DETEKSI SERANGAN *MALWARE* MENGGUNAKAN METODE *SUPPORT VECTOR MACHINE*

SKRIPSI

Disusun Oleh :

Hery Sanjaya Simbolon

210210069

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK DAN KOMPUTER

UNIVERSITAS PUTERA BATAM

2025

DETEKSI SERANGAN *MALWARE* MENGGUNAKAN METODE *SUPPORT VECTOR MACHINE*

SKRIPSI

Untuk memenuhi salah satu syarat

memperoleh gelar Sarjana

Disusun Oleh :

Hery Sanjaya Simbolon

210210069

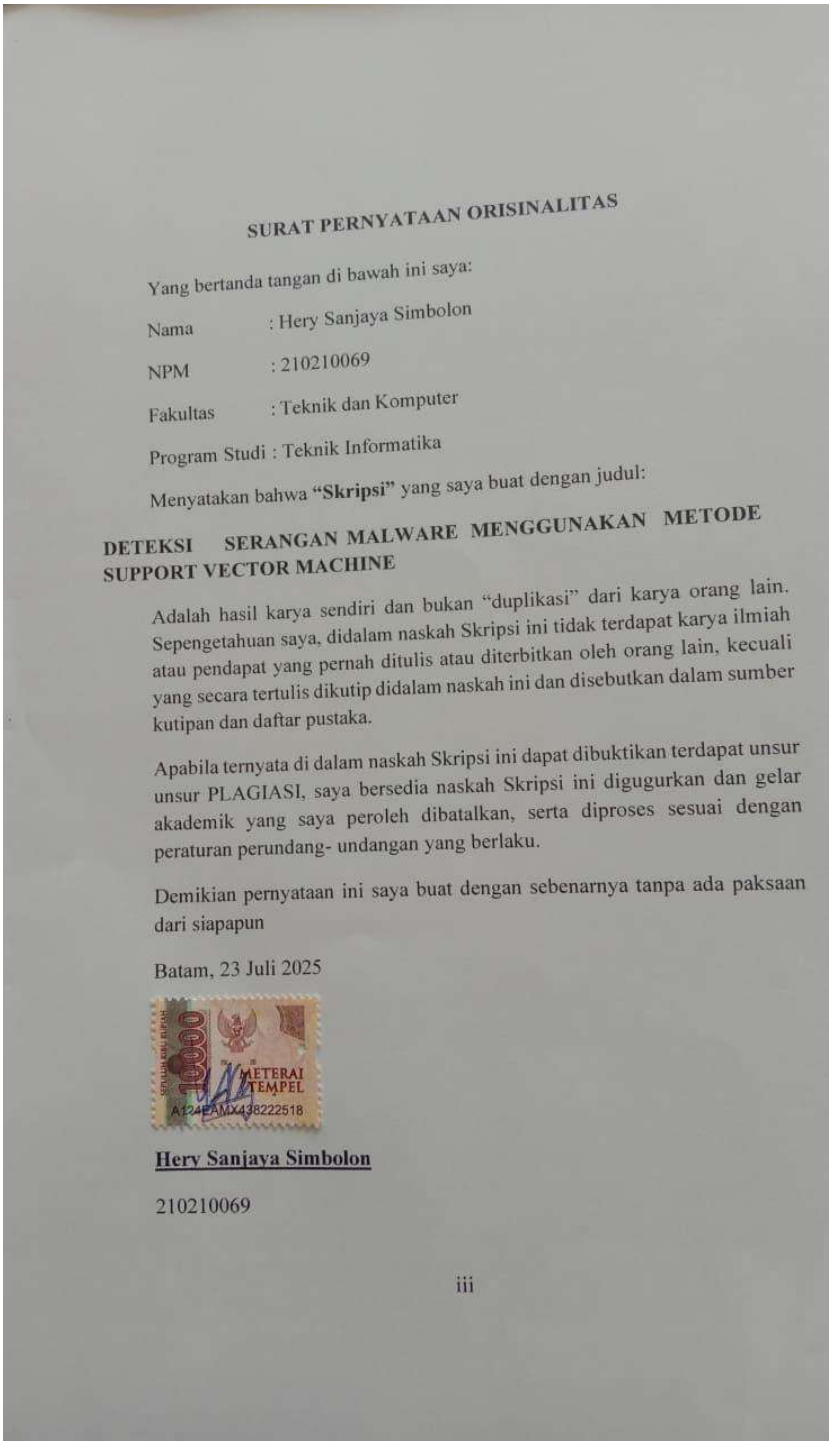
PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK DAN KOMPUTER

UNIVERSITAS PUTERA BATAM

20

SURAT PERNYATAAN ORISINALITAS



SURAT PERNYATAAN ORISINALITAS

Yang bertanda tangan di bawah ini saya:

Nama : Hery Sanjaya Simbolon

NPM : 210210069

Fakultas : Teknik dan Komputer

Program Studi : Teknik Informatika

Menyatakan bahwa **"Skripsi"** yang saya buat dengan judul:

DETEKSI SERANGAN MALWARE MENGGUNAKAN METODE SUPPORT VECTOR MACHINE

Adalah hasil karya sendiri dan bukan "duplikasi" dari karya orang lain. Sepengetahuan saya, didalam naskah Skripsi ini tidak terdapat karya ilmiah atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip didalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata di dalam naskah Skripsi ini dapat dibuktikan terdapat unsur unsur PLAGIASI, saya bersedia naskah Skripsi ini digugurkan dan gelar akademik yang saya peroleh dibatalkan, serta diproses sesuai dengan peraturan perundang- undangan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenarnya tanpa ada paksaan dari siapapun

Batam, 23 Juli 2025

Hery Sanjaya Simbolon

210210069

iii

HALAMAN PENGESAHAN

DETEKSI SERANGAN MALWARE MENGGUNAKAN METODE SUPPORT VECTOR MACHINE

HALAMAN PENGESAHAN

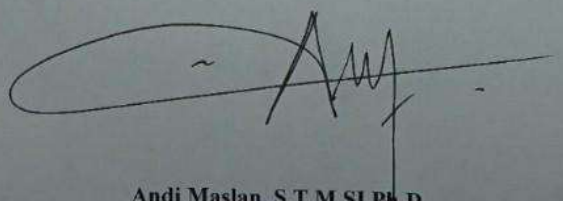
SKRIPSI

Untuk memenuhi salah satu syarat memproleh gelar sarjana

Oleh
Hery Sanjaya Simbolon
210210069

Telah disetujui oleh Pembimbing pada tanggal

Batam, 23 Juli 2025



Andi Maslan, S.T,M.SI,Ph.D.
Pembimbing

ABSTRAK

Pengembangan teknologi informasi yang pesat telah meningkatkan potensi ancaman terhadap keamanan sistem, salah satunya adalah serangan malware. Malware adalah perangkat lunak berbahaya yang memiliki kemampuan untuk mengganggu, merusak, atau mencuri data sistem komputer tanpa pengetahuan pengguna. Untuk mencegah kerusakan lebih lanjut pada sistem, deteksi aktivitas malware menjadi sangat penting. Tujuan dari penelitian ini adalah untuk membuat model klasifikasi yang dapat mengidentifikasi serangan malware berdasarkan perilaku proses sistem operasi saat menggunakan metode Support Vector Machine (SVM). Dataset yang digunakan memiliki 100.000 entri data yang memiliki 33 atribut yang menunjukkan aktivitas proses seperti penggunaan CPU, memori, dan konteks pergeseran. Pembagian data menjadi data latih dan data uji, analisis data exploratory (EDA) untuk memahami karakteristik data, preprocessing data untuk membersihkan dan menstandarisasi atribut, seleksi fitur berdasarkan korelasi untuk mengurangi kompleksitas model, dan pengembangan dan pelatihan model klasifikasi menggunakan SVM dengan kernel linear. Menggunakan confusion matrix dan metrik evaluasi seperti akurasi, precision, recall, dan skor F1, model dievaluasi. Hasil pengujian menunjukkan bahwa model SVM yang dibangun memiliki performa yang sangat baik dengan akurasi sebesar 99,57%, ketepatan sebesar 99,76%, recall sebesar 99,38%, dan skor F1 sebesar 99,57%. Model ini juga memiliki kemampuan untuk membedakan proses yang merupakan malware dari proses normal dengan jumlah kesalahan klasifikasi yang sangat kecil. Hasilnya menunjukkan bahwa SVM dapat melakukan deteksi malware berbasis perilaku proses sistem dengan cukup baik. Penelitian ini dapat berkontribusi pada pengembangan sistem keamanan otomatis yang dapat mendeteksi ancaman secara real-time dan membantu memperkuat pertahanan sistem terhadap serangan siber.

***Kata kunci**: Malware, SVM, Klasifikasi, Security, Cyber*

ABSTRACT

The rapid development of information technology has increased the potential for threats to system security, one of which is malware attacks. Malware is malicious software that has the ability to disrupt, damage, or steal computer system data without user knowledge. To prevent further damage to the system, malware activity detection is very important. The purpose of this study is to create a classification model that can identify malware attacks based on the behavior of operating system processes when using the Support Vector Machine (SVM) method. The dataset used has 100,000 data entries that have 33 attributes that indicate process activity such as CPU usage, memory, and context shifts. Data is divided into training data and test data, exploratory data analysis (EDA) to understand data characteristics, data preprocessing to clean and standardize attributes, feature selection based on correlation to reduce model complexity, and development and training of a classification model using SVM with a linear kernel. Using a confusion matrix and evaluation metrics such as accuracy, precision, recall, and F1 score, the model is evaluated. Test results show that the developed SVM model performed very well, with an accuracy of 99.57%, a precision of 99.76%, a recall of 99.38%, and an F1 score of 99.57%. This model also distinguished malware processes from normal processes with a very small number of misclassifications. The results indicate that SVM can perform malware detection based on the behavior of system processes quite well. This research can contribute to the development of automated security systems that can detect threats in real time and help strengthen system defenses against cyberattacks.

***Keywords**: Malware, SVM, Classification, Security, Cyber*

KATA PENGANTAR

Puji syukur kita panjatkan kepada Tuhan Yang Maha Esa atas Rahmat-Nya yang dianugrahkan kepada kita karena penulis telah berhasil menyelesaikan Skripsi dengan judul "Deteksi Serangan Malware Menggunakan Metode Metode Support Vector Machine".Penyusunan Skripsi ini diciptakan untuk sebagai salah satu syarat untuk memperoleh gelar pada Universitas Putera Batam. Selain itu, penulis juga menyadari bahwa Skripsi ini masih terdapat kekurangan dan jauh dari kata sempuran, Oleh karena itu, penulis merima banyak bimbingan dan saran dari beberapa pihak.

Oleh sebab itu, penulis ingin menyampaikan ucapan terima kasih dengan segala kerendahan hati kepada :

1. Rektor Universitas Putera Batam, Ibu Dr. Nur Elfi Husda, S.Kom.,M.SI.
2. Dekan Fakultas Teknik dan Komputer, Bapak Welly Sugianto, S.T.,M.M., Ph.D
3. Ketua Program Studi Teknik Informatika Bapak Andi Maslan,.S.T.,M.SI., Ph.D Sekaligus sebagai dosen Pembimbing Skripsi
4. Ibu Alfannisa Annurullah Fajrin, S.Kom, M.Kom. Sebagai dosen pembimbing akademik.
5. Dosen dan Staff Universitas Putera Batam
6. Kedua orang tua penulis yang senantiasa mendukung penulis selama kegiatan perkuliahan.

7. Teman-teman penulis yang juga senantiasa mendukung penulis selama kegiatan perkuliahan

Batam, 23 Juli 2025

Hery Sanjaya Simbolon

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR RUMUS


UPB
Universitas Putera Batam