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)

TESIS

HAIKAL SHIDDIQ
55421110004

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)

TESIS

Diajukan sebagai Salah Satu Syarat untuk memperoleh gelar Magister Teknik Elektro

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	Ketua Program Studi
(Dr. Ir. Zulfa Fitri Ikatrinasari, M.T)	(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 penyususan 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

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

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*

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.