



UNIVERSITAS
MERCU BUANA

**Pengembangan *Intrusion Detection System* (IDS) Berbasis
*Machine Learning***

TESIS

**OLEH
ADY SURYADI
55419120016**

UNIVERSITAS

MERCU BUANA

**PROGRAM STUDI MAGISTER TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS MERCU BUANA
2022**



UNIVERSITAS
MERCU BUANA

**Pengembangan *Intrusion Detection System* (IDS) Berbasis
*Machine Learning***

TESIS

Diajukan sebagai Salah Satu Syarat untuk Menyelesaikan
Program Studi Megister Teknik Elektro

**OLEH
ADY SURYADI
55419120016**

UNIVERSITAS

MERCU BUANA

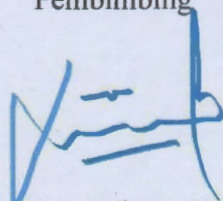
**PROGRAM STUDI MAGISTER TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS MERCU BUANA
2022**

PENGESAHAN TESIS

Judul : Pengembangan *Intrusion Detection System* (IDS)
berbasis *machine learning*
Nama : ADY SURYADI
NIM : 55419120016
Program Studi : Magister Teknik Elektro
Tanggal : 25 Februari 2022

Mengesahkan

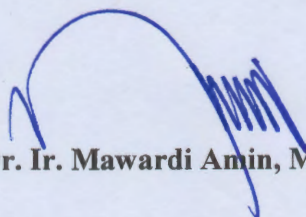
Pembimbing



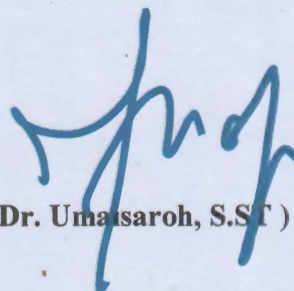
(Dr. Marza Ihsan Marzuki, M.T.)

Dekan Fakultas Teknik

Ketua Program Studi
Magister Teknik Elektro



(Dr. Ir. Mawardi Amin, M.T.)



(Dr. Umatsaroh, S.Si)

PERNYATAAN *SIMILARITY CHECK*

Saya yang bertanda tangan di bawah ini menyatakan, bahwa karya ilmiah yang ditulis oleh

Nama : ADY SURYADI
NIM : 55419120016
Program Studi : Magister Teknik Elektro

dengan judul

“PENGEMBANGAN INTRUSION DETECTION SYSTEM (IDS) BERBASIS MACHINE LEARNING”,

telah dilakukan pengecekan *similarity* dengan sistem Turnitin pada tanggal 8/Maret/2022, didapatkan nilai persentase sebesar 13 %.

Jakarta, 8 Maret 2022
Administrator Turnitin



Aric Pangudi, A.Md

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan dengan sebenar-benarnya bahwa semua pernyataan dalam tesis ini :

Judul : Pengembangan *Intrusion Detection System* (IDS) berbasis *machine learning*
Nama : ADY SURYADI
NIM : 55419120016
Program Studi : Magister Teknik Elektro
Tanggal : 25 Februari 2022

Merupakan hasil studi pustaka, penelitian lapangan dan karya saya sendiri dengan bimbingan Komisi Dosen Pembimbing yang ditetapkan dengan Surat Keputusan Ketua Program Studi Magister teknik Elektro Universitas Mercu Buana.

Karya ilmiah ini belum pernah diajukan untuk memperoleh gelar kesarjanaan pada program sejenis di perguruan tinggi lain. Semua informasi, data dan hasil pengolahan yang digunakan, telah dinyatakan secara jelas sumbernya dan dapat diperiksa kebenarannya.

Jakarta, 25 Februari 2022



(**Ady Suryadi**)

KATA PENGANTAR

Puji syukur yang sedalam-dalamnya penulis panjatkan kehadirat Allah SWT atas segala nikmat, rahmat dan karunia-Nya yang disertai dengan do'a, sehingga dapat terselesaikannya tesis ini.

Penulis bersyukur telah menyelesaikan tesis ini sesuai dengan waktu yang ditentukan atas kerja keras, ikhtiar dan doa. Di dalam penulisan tesis ini penulis banyak mendapatkan bimbingan dan dukungan dari berbagai pihak. Oleh karena itu, penulis mengucapkan banyak terima kasih yang sebesar-besarnya kepada :

1. Bapak Dr. Marza Ihsan Marzuki, M.T. selaku Dosen Pembimbing yang selalu memberikan masukan dan arahan dalam pembuatan tesis ini.
2. Bapak Dr. Mawardi Amin, MT selaku Dekan Fakultas Teknik
3. Ibu Dr. Umairah, S.ST selaku Ketua Program Studi Magister Teknik Elektro
4. Keluarga besar dan Istri, yang selalu memberikan do'a dan semangat sehingga terselesaikannya tesis ini.

Penulis menyadari bahwa dalam penulisan tesis ini masih jauh dari sempurna. Oleh karena itu kritik dan sarannya untuk membangun semangat dari penulis akan diterima dengan senang hati. Semoga penulisan tesis ini dapat bermanfaat bagi kita semua.

Jakarta, 25 Februari 2022

Ady Suryadi

Abstrak

Penggunaan internet yang terus meningkat memerlukan sistem deteksi serangan yang handal agar penyusup atau *cracker* yang hendak melakukan *cyberattacks* dapat terdeteksi dengan cepat. Mitigasi dan pertahanan dari ancaman serangan *cyber* menjadi sangat penting mengingat masyarakat sudah mulai ketergantungan pada teknologi internet yang bisa mengancam setiap saat. Ketika sejumlah besar paket datang, maka perlu dideteksi apakah paket tersebut paket data normal atau paket data serangan. *Intrusion Detection System* (IDS) dapat digunakan untuk mendeteksi setiap serangan pada jaringan atau sistem informasi. Deteksi anomali adalah jenis IDS yang mendeteksi serangan anomali pada jaringan berdasarkan probabilitas statistik.

Pada penelitian ini deteksi serangan dilakukan dengan menggunakan metode *Knowledge Discovery in Databases* (KDD) berbasis *machine learning* untuk menganalisis serangan berdasarkan 2 (dua) sumber dataset yaitu UNSW-NB15 dan CICIDS2017. Algoritma J48, naïve bayes dan AdaBoostM1 digunakan untuk melakukan klasifikasi serangan. Pemrosesan data menggunakan tools WEKA.

Seleksi jumlah atribut dilakukan menggunakan metode *CFs-Greedy stepwise* untuk memilih atribut yang sangat berpengaruh terhadap pendeteksian serangan untuk efisiensi. Hasil pengujian menunjukkan algoritma J48 menghasilkan akurasi tertinggi sebesar 99.839%.

Keyword : *Data mining, Intrusion Detection System, Cyberattacks, Algoritma Machine Learning, WEKA.*

U N I V E R S I T A S

MERCU BUANA

Daftar Isi

HALAMAN JUDUL.....	ii
PENGESAHAN TESIS	iii
PERNYATAAN SIMILARITY CHECK.....	iv
PERNYATAAN.....	v
KATA PENGANTAR	vi
ABSTRAK	vii
Daftar Isi	viii
Daftar Gambar	xii
Daftar Table	xiv
BAB I Pendahuluan	1
A. Latar Belakang.....	1
B. Perumusan Masalah.....	5
C. Batasan Masalah.....	6
D. Tujuan Penelitian.....	6
BAB II Studi Pustaka	7
A. Penelitian Terkait.....	7
B. Machine Learning.....	8
C. Klasifikasi.....	9

D.	Correlation-Based Feature Selection.....	9
E.	10-Fold Cross-Validation.....	10
F.	Intrusion Detection System.....	10
G.	Jenis-jenis Serangan.....	11
1.	Malware.....	12
2.	Denial of Services.....	12
3.	Spam.....	12
H.	WEKA.....	13
I.	J48.....	14
J.	Naïve bayes.....	14
K.	Adaptive Boosting classifier (AdaBoost.M1).....	15
L.	Dataset.....	15
1.	UNSW-NB15.....	16
2.	CICIDS2017.....	16
M.	Knowledge Discovery in Databases (KDD).....	17

BAB III Metodologi Penelitian..... 18

A.	Rancangan Penelitian.....	18
1.	Selecting.....	19
2.	Preprocessing.....	19
3.	Transformation.....	20

4.	Machine learning	20
5.	Interpretation / Evaluation	20
a)	Confusion Matrix	20
BAB IV	Hasil dan Pembahasan	23
A.	Spesifikasi perangkat yang digunakan	23
B.	Selecting	23
C.	Preprocessing dataset.....	25
D.	Transformation	30
E.	Machine learning.....	32
F.	Interpretation / Evaluation.....	33
1.	Evaluasi proses dataset dengan algoritma J48 dengan Correlation-based Feature Selection (CFS)	33
2.	Accuracy J48 dengan CFS dataset UNSWNB15	33
3.	Precision J48 dengan CFS dataset UNSWNB15	39
4.	Recall J48 dengan CFS dataset UNSWNB15	41
5.	Accuracy J48 dengan CFS dataset CICIDS2017.....	43
6.	Precision J48 dengan CFS dataset CICIDS2017	47
7.	Recall J48 dengan CFS dataset CICIDS2017.....	48
8.	Evaluasi proses dataset dengan algoritma naïve bayes dengan Correlation-based Feature Selection (CFS)	50

9.	Accuracy Naïve bayes dengan CFS dataset UNSWNB15	51
10.	Precision Naïve bayes dengan CFS dataset UNSWNB15	52
11.	Recall Naïve bayes dengan CFS dataset UNSWNB15	53
12.	Accuracy Naïve bayes dengan CFS dataset CICIDS2017.....	54
13.	Precision Naïve bayes dengan CFS dataset CICIDS2017	56
14.	Recall Naïve bayes dengan CFS dataset CICIDS2017.....	57
15.	Evaluasi proses dataset dengan algoritma AdaBoostM1 dengan Correlation-based Feature Selection (CFS)	58
16.	Accuracy AdaBoostM1 dengan CFS dataset UNSWNB15	59
17.	Precision AdaBoostM1 dengan CFS dataset UNSWNB15 ...	61
18.	Recall AdaBoostM1 dengan CFS dataset UNSWNB15	62
19.	Accuracy AdaBoostM1 dengan CFS dataset CICIDS2017.....	63
20.	Precision AdaBoostM1 dengan CFS dataset CICIDS2017 ...	65
21.	Recall AdaBoostM1 dengan CFS dataset CICIDS2017.....	66
G.	Hasil pengujian.....	67

BAB V Penutup..... 70

A. Kesimpulan..... 70

Daftar Pustaka..... 72

Daftar Gambar

Gambar 2.1 Rumus <i>Correlation-based Feature Selection</i> (CFS).....	10
Gambar 2.2 Grafik spam sampai tahun 2017 (Marinos & Lourenço, 2018)	13
Gambar 2.3 Rumus naïve bayes (Anwar et al., 2019)	15
Gambar 2.4 Tahapan proses KDD	17
Gambar 3.1 Tahapan penelitian	18
Gambar 4.1 Distribusi <i>Dataset</i> UNSW-NB15	24
Gambar 4.2 Distribusi <i>Dataset</i> CICIDS2017	25
Gambar 4.3 Preprocessing <i>Dataset</i> CICIDS2017	25
Gambar 4.4 Preprocessing dataset UNSWNB15	26
Gambar 4.5 Menu utama WEKA.....	26
Gambar 4.6 Pemilihan dataset.....	27
Gambar 4.7 Menu seleksi fitur pada WEKA	27
Gambar 4.8 Jumlah data yang diproses dataset CICIDS2017	29
Gambar 4.9 Jumlah data yang diproses dataset UNSWNB15	29
Gambar 4.10 Hasil CFS <i>dataset</i> UNSWNB15 pada aplikasi WEKA	30
Gambar 4.11 Hasil CFS <i>dataset</i> CICIDS2017 pada aplikasi WEKA.....	31
Gambar 4.12 Confusion Matrix UNSWNB15 - J48 dengan CFS	33
Gambar 4.13 Hasil proses algoritma J48 dataset UNSWNB15.....	38
Gambar 4.14 Confusion Matrix WEKA dataset CICIDS2017 algoritma J48 dengan CFS	43
Gambar 4.15 Hasil proses algoritma J48 dataset CICIDS2017	46
Gambar 4.16 Hasil proses algoritma naïve bayes dataset UNSWNB15...	52

Gambar 4.17 Hasil proses algoritma naïve bayes dataset CICIDS2017... 56

Gambar 4.18 Hasil proses algoritma AdaBoostM1 dataset UNSWNB15 61

Gambar 4.19 Hasil proses algoritma AdaBoostM1 dataset CICIDS2017 65



U N I V E R S I T A S

MERCU BUANA

Daftar Table

Tabel 2.1 Penelitian Terkait Sistem Intrusi.....	7
Tabel 3.1 Matrik Konfusi.....	21
Tabel 4.1 Spesifikasi perangkat yang digunakan.....	23
Tabel 4.2 Dataset UNSW-NB15 (Moustafa & Slay, 2015).....	23
Tabel 4.3 Dataset CICIDS2017 (Sharafaldin et al., 2018).....	24
Tabel 4.4 Hasil seleksi atribut UNSW-NB15	31
Tabel 4.5 Hasil seleksi atribut CICIDS2017.....	32
Tabel 4.6 penjelasan class pada dataset UNSWNB15	34
Tabel 4.7 Total confusion matrik UNSWNB15 - J48 dengan CFS	34
Tabel 4.8 Class confusion matrix UNSWNB15 – CFS algoritma J48	36
Tabel 4.9 Akurasi class UNSWNB15 – J48 dengan CFS.....	37
Tabel 4.10 Precision class UNSWNB15 – J48 dengan CFS	40
Tabel 4.11 Recall class UNSWNB15 – J48 dengan CFS	42
Tabel 4.12 penjelasan class pada dataset CICIDS2017	43
Tabel 4.13 Confusion matrix seluruh class CICIDS2017 – CFS algoritma J48	44
Tabel 4.14 akurasi class CICIDS2017 – J48 dengan CFS	45
Tabel 4.15 Precision CICIDS2017 – J48 dengan CFS	47
Tabel 4.16 Recall CICIDS2017 – J48 dengan CFS	49
Tabel 4.17 Confusion matrix seluruh class UNSWNB15 – CFS algoritma naïve bayes	50
Tabel 4.18 Akurasi UNSWNB15 – naïve bayes dengan CFS	51
Tabel 4.19 Precision UNSWNB15 – naïve bayes dengan CFS	52

Tabel 4.20 Recall UNSWNB15 – naïve bayes dengan CFS.....	53
Tabel 4.21 Confusion matrix seluruh class CICIDS2017 – CFS algoritma naïve bayes	54
Tabel 4.22 Akurasi CICIDS2017 – naïve bayes dengan CFS	55
Tabel 4.23 Precission CICIDS2017 – naïve bayes dengan CFS.....	56
Tabel 4.24 Recall CICIDS2017 – naïve bayes dengan CFS	57
Tabel 4.25 Confusion matrix seluruh class UNSWNB15 – CFS algoritma AdaBoostM1	59
Tabel 4.26 Akurasi UNSWNB15 – AdaBoostM1 dengan CFS	60
Tabel 4.27 Precission UNSWNB15 – AdaBoostM1 dengan CFS.....	61
Tabel 4.28 Recall UNSWNB15 – AdaBoostM1 dengan CFS	62
Tabel 4.29 Confusion matrix seluruh class CICIDS2017 – CFS algoritma AdaBoostM1	63
Tabel 4.30 Akurasi CICIDS2017 – AdaBoostM1 dengan CFS.....	64
Tabel 4.31 Precission CICIDS2017 – AdaBoostM1 dengan CFS.....	65
Tabel 4.32 Recall CICIDS2017 – AdaBoostM1 dengan CFS	66
Tabel 4.33 Perbandingan hasil algoritma J48	68
Tabel 4.34 Perbandingan hasil algoritma Naïve Bayes	68
Tabel 4.35 Perbandingan hasil algoritma AdaBoostM1	69