

**PENDETEKSIAN SERANGAN DOS MENGGUNAKAN  
METODE NAIVE BAYES PADA PERANGKAT  
BERBASIS TEKNOLOGI *INTERNET OF THINGS***

**TESIS**



oleh

**Fransiscus Fery Setiadi**

**NIM 1729101033**

**UNIVERSITAS PENDIDIKAN GANESHA**

**PROGRAM PASCASARJANA**

**PROGRAM STUDI ILMU KOMPUTER**

**JANUARI 2021**

**PENDETEKSIAN SERANGAN DOS MENGGUNAKAN  
METODE NAIVE BAYES PADA PERANGKAT  
BERBASIS TEKNOLOGI *INTERNET OF THINGS***

**TESIS**

**Diajukan kepada  
Universitas Pendidikan Ganesha  
Untuk Memenuhi Sebagian Persyaratan  
Memperoleh Gelar Magister Komputer  
Program Pascasarjana Jurusan Ilmu Komputer**

**oleh  
Fransiscus Fery Setiadi  
NIM 1729101033**

**UNIVERSITAS PENDIDIKAN GANESHA**

**PROGRAM PASCASARJANA**

**PROGRAM STUDI ILMU KOMPUTER**


**JANUARI 2021**

## LEMBAR PERSETUJUAN PEMBIMBING

Tesis oleh Fransiscus Fery Setiadi ini telah diperiksa dan disetujui untuk mengikuti Ujian Tesis.

Singaraja, 20 Oktober 2020

Pembimbing I,



Kadek Yota Ernanda Aryanto, S.Kom., M.T., Ph.D.

NIP. 19780324 2005 01 1 001

Pembimbing II,



Made Windu Antara Kesiman, S.T., M.Sc., Ph.D.

NIP. 19821111 200812 1 001

## LEMBAR PERSETUJUAN PENGUJI

Tesis oleh Fransiscus Fery Setiadi ini telah berhasil dipertahankan di depan tim penguji dan dinyatakan diterima sebagai sebagian persyaratan untuk memperoleh gelar Magister Komputer di Program Studi Ilmu Komputer, Program Pascasarjana, Universitas Pendidikan Ganesha.

Disetujui pada tanggal: 20 Januari 2021

Oleh Tim Penguji

  
..... Ketua Dr. Gede Indrawan, S.T., M.T.  
NIP. 19760102 200312 1 001

  
..... Anggota Dr. I Gede Aris Gunadi, S.Si., M.Kom.  
NIP. 19770318 200812 1 004


  
..... Anggota Dr. I Nyoman Sukajaya, M.T.  
NIP. 19671115 199303 1 001

  
..... Anggota Made Windu Antara Kesiman, S.T., M.Sc., Ph.D.  
NIP. 19821111 200812 1 001

  
..... Anggota Kadek Yota Ernanda Aryanto, S.Kom., M.T., Ph.D.  
NIP. 19780324 200501 1 001



Mengetahui,  
Direktur Pascasarjana Undiksha,

  
..... Prof. Dr. I Gusti Putu Suharta, M.Si  
NIP. 19621215 198803 1 002



## LEMBAR PERYATAAN

Saya menyatakan dengan sesungguhnya bahwa tesis yang saya susun sebagai syarat untuk memperoleh gelar Magister Pendidikan dari Pascasarjana Universitas Pendidikan Ganesha seluruhnya merupakan hasil karya saya sendiri. Bagian-bagian tertentu dalam penulisan tesis yang saya kutip dari hasil karya orang lain telah dituliskan sumbernya secara jelas dan sesuai dengan norma, kaidah, serta etika akademis.

Apabila di kemudian hari ditemukan seluruh atau sebagian tesis ini bukan hasil karya saya sendiri atau adanya plagiat dalam bagian-bagian tertentu, saya bersedia menerima sanksi pencabutan gelar akademik yang saya sandang dan sanksi-sanksi lainnya sesuai dengan peraturan perundang-undangan yang berlaku di wilayah Negara Kesatuan Republik Indonesia.

Singaraja, 20 Oktober 2020

Yang memberi pernyataan,



Fransiscus Fery Setiadi



## PRAKATA

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas anugrah-Nya, sehingga tesis yang berjudul *“Pendeteksian Serangan DoS Menggunakan Metode Naive Bayes Pada Perangkat Berbasis Teknologi Internet of Things”*, dapat diselesaikan sesuai dengan yang direncanakan.

Tesis ini ditulis untuk memenuhi salah satu persyaratan untuk memperoleh gelar Magister Ilmu Komputer pada Universitas Pendidikan Ganesha.

Terselesaikannya tesis ini telah banyak memperoleh uluran tangan dari berbagai pihak. Untuk itu, ijin penulis menyampaikan terima kasih dan penghargaan kepada pihak-pihak berikut.

1. Kadek Yota Ernanda Aryanto, S.Kom., M.T., Ph.D., sebagai pembimbing I yang telah dengan sabar membimbing dan memberikan motivasi yang demikian bermakna, sehingga penulis mampu melewati berbagai masalah dalam perjalanan studi dan penyelesaian tesis ini;
2. Made Windu Antara Kesiman, S.T., M.Sc., Ph.D., sebagai pembimbing II, yang selalu mengarahkan, memberikan semangat dan harapan kepada penulis selama penelitian dan penulisan naskah, sehingga tesis ini dapat terwujud dengan baik sesuai harapan;
3. Dr. I Nyoman Sukajaya, M.T. dan Dr. I Gede Aris Gunadi, S.Si. M.Kom. sebagai penguji yang telah banyak memberikan masukan-masukan yang bermanfaat untuk penyempurnaan tesis ini;
4. Bapak Rektor Universitas Pendidikan Ganesha, yang telah memberikan bantuan secara moral dan memfasilitasi berbagai kepentingan studi, selama penulis menempuh perkuliahan di Program Pascasarjana Undiksha;
5. Bapak Direktur Program Pascasarjana Undiksha dan staf, yang telah banyak membantu selama penulis mengikuti studi dan menyelesaikan penulisan tesis;
6. Bapak Ketua Program Studi Ilmu Komputer dan staf dosen pengajar yang telah banyak membantu dan memotivasi penulis selama perjalanan studi dan

penyusunan tesis ini;

7. PT. Archipelago International serta rekan-rekan kerja yang telah memberikan izin dan bantuan secara administratif maupun material sehingga penulis memperoleh kesempatan melanjutkan studi dan menyelesaikan tesis ini;
8. Bapak I Nyoman Sudana dan Ibu Ni Nyoman Rai Pujiwati selaku Kedua Orang Tua penulis, yang telah banyak membantu secara moral selama perjalanan studi yang penulis lakoni di Program Studi Ilmu Komputer;
9. Ni Kadek Sri Arthami selaku Istri Penulis dan Federica Putu Chrisya Setiana selaku anak Penulis yang telah banyak membantu secara material dan moral selama perjalanan studi yang penulis lakoni di Program Studi Ilmu Komputer;
10. Rekan-rekan seangkatan di Program Studi Ilmu Komputer yang dengan karakternya masing-masing telah banyak berkontribusi membentuk kemandirian penulis selama menjalani studi dan menyelesaikan tesis ini;

Semoga semua bantuan yang telah mereka taburkan dalam perjalanan studi penulis, terhargaikan dengan sepantasnya oleh Tuhan Yang Maha Esa, sehingga mereka diberi jalan, rejeki, dan keharmonian dalam menjalani setiap langkah kehidupan.

Penulis menyadari bahwa tesis ini belum dapat dikategorikan sempurna. Namun terlepas dari semua predikat tersebut, yang jelas, kehadirannya dalam konstelasi masyarakat akademis akan ikut serta memberikan warna bagi pembangunan dunia pendidikan walau hanya setitik. Mudah-mudahan tesis ini bermanfaat bagi masyarakat akademis.

Singaraja, 20 Oktober 2020

Penulis

## DAFTAR ISI

PRAKATA .....	i
ABSTRAK.....	iii
ABSTRACT .....	iv
DAFTAR ISI.....	v
DAFTAR TABEL.....	vii
DAFTAR GAMBAR .....	ix
BAB I <u>P</u> ENDAHULUAN.....	1
1.1. Latar Belakang .....	1
1.2. Rumusan Masalah .....	3
1.3. Batasan Masalah .....	4
1.4. Tujuan Penelitian.....	4
1.5. Manfaat Penelitian.....	4
BAB II <u>K</u> AJIAN TEORI.....	5
2.1. Penulisan Terkait.....	5
2.2. <i>Intrusion Detection System (IDS)</i> .....	6
2.3. Serangan pada perangkat <i>Internet of Things (IoT)</i> .....	7
2.4. Naive Bayes <i>Classifier</i> .....	10
2.5. Fungsi Gaussian.....	10
2.6. Dataset.....	12
2.6.1. Dataset NSL-KDD .....	12
2.6.2. Format Dataset KDD „99 .....	13
2.6.3. Fitur Dataset NSLKDD .....	15
2.7. Snort.....	17
2.8. Raspberry Pi.....	19
BAB III <u>M</u> ETODOLOGI PENELITIAN.....	20
3.1. Kajian Literatur.....	21
3.2. Metode .....	21

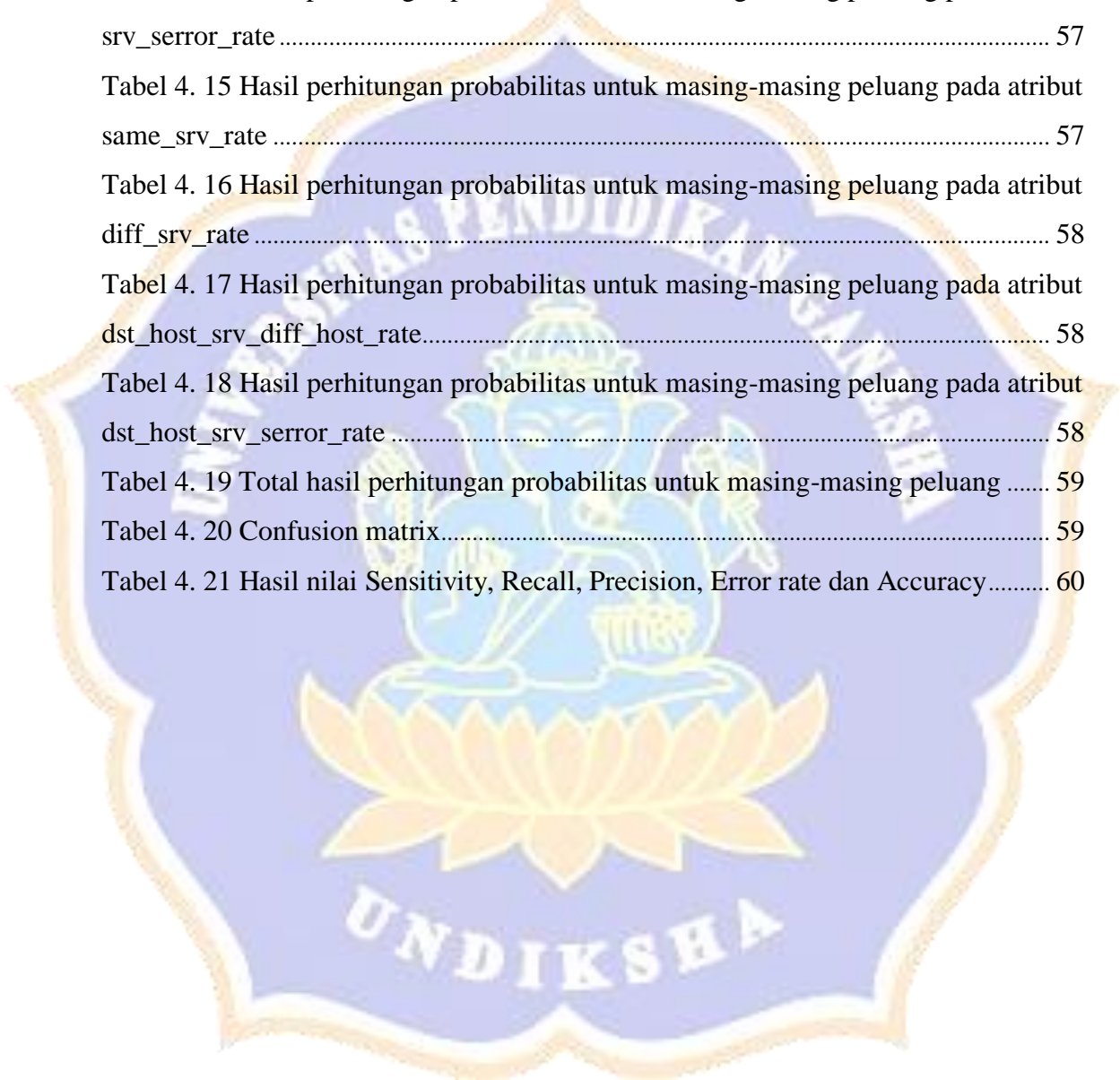


3.3.	Seleksi Fitur .....	28
3.4.	Dataset .....	29
3.5.	Identifikasi Sistem .....	30
3.6.	Simulasi Pengambilan Data <i>Testing</i> .....	31
3.7.	Analisis .....	33
<b>BAB IV HASIL PENELITIAN &amp; PEMBAHASAN.....</b>		<b>35</b>
4.1.	.....PenyiapanPerangkatdanSistem	35
4.1.1.	Hasil penyiapan perangkat .....	35
4.1.2.	Hasil instalasi Sistem Operasi .....	36
4.1.3.	Hasil instalasi aplikasi Snort .....	37
4.2.	Hasil Simulasi Sistem .....	37
4.2.1.	Hasil Snort <i>Rule</i> .....	38
4.2.2.	Hasil Simulasi Serangan .....	39
4.2.3.	Hasil Snort <i>Log</i> .....	40
4.2.4.	KDD99 Extractor .....	42
4.3.	Hasil Data <i>Testing</i> .....	43
4.4.	Hasil Data <i>Training</i> .....	44
4.5.	Hasil Proses Seleksi Atribute .....	45
4.6.	Hasil Klasifikasi Data Kontinyu .....	47
4.7.	Hasil Perhitungan Naïve Bayes .....	51
4.7.1.	Hasil Menghitung Class Probabilities .....	51
4.7.2.	Hasil Menghitung Conditional Probabilities .....	52
4.8.	Hasil Akurasi Naïve Bayes .....	59
4.9.	Hasil Interface Simulasi Aplikasi Deteksi DoS.....	62
<b>BAB V PENUTUP .....</b>		<b>70</b>
5.1.	.....Rangkuman	70
5.2.	Kesimpulan .....	71
5.3.	Saran .....	72
<b>DAFTAR RUJUKAN .....</b>		<b>73</b>

## DAFTAR TABEL

Tabel 2. 1 Fitur dasar dari koneksi TCP individual .....	15
Tabel 2. 2 Fitur konten dalam koneksi yang disarankan oleh domain .....	16
Tabel 2. 3 Fitur lalu lintas dihitung menggunakan waktu dua detik .....	16
Tabel 3. 1 Dataset NSLKDD diambil secara acak .....	23
Tabel 3. 2 Data testing NSLKDD .....	23
Tabel 3. 3 Probabilitas service .....	25
Tabel 3. 4 Probabilitas flag .....	25
Tabel 3. 5 Nilai mean dan standar deviasi pada attribute src_bytes .....	25
Tabel 3. 6 Nilai mean dan standar deviasi pada attribute dst_bytes .....	26
Tabel 3. 7 Nilai mean dan standar deviasi pada attribute srv_error_rate .....	26
Tabel 3. 8 Nilai mean dan standar deviasi pada attribute same_srv_rate .....	26
Tabel 3. 9 Nilai mean dan standar deviasi pada attribute diff_srv_rate .....	26
Tabel 3. 10 Nilai mean dan standar deviasi pada attribute dst_host_srv_diff_host_rate .....	26
Tabel 3. 11 Nilai mean dan standar deviasi pada attribute dst_host_srv_error_rate .....	27
Tabel 3. 12 Perhitungan metode Naïve Bayes .....	27
Tabel 4. 1 Hasil nilai <i>mean</i> dan standar deviasi atribut src_bytes .....	47
Tabel 4. 2 Hasil nilai <i>mean</i> dan standar deviasi atribut dst_bytes .....	48
Tabel 4. 3 Hasil nilai <i>mean</i> dan standar deviasi atribut srv_error_rate .....	48
Tabel 4. 4 Hasil nilai <i>mean</i> dan standar deviasi atribut same_srv_rate .....	49
Tabel 4. 5 Hasil nilai <i>mean</i> dan standar deviasi atribut diff_srv_rate .....	49
Tabel 4. 6 Hasil nilai <i>mean</i> dan standar deviasi atribut dst_host_srv_diff_host_rate .....	50
Tabel 4. 7 Hasil nilai <i>mean</i> dan standar deviasi atribut dst_host_srv_error_rate ..	50
Tabel 4. 8 Contoh data <i>testing</i> .....	51
Tabel 4. 9 Hasil nilai probabilitas dari masing-masing kelas masalah .....	52
Tabel 4. 10 Hasil perhitungan untuk masing-masing peluang pada atribut service ...	53

Tabel 4. 11 Hasil perhitungan untuk masing-masing peluang pada atribut flag.....	55
Tabel 4. 12 Hasil perhitungan probabilitas untuk masing-masing peluang pada atribut src_bytes.....	56
Tabel 4. 13 Hasil perhitungan probabilitas untuk masing-masing peluang pada atribut dst_bytes.....	56
Tabel 4. 14 Hasil perhitungan probabilitas untuk masing-masing peluang pada atribut srv_error_rate .....	57
Tabel 4. 15 Hasil perhitungan probabilitas untuk masing-masing peluang pada atribut same_srv_rate .....	57
Tabel 4. 16 Hasil perhitungan probabilitas untuk masing-masing peluang pada atribut diff_srv_rate .....	58
Tabel 4. 17 Hasil perhitungan probabilitas untuk masing-masing peluang pada atribut dst_host_srv_diff_host_rate.....	58
Tabel 4. 18 Hasil perhitungan probabilitas untuk masing-masing peluang pada atribut dst_host_srv_error_rate .....	58
Tabel 4. 19 Total hasil perhitungan probabilitas untuk masing-masing peluang .....	59
Tabel 4. 20 Confusion matrix.....	59
Tabel 4. 21 Hasil nilai Sensitivity, Recall, Precision, Error rate dan Accuracy.....	60



## DAFTAR GAMBAR

Gambar 2. 1 Serangan terhadap perangkat IoT.....	8
Gambar 3. 1 Alur Metodologi Penelitian.....	20
Gambar 3. 2 Arsitektur IDS.....	33
Gambar 4. 1 Hasil penyiapan perangkat.....	36
Gambar 4. 2 Versi Sistem Operasi Raspbian.....	36
Gambar 4. 3 Versi aplikasi Snort.....	37
Gambar 4. 4 Hasil Snort <i>rules</i> yang terbaca.....	38
Gambar 4. 5 Low Orbit Ion Cannon.....	39
Gambar 4. 6 Hasil <i>alert</i> dari serangan <i>SYN flood</i> .....	40
Gambar 4. 7 Hasil data Snort <i>log</i> .....	41
Gambar 4. 8 Hasil tcpdump Snort menggunakan tshark.....	41
Gambar 4. 9 Hasil pcap file ekstraktor dengan format KDD99.....	42
Gambar 4. 10 Hasil data <i>testing</i> .....	43
Gambar 4. 11 Hasil data <i>training</i> dari dataset NSLKDD.....	44
Gambar 4. 12 Hasil seleksi atribut menggunakan Info Gain weka.....	46
Gambar 4. 13 Hasil seleksi atribut menggunakan CFS weka.....	47
Gambar 4. 14 Tampilan halaman <i>login</i> .....	63
Gambar 4. 15 Tampilan halaman <i>about</i> .....	64
Gambar 4. 16 Tampilan halaman <i>DataTraining</i> .....	65
Gambar 4. 17 Tampilan halaman <i>dataTest</i> .....	66
Gambar 4. 18 Tampilan halaman <i>add DataTest</i> .....	67
Gambar 4. 19 Tampilan halaman <i>edit dataTest</i> .....	68
Gambar 4. 20 Tampilan halaman <i>delete</i> .....	69



