



Perbandingan Metode *Supervised Machine Learning* – *Support Vector Machine* (SVM) dan *K-Nearest Neighbor Classifier* (KNN) dalam Analisis Pola *Cyber Attack* Pada *Dataset Network Intrusion Detection System* (NIDS)



**PROGRAM STUDI MAGISTER TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS MERCUBUANA
JAKARTA
2024**



Perbandingan Metode *Supervised Machine Learning* – *Support Vector Machine* (SVM) dan *K-Nearest Neighbor Classifier* (KNN) dalam Analisis Pola *Cyber Attack* Pada *Dataset Network Intrusion Detection System* (NIDS)



Diajukan sebagai Salah Satu Syarat untuk memperoleh gelar Magister Teknik Elektro

UNIVERSITAS
MERCU BUANA

**HAIKAL SHIDDIQ
55421110004**

**PROGRAM STUDI MAGISTER TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS MERCUBUANA
JAKARTA
2024**

HALAMAN PENYATAAN KARYA SENDIRI

Saya yang bertanda tangan di bawah ini:

Nama : HAIKAL SHIDDIQ

NIM : 55421110004

Program Studi : MAGISTER TEKNIK ELEKTRO

Judul Laporan Tesis : Perbandingan Metode *Supervised Machine Learning – Support Vector Machine (SVM)* dan *K-Nearest Neighbor Classifier (KNN)* dalam Analisis Pola *Cyber Attack* Pada *Dataset Network Intrusion Detection System (NIDS)*

Menyatakan bahwa Laporan Tesis ini adalah hasil karya saya sendiri dan bukan plagiat, serta semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar. Apabila ternyata ditemukan di dalam Laporan Tesis saya terdapat unsur plagiat, maka saya siap mendapatkan sanksi akademis yang berlaku di Universitas Mercu Buana.

Jakarta, 11 September 2024



Haikal Shiddiq

HALAMAN PENGESAHAN

Laporan Tesis ini diajukan oleh:

Nama : Haikal Shiddiq
NIM : 55421110004
Program Studi : Magister Teknik Elektro
Konsentrasi : Keamanan Jaringan
Judul Laporan Tesis : Perbandingan Metode Supervised Machine Learning – Support Vector Machine (SVM) dan K-Nearest Neighbor Classifier (KNN) dalam Analisis Pola Cyber Attack Pada Dataset Network Intrusion Detection System (NIDS)

Telah berhasil dipertahankan pada sidang di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Strata 2 pada Program Studi Magister Teknik Elektro Fakultas Teknik / Program Pascasarjana Universitas Mercu Buana.

Disahkan oleh:

Pembimbing : Prof. Dr. Ir. Setiyo Budiyanto,
S.T., M.T., IPM., Asean-Eng.,
APEC-Eng

()

NIDN : 0312118206

Ketua Sidang : Yudhi Gunardi, S.T., M.T. Ph.D
NIDN : 0330086902

()

Penguji 1 : Fadli Sirait, S.Si., M.T., Ph.D
NIDN : 0320057603

()

Jakarta, 18 September 2024

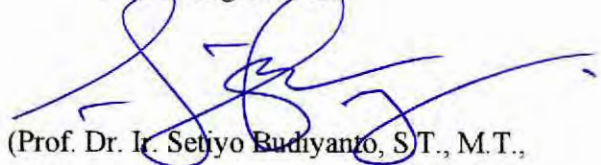
Mengetahui,

Dekan Fakultas Teknik



(Dr. Ir. Zulfa Fitri Ikatrinasari, M.T)

Ketua Program Studi



(Prof. Dr. Ir. Setiyo Budiyanto, S.T., M.T.,
IPM., Asean-Eng., APEC-Eng.)

KATA PENGANTAR

Alhamdulillah puji syukur penulis panjatkan kehadirat Allah SWT atas limpahan rahmat dan hidayah-Nya, sehingga saya dapat menyelesaikan Tesis ini dengan judul “Perbandingan Metode *Supervised Machine Learning – Support Vector Machine (SVM)* dan *K-Nearest Neighbor Classifier (KNN)* dalam Analisis Pola *Cyber Attack* Pada *Dataset Network Intrusion Detection System (NIDS)*”.

Penulisan tesis ini merupakan salah satu syarat wajib dalam perjalanan saya menuju gelar Magister Teknik di Program Studi Magister Teknik Elektro Universitas Mercu Buana. Saya sangat menyadari bahwa pencapaian ini tidak dapat terwujud tanpa dukungan, bantuan, dan bimbingan dari berbagai pihak sepanjang perjalanan pendidikan dan penelitian saya. Oleh karena itu, dengan tulus dan penuh rasa terima kasih, saya ingin menyampaikan penghargaan kepada:

1. Prof. Dr. Ir. Setiyo Budiyanto, S.T., M.T., IPM., Asean-Eng., APEC-Eng., selaku dosen pembimbing yang telah dengan tulus memberikan waktu, tenaga, dan bimbingan intelektualnya dalam proses penyusunan tesis ini.
2. Para dosen Program Studi Magister Teknik Elektro yang telah berdedikasi dalam proses pembelajaran kami, memberikan wawasan yang berharga, dan mendorong kami untuk berkembang secara akademis.
3. Kedua Orang Tuaku yang telah memberikan doa dan motivasi sehingga penyusunan Tesis ini dapat terselesaikan dengan baik.
4. Teman-teman seangkatan Magister Teknik Elektro Universitas Mercu Buana, yang telah memberikan dukungan dan kolaborasi yang sangat berarti dalam perjalanan ini.

Semoga Allah SWT membalas segala kebaikan, doa dan dukungan dari semua pihak yang telah saya sebutkan. Semoga tesis ini dapat memberikan kontribusi positif dalam pengembangan ilmu pengetahuan.

Jakarta, 11 September 2024



HAIKAL SHIDDIQ

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Mercu Buana, saya yang bertanda tangan di bawah ini:

Nama : HAIKAL SHIDDIQ

NIM : 55421110004

Program Studi : MAGISTER TEKNIK ELEKTRO

Judul Laporan Tesis : Perbandingan Metode *Supervised Machine Learning – Support Vector Machine* (SVM) dan *K-Nearest Neighbor Classifier* (KNN) dalam Analisis Pola *Cyber Attack* Pada *Dataset Network Intrusion Detection System* (NIDS)

Demi pengembangan ilmu pengetahuan, dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Non-Eksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul di atas beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Laporan Tesis saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 11 September 2024

Yang menyatakan,



HAIKAL SHIDDIQ

ABSTRAK

Nama : HAIKAL SHIDDIQ
NIM : 55421110004
Program Studi : MAGISTER TEKNIK ELEKTRO
Judul Laporan Tesis : Perbandingan Metode *Supervised Machine Learning – Support Vector Machine* (SVM) dan *K-Nearest Neighbor Classifier* (KNN) dalam Analisis Pola *Cyber Attack* Pada *Dataset Network Intrusion Detection System* (NIDS)
Dosen Pembimbing : Prof. Dr. Ir. Setiyo Budiyanto, S.T., M.T., IPM., Asean-Eng., APEC Eng.

Penelitian ini bertujuan untuk menganalisis *dataset opensource* NF-UQ-NIDS-v2 menggunakan *supervised learning - Support Vector Machine* (SVM) dan *K-Nearest Neighbor Classifier* (KNN) dalam menghitung tingkat akurasi, *precision*, *recall* dan *f1-score* pada satuan persentase.

Metode SVM dan KNN digunakan dengan *training* dan *test* menggunakan *cross validation* (cv) sebanyak 10 kali dan *dataset* tersebut dibagi menjadi 4 bagian besar agar proses analisisnya lebih mudah. Hasil menunjukkan metode *K-Nearest Neighbor* (KNN) memiliki akurasi lebih tinggi yaitu >90% dibandingkan metode *Support Vector Machine* (SVM) untuk seluruh grup *dataset*. Namun untuk membuat sebuah prediksi terkait jumlah tipe serangan yang sama cenderung menggunakan model *Support Vector Machine* (SVM) yang terlihat dari *heatmap prediction*.

Pola serangan DoS/DDoS paling sering terjadi dan metode *Support Vector Machine* (SVM) serta *K-Nearest Neighbor Classifier* (KNN) efektif untuk menganalisis pola serangan. Data ini bersifat *opensource* sehingga hasil *training* dan *test* dapat berubah dengan *update* data. Dengan pola serangan DoS/DDoS ini diharapkan setiap pemilik sistem aplikasi berbasis *web server* yang di *publish* ke internet dapat melakukan pencegahan serangan tersebut dengan memperkuat keamanan akses di jaringan dan sistem.

Kata Kunci : *Supervised learning, Support Vector Machine* (SVM), *K-Nearest Neighbor Classifier* (KNN), *dataset, cyber security, data analysis, analisis serangan cyber*

ABSTRACT

Name : HAIKAL SHIDDIQ
NIM : 55421110004
Study Program : MAGISTER TEKNIK ELEKTRO
Title Thesis : *Analysis of Cyber Attack Patterns on the Network Intrusion Detection System (NIDS) Dataset Using Supervised Machine Learning Methods - Support Vector Machine (SVM) and K-Nearest Neighbor Classifier (KNN)*
Consellor : Prof. Dr. Ir. Setiyo Budiyanto, S.T., M.T., IPM., Asean-Eng., APEC Eng.

This study aims to analyze the opensource NF-UQ-NIDS-v2 dataset using supervised learning - Support Vector Machine (SVM) and K-Nearest Neighbor Classifier (KNN) in calculating the level of accuracy, precision, recall and f1-score in percentage units.

The SVM and KNN methods are used with training and testing using cross validation (cv) 10 times and the dataset is divided into 4 large parts to make the analysis process easier. The results show that the K-Nearest Neighbor (KNN) method has a higher accuracy of >90% compared to the Support Vector Machine (SVM) method for all dataset groups. However, to make a prediction regarding the number of the same type of attack, the Support Vector Machine (SVM) model tends to be used as seen from the heatmap prediction.

The DoS/DDoS attack pattern occurs most often and the Support Vector Machine (SVM) and K-Nearest Neighbor Classifier (KNN) methods are effective in analyzing attack patterns. This data is opensource so that the training and test results can change with data updates. With this DoS/DDoS attack pattern, it is hoped that every owner of a web server-based application system published to the internet can prevent such attacks by strengthening access security on the network and system.

Keywords : *Supervised learning, Support Vector Machine (SVM), K-Nearest Neighbor Classifier (KNN), dataset, cyber security, data analysis, cyber attack analysis*

DAFTAR ISI

	Halaman
HALAMAN PENYATAAN KARYA SENDIRI	iii
HALAMAN PENGESAHAN.....	iv
KATA PENGANTAR.....	v
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS.....	vi
ABSTRAK	vii
ABSTRACT	viii
DAFTAR ISI.....	ix
DAFTAR TABEL	xii
DAFTAR GAMBAR	xiii
DAFTAR SINGKATAN.....	xvi
PERNYATAAN <i>SIMILARITY CHECK</i>	xvii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah.....	5
1.3 Tujuan Penelitian.....	5
1.4 Batasan Masalah.....	6
BAB II TINJAUAN PUSTAKA	7
2.1 State of The Art	8
2.2 Web Server	12
2.1.1 DDoS.....	12
2.1.2 <i>Phishing</i>	12
2.1.3 XSS	13
2.1.4 SQL Injection	13
2.1.5 <i>Botnet</i>	13
2.1.6 <i>Brute Force</i>	14
2.1.7 Zero Day Exploit.....	14
2.1.8 <i>Malware</i>	14

2.3	Machine Learning.....	15
2.4	Supervised Learning.....	15
2.5	Dataset.....	17
2.6	Rumus Menghitung Akurasi.....	18
2.7	Rumus Menghitung <i>Precision</i>	19
2.8	Rumus Menghitung Sensitivity (<i>Recall</i>).....	19
2.9	Rumus Menghitung F1-Score.....	19
2.10	Kaggle.....	20
2.11	<i>Python</i>	20
2.12	Tabel <i>Confusion Matrix</i>	20
2.13	<i>Heatmap</i>	21
2.14	Kerangka Teori.....	22
2.15	Metode Penelitian yang Digunakan Dalam Studi Terdahulu.....	23
2.16	Kerangka Kerja Penelitian.....	24
2.17	Rangkuman.....	26
BAB III	METODE PENELITIAN.....	27
3.1	Kerangka Penelitian.....	27
3.2	Obyek Penelitian.....	30
3.3	Alat Bantu Penelitian.....	31
3.3.1	Perangkat Keras (<i>Hardware</i>) yang akan digunakan untuk analisa.....	31
3.3.2	Perangkat Lunak (<i>Software</i>) yang akan digunakan untuk analisa.....	32
3.4	Dataset NF-UQ-NIDS-v2.....	32
3.5	Rencana dan Jadwal Penelitian.....	35
3.6	Melakukan Analisis Data dan Visualisasi.....	36
3.7	Melakukan <i>Preprocessing</i> Data.....	42
BAB IV	HASIL PENELITIAN DAN PEMBAHASAN.....	46
4.1	Data Untuk Penelitian.....	46
4.2	<i>Training</i> dengan <i>Support Vector Machine</i> (SVM).....	47
4.3	<i>Test</i> dengan <i>Support Vector Machine</i> (SVM).....	51
4.3.1	Hasil Evaluasi Model SVM.....	55
4.4	<i>Training</i> dengan <i>K-Nearest Neighbor Classifier</i> (KNN).....	71
4.5	<i>Test</i> dengan <i>K-Nearest Neighbor Classifier</i> (KNN).....	75
4.5.1	Hasil Evaluasi Model KNN.....	78

4.6	Evaluasi Hasil <i>Training</i> Tiap Model Machine Learning.....	94
4.7	Antisipasi Serangan <i>Cyber</i> Terhadap Keamanan Data.....	100
BAB V	KESIMPULAN DAN SARAN.....	101
5.1	Kesimpulan.....	101
5.2	Saran.....	102
DAFTAR PUSTAKA	103
LAMPIRAN	106



DAFTAR TABEL

	Halaman
Tabel 2.1 Daftar Jurnal Untuk Referensi Perhitungan Algoritma SVM dan KNN	8
Tabel 2.2 Tabel Range Tingkat Akurasi	18
Tabel 3.1 Kategorisasi Alat Bantu Penelitian	31
Tabel 3.2 Tabel Deskripsi Dataset	33
Tabel 3.3 Rencana dan Jadwal Penelitian	35
Tabel 3.4 Melihat Sampel Data 5 Teratas Dalam Dataset	36
Tabel 3.5 Daftar Istilah Serangan Untuk Dianalisis	39
Tabel 4.1 Daftar Hasil Training Model SVM	94
Tabel 4.2 Daftar Hasil Test Model SVM	96
Tabel 4.3 Daftar Hasil Training Model KNN	97
Tabel 4.4 Daftar Hasil Test Model KNN	99



DAFTAR GAMBAR

	Halaman
Gambar 1.1 Top 10 Anomali Serangan	2
Gambar 2.1 Algoritma K-Nearest Neighbor	16
Gambar 2.2 Algoritma Support Vector Machine	17
Gambar 2.3 Tabel Confusion Matrix	21
Gambar 2.4 Kerangka Teori.....	22
Gambar 2.5 Kerangka Kerja Penelitian.....	24
Gambar 3.1 Tabel Confusion Matrix	27
Gambar 3.2 Dataset NF-UQ-NIDS-v2 dari Kaggle	30
Gambar 3.3 Import Library	36
Gambar 3.4 Hasil Menghitung Jumlah Dataset	37
Gambar 3.5 Tipe Data Per Kolom	37
Gambar 3.6 Melihat Jumlah Baris dan Kolom di Dataset	38
Gambar 3.7 Hasil Pengecekan Data Pada Setiap Kolom	38
Gambar 3.8 Menghitung Jumlah Serangan	39
Gambar 3.9 Jumlah Serangan Dari Setiap Jenis Serangan Dengan Nama Label Attack_Class	40
Gambar 3.10 Visualisasi Daigram Batang Untuk Tipe Serangan	41
Gambar 3.11 Hasil Fitur Yang Akan Dipilih Untuk Analisis Menggunakan Machine Learning	42
Gambar 3.12 Dataset Group 1	43
Gambar 3.13 Dataset Group 2	44
Gambar 3.14 Dataset Group 3	44
Gambar 3.15 Dataset Group 4	45
Gambar 4.1 Training Model SVM Untuk Group NF-BoT-IoT-v2.....	47
Gambar 4.2 Training Model SVM Untuk Group NF-CSE-CIC-IDS2018-v2	48
Gambar 4.3 Training Model SVM Untuk Group NF-ToN-IoT-v2	49
Gambar 4.4 Training Model SVM Untuk Group NF-UNSW-NB15-v2	50
Gambar 4.5 Test Model SVM Untuk Group NF-BoT-IoT-v2	51
Gambar 4.6 Test Model SVM Untuk Group NF-CSE-CIC-IDS2018-v2	52
Gambar 4.7 Test Model SVM Untuk Group NF-ToN-IoT-v2	53
Gambar 4.8 Test Model SVM Untuk Group NF-UNSW-NB15-v2	54

Gambar 4.9 Hasil Training Metode SVM Pada Grup NF-BoT-IoT-v2	55
Gambar 4.10 Hasil Training Predicted Label Training Metode SVM Pada Grup NF-BoT-IoT-v2.....	56
Gambar 4.11 Hasil Test Metode SVM Pada Grup NF-BoT-IoT-v2.....	57
Gambar 4.12 Hasil Test Predicted Label Training Metode SVM Pada Grup NF-BoT-IoT-v2	58
Gambar 4.13 Hasil Training Metode SVM Pada Grup NF-CSE-CIC-IDS2018-v2	59
Gambar 4.14 Hasil Predicted Label Training Metode SVM Pada Grup NF-CSE-CIC-IDS2018-v2	60
Gambar 4.15 Hasil Test Metode SVM Pada Grup NF-CSE-CIC-IDS2018-v2	61
Gambar 4.16 Hasil Predicted Label Test Metode SVM Pada Grup NF-CSE-CIC-IDS2018-v2	62
Gambar 4.17 Hasil Training Metode SVM Pada Grup NF-ToN-IoT-v2	63
Gambar 4.18 Hasil Predicted Label Training Metode SVM Pada Grup NF-ToN-IoT-v2	64
Gambar 4.19 Hasil Test Metode SVM Pada Grup NF-ToN-IoT-v2	65
Gambar 4.20 Hasil Predicted Label Training Metode SVM Pada Grup NF-ToN-IoT-v2	66
Gambar 4.21 Hasil Training Metode SVM Pada Grup NF-UNSW-NB15-v2	67
Gambar 4.22 Hasil Predicted Label Training Metode SVM Pada Grup NF-UNSW-NB15-v2	68
Gambar 4.23 Hasil Test Metode SVM Pada Grup NF-UNSW-NB15-v2	69
Gambar 4.24 Hasil Predicted Label Test Metode SVM Pada Grup NF-UNSW-NB15-v2	70
Gambar 4.25 Training Model KNN Untuk Group NF-BoT-IoT-v2	71
Gambar 4.26 Training Model KNN Untuk Group NF-CSE-CIC-IDS2018-v2	72
Gambar 4.27 Training Model KNN Untuk Group NF-ToN-IoT-v2	73
Gambar 4.28 Training Model KNN Untuk Group NF-UNSW-NB15-v2	74
Gambar 4.29 Test Model KNN Untuk Group NF-BoT-IoT-v2	75
Gambar 4.30 Test Model KNN Untuk Group NF-CSE-CIC-IDS2018-v2	76
Gambar 4.31 Test Model KNN Untuk Group NF-ToN-IoT-v2.....	76
Gambar 4.32 Test Model KNN Untuk Group NF-UNSW-NB15-v2	77
Gambar 4.33 Hasil Training Metode KNN Pada Grup NF-BoT-IoT-v2.....	78
Gambar 4.34 Hasil Predicted Label Training Metode KNN Pada Grup NF-BoT-IoT-v2.....	79
Gambar 4.35 Hasil Test Metode KNN Pada Grup NF-BoT-IoT-v2.....	80
Gambar 4.36 Hasil Predicted Label Test Metode KNN Pada Grup NF-BoT-IoT-v2.....	81

Gambar 4.37 Hasil Training Metode KNN Pada Grup NF-CSE-CIC-IDS2018-v2	82
Gambar 4.38 Hasil Predicted Label Training Metode KNN Pada Grup NF-CSE-CIC-IDS2018-v2.....	83
Gambar 4.39 Hasil Test Metode KNN Pada Grup NF-CSE-CIC-IDS2018-v2	84
Gambar 4.40 Hasil Predicted Label Test Metode KNN Pada Grup NF-CSE-CIC-IDS2018-v2	85
Gambar 4.41 Hasil Training Metode KNN Pada Grup NF-ToN-IoT-v2.....	86
Gambar 4.42 Hasil Predicted Label Training Metode KNN Pada Grup NF-ToN-IoT-v2.....	87
Gambar 4.43 Hasil Test Metode KNN Pada Grup NF-ToN-IoT-v2.....	88
Gambar 4.44 Hasil Predicted Label Test Metode KNN Pada Grup NF-ToN-IoT-v2	89
Gambar 4.45 Hasil Training Metode KNN Pada Grup NF-UNSW-NB15-v2	90
Gambar 4.46 Hasil Predicted Label Training Metode KNN Pada Grup NF-UNSW-NB15-v2	91
Gambar 4.47 Hasil Test Metode KNN Pada Grup NF-UNSW-NB15-v2	92
Gambar 4.48 Hasil Predicted Label Test Metode KNN Pada Grup NF-UNSW-NB15-v2	93
Gambar 4.49 Bar Chart Daftar Hasil Training Model SVM.....	94
Gambar 4.50 Pie Chart Evaluasi Hasil Training Model SVM - Prediction Attack Matching .	95
Gambar 4.51 Bar Chart Daftar Hasil Test Model SVM.....	96
Gambar 4.52 Pie Chart Evaluasi Hasil Test Model SVM - Prediction Attack Matching	97
Gambar 4.53 Bar Chart Daftar Hasil Training Model KNN.....	98
Gambar 4.54 Pie Chart Evaluasi Hasil Training Model KNN - Prediction Attack	98
Gambar 4.55 Bar Chart Daftar Hasil Test Model KNN.....	99
Gambar 4.56 Pie Chart Evaluasi Hasil Test Model KNN - Prediction Attack Matching	100

DAFTAR SINGKATAN

CV : *Cross Validation*

NIDS : *Network Intrusion Detection System*

SVM : *Support Vector Machine*

KNN : *K-Nearest Neighbor*

DDoS : *Distributed Denial of Service*

BSSN : *Badan Siber dan Sandi Negara*

HTTP : *Hypertext Transfer Protocol*

FFN : *Fast Flux Network*

TCP : *Transmission Control Protocol*

UDP : *User Datagram Protocol*

SDN : *Software Define Network*

SQL : *Structured Query Language*

XSS : *Cross-Site Scripting*

TP : *True Positive*

FP : *False Positive*

FN : *False Negative*

TN : *True Negative*

OS : *Operating System*

CTI : *Cyber Threat Intelligence*



UNIVERSITAS
MERCU BUANA

PERNYATAAN *SIMILARITY CHECK*

Saya yang bertanda tangan di bawah ini:

Nama : HAIKAL SHIDDIQ

NIM : 55421110004

Program Studi : MAGISTER TEKNIK ELEKTRO

Judul Laporan Tesis : Perbandingan Metode Supervised Machine Learning – Support Vector Machine (SVM) dan K-Nearest Neighbor Classifier (KNN) dalam Analisis Pola Cyber Attack Pada Dataset Network Intrusion Detection System (NIDS).

Telah dilakukan *similarity check* dengan system *Turnitin* pada tanggal 18 September 2024 didapatkan nilai persentase sebesar 20%.

Jakarta, 18 September 2024

Administrasi Turnitin



Saras Nur Praticha, S.Psi, MM.