ANALISIS CICIDS2017 MENGGUNAKAN FITUR WRAPPER UNTUK KONFIGURASI FIREWALL SECARA ADAPTIVE

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer

disusun oleh

MAHMUDIN RAMDANI

19.83.0345

Kepada

PROGRAM SARJANA

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

ANALISIS CICIDS2017 MENGGUNAKAN FITUR WRAPPER UNTUK KONFIGURASI FIREWALL SECARA ADAPTIVE

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

MAHMUDIN RAMDANI

19.83.0345

Kepada

PROGRAM SARJANA

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS CICIDS2017 MENGGUNAKAN FITUR WRAPPER UNTUK KONFIGURASI FIREWALL SECARA ADAPTIVE

yang disusun dan diajukan oleh

Mahmudin Ramdani

19.83.0345

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 26 Mei 2023

Dosen Pembimbing,

Muhammad Koprawi, S.Kom., M.Eng

NIK. 190302454

HALAMAN PENGESAHAN
SKRIPSI

ANALISIS CICIDS2017 MENGGUNAKAN FITUR WRAPPER UNTUK KONFIGURASI FIREWALL SECARA ADAPTIVE

yang disusun dan diajukan oleh

Mahmudin Ramdani
19.83.0345

Telah dipertahankan di depan Dewan Penguji
pada tanggal 26 Mei 2023

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Banu Santoso, S.T., M.Eng NIK. 190302327	
Joko Dwi Santoso, M.Kom NIK. 190302181	
Muhammad Koprawi, S.Kom., M.Eng NIK. 190302454	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 26 Mei 2023

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Mahmudin Ramdani
NIM : 19.83.0345

Menyatakan bahwa Skripsi dengan judul berikut:
ANALISIS CICIDS2017 MENGGUNAKAN FITUR WRAPPER UNTUK KONFIGURASI FIREWALL SECARA ADAPTIVE

Dosen Pembimbing : Muhammad Koprawi, S.Kom., M.Eng

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

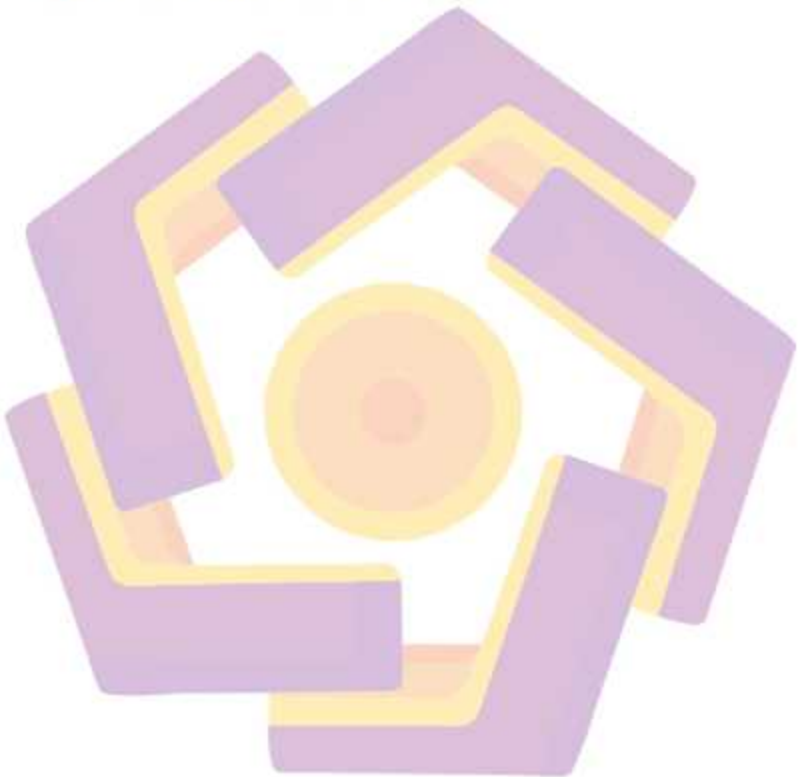
Yogyakarta, 26 Mei 2023

Yang Menyatakan,

Mahmudin Ramdani

HALAMAN PERSEMBAHAN

Alhamdulillah hirobbil alamin, puji syukur atas nikmat yang telah diberikan Allah SWT sehingga penulis dapat menyelesaikan skripsi ini. Dengan bangga saya mempersembahkan hasil Skripsi ini untuk orang tua dan saudara serta teman-teman saya yang senantiasa memberi dukungan tiada henti untuk saya serta kasih sayangnya, sehingga penulis dapat menggapai tujuan hidup dan menjalani hidup dengan penuh anugerah.



KATA PENGANTAR

Puji syukur saya panjatkan kepada Allah SWT Tuhan Yang Maha Esa, dengan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan Skripsi dengan judul: "Analisis Cicids2017 Menggunakan Fitur Wrapper Untuk Konfigurasi Firewall Secara Adaptive". Shalawat serta salam tidak lupa senantiasa dilimpahkan kepada Nabi Muhammad Shallallahu 'Alaihi Wasallam, yang telah membawa kita dari zaman jahiliyah menuju ke zaman terang benderang. Sebagai wujud rasa syukur penulis atas selesainya penulisan Skripsi ini maka penulis ingin mengucapkan terimakasih kepada:

1. Bapak Muhammad Koprawi, S.Kom., M.Eng, selaku pembimbing yang telah memberikan arahan serta bimbingan sehingga penulis mampu menyelesaikan skripsi ini.
2. Bapak Anggit Ferdita Nugraha.ST., M.Eng, sebagai teman ngobrol yang telah memberikan arahan serta bimbingan sehingga penulis mampu menyelesaikan skripsi ini.
3. Orang tua saya yang senantiasa memberikan dukungan yang tiada hentinya kepada saya.
4. Yang terakhir saya ucapkan banyak terima kasih kepada diri saya sendiri yang telah mendorong diri ini yang penuh dengan kemageran untuk dapat menyelesaikan skripsi ini pada tepat waktu.

Yogyakarta, 26 Mei 2023

Mahmudin Ramdani

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMBANG DAN SINGKATAN

ML	Machine Learning
AI	Artificial Intelligence
DT	Decision Tree
IDS	Intrusion Detection Systems
PCAP	Packet Capture
SFS	Sequential Forward Selection
BE	Backward Elimination
RFE	Recursive Feature Selection
IP	Internet Protocol
SVM	Support Vector Machines
RR	Random Forest
KNN	K Nearest Neighbor
PCA	Principal Component Analysis
IPSs	Intrusion Prevention Systems
TP	True Positif
FP	False Positif
FN	False Negatif
TN	True Negatif

INTISARI

Keamanan terbaru dalam teknologi jaringan telah membuka peluang yang sangat luar biasa untuk kerentanan system dalam sistem yang digunakan di seluruh dunia. Namun pada kenyataannya, deteksi ancaman hanyalah fungsi dasar yang memerlukan pengetahuan tambahan untuk mengotomatiskan ekstraksi data firewall. Dalam beberapa kasus dari informasi keamanan cyber menjadi pusat perhatian mengingat kerentanan ekosistem komputasi dengan sistem jaringan yang semakin beralih ke tangan peretas. Dataset yang digunakan dalam penelitian ini diambil dari Kaggle yang dimana terdapat kumpulan data CICIDS2017 berisi serangan umum yang jinak dan terbaru, yang menyerupai data dunia nyata sebenarnya sesuai dengan Packet Capture (PCAP). Ini juga mencakup hasil analisis lalu lintas jaringan menggunakan CICFlowMeter dengan arus berlabel berdasarkan stempel waktu, IP sumber dan tujuan, port sumber dan tujuan, protokol dan serangan (file CSV). Dataset ini berdasarkan periode pengambilan data dimulai pada pukul 09.00, Senin, 3 Juli 2017, dan berakhir pada pukul 17.00. pada Jumat, 7 Juli 2017, dengan total 5 hari. Penggunaan Sequential Forward Selection (SFS) sebagai fitur wrapper yang digunakan untuk mengetahui fitur paling dominan. Algoritma klasifikasi yang digunakan yakni Decision Tree untuk memecahkan permasalahan klasifikasi. Berdasarkan eksperimen yang dilakukan menggunakan CICIDS2017 adalah Intrusion Detection Evaluation Dataset dari Kaggle Repository, yang dimana kinerja tertinggi menggunakan sequential forward selection yang menghasilkan kinerja sebesar 99.88%. Dari hasil yang didapat jika bernilai 1 adalah dataset normal atau tidak terindikasi serangan sedangkan dataset yang bernilai -1 adalah dataset yang terindikasi serangan atau tidak normal. Dari hasil tersebut menunjukan klasifikasi decision tree dengan menggunakan fitur wrapper mampu berkerja secara efisien dan tepat dibandingkan hanya menggunakan klasifikasi tunggal.

Kata kunci: *Firewall, CICIDS2017, Decision Tree, Wrapper, Machine Learning*

ABSTRACT

The latest security in network technology has opened up tremendous opportunities for system vulnerabilities in systems used around the world. But in reality, threat detection is just a basic function that requires additional knowledge to automate firewall data extraction. In some cases, cyber information security takes center stage given the vulnerability of the computing ecosystem with network systems increasingly passing into the hands of hackers. The dataset used in this study was taken from Kaggle where the CICIDS2017 dataset contained the latest and benign common attacks, which resembled real-world data corresponding to Packet Capture (PCAP). It also includes the results of network traffic analysis using CICFlowMeter with flows labeled based on timestamp, source and destination IP, source and destination ports, protocols and attacks (CSV file). This data set is based on the data collection period starting at 09.00, Monday, July 3, 2017, and ending at 17.00, on Friday, July 7, 2017, for a total of 5 days. The use of Sequential Forward Selection (SFS) as a wrapper feature is used to determine the most dominant features. The classification algorithm used is the Decision Tree to solve classification problems. Based on experiments conducted using CICIDS2017 is the Intrusion Detection Evaluation Dataset from Kaggle Repository, where the highest performance uses sequential forward selection which results in a performance of 99.88%. From the results obtained if the value of 1 is a normal dataset or not indicated by attack while the dataset with a value of -1 is a dataset that is indicated by attack or abnormal. From these results, it shows that decision tree classification using the wrapper feature is able to work efficiently and precisely compared to only using a single classification.

Keyword: Firewall, CICIDS2017, Decision Tree, Wrapper, Machine Learning