>library</i> pada program penerima .....	19
Gambar 3.8 Proses enkripsi pada program pengirim .....	21
Gambar 3.9 Proses konfigurasi program pengirim .....	21
Gambar 3.10 Tampilan program <i>wsn_transmitter.py</i> .....	22
Gambar 3.11 Proses konfigurasi program penerima .....	23
Gambar 3.12 Proses dekripsi pada program .....	24
Gambar 3.13 Tampilan pada program <i>wsn_server.py</i> .....	24
Gambar 4.1 Alokasi <i>sensor node</i> dan <i>server node</i> saat pengujian .....	25
Gambar 4.2 Proses pengiriman dan penerimaan .....	26
Gambar 4.3 Isi <i>file</i> csv hasil pengujian .....	27
Gambar 4.4 Rata-rata <i>delay</i> tanpa enkripsi .....	27
Gambar 4.5 <i>Delay</i> tanpa enkripsi berdasarkan waktu .....	28
Gambar 4.6 Rata-rata <i>delay</i> dengan enkripsi .....	29
Gambar 4.7 <i>Delay</i> dengan enkripsi berdasarkan waktu .....	29
Gambar 4.8 Perbandingan <i>delay</i> .....	30
Gambar 4.9 Paket data yang dikirimkan dengan enkripsi .....	31
Gambar 4.10 Paket data yang dikirimkan tanpa enkripsi .....	32



Gambar 5.1 Hasil pengujian <i>delay</i> pada jarak 100 meter .....	45
Gambar 5.2 Hasil pengujian pada jarak 200 meter .....	46
Gambar 5.3 Hasil pengujian <i>delay</i> pada jarak 300 meter .....	47
Gambar 5.4 Hasil uji plagiarisme.....	48

## DAFTAR TABEL

Tabel 2.1 Parameter <i>delay</i> ( <i>latency</i> ).....	12
--	----