PENGEMBANGAN MODEL MACHINE LEARNING UNTUK DETEKSI ANOMALI DAN SERANGAN PADA JARINGAN KOMPUTER

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi S1 INFORMATIKA

disusun oleh

ERMAN SAPUTRA

21.11.3859

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

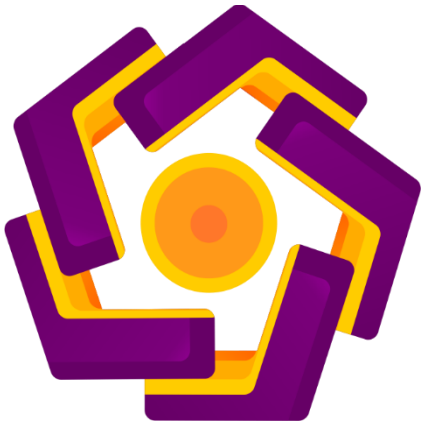
2025

PENGEMBANGAN MODEL MACHINE LEARNING UNTUK DETEKSI ANOMALY DAN SERANGAN PADA JARINGAN KOMPUTER

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi S1 INFORMATIKA



disusun oleh

ERMAN SAPUTRA

21.11.3859

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

HALAMAN PERSETUJUAN

SKRIPSI

PENGEMBANGAN MODEL MACHINE LEARNING UNTUK DETEKSI ANOMALY DAN SERANGAN PADA JARINGAN KOMPUTER

yang disusun dan diajukan oleh

Nama Mahasiswa

Erman Saputra

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 22 Juli 2025

Dosen Pembimbing,

Hanafi, S.Kom., M.Eng., Ph.D.
NIK. 190302024

HALAMAN PENGESAHAN

SKRIPSI

PENGEMBANGAN MODEL MACHINE LEARNING UNTUK DETEKSI ANOMALY DAN SERANGAN PADA JARINGAN KOMPUTER

yang disusun dan diajukan oleh

Nama Mahasiswa

Erman Saputra

Telah dipertahankan di depan Dewan Penguji
pada tanggal 22 Juli 2025

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Bayu Setiaji, M.Kom. **NIK. 190302216**	
Bambang Pilu Hartato S.Kom., M.Eng. **NIK. 190302707**	
Hanafi, S.Kom., M.Eng., Ph.D.D **NIK. 190302024**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 22 Juli 2025

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Erman Saputra
NIM : 21.11.3859

Menyatakan bahwa Skripsi dengan judul berikut:

Tuliskan Judul Skripsi

Dosen Pembimbing : Hanafi, S.Kom., M.Eng., Ph.D.

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, 22 Juli 2025

Yang Menyatakan,

Nama Mahasiswa

HALAMAN PERSEMBAHAN
KATA PENGANTAR

Alhamdulillah, puji syukur penulis panjatkan ke hadirat Allah SWT, karena atas limpahan rahmat, taufik, dan hidayah-Nya, penulis dapat menyelesaikan skripsi yang berjudul: "PENGEMBANGAN MODEL MACHINE LEARNING UNTUK DETEKSI ANOMALI DAN SERANGAN PADA JARINGAN KOMPUTER". Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik Komputer pada Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta.Ucapan terima kasih penulis:

1. Allah SWT, atas segala nikmat, kemudahan, dan kekuatan yang diberikan selama proses penyusunan skripsi ini.
2. Prof. Dr. M. Suyanto, M.M., selaku Rektor Universitas Amikom Yogyakarta.
3. Hanafi, S.Kom., M.Eng., Ph.D, selaku dosen pembimbing yang telah memberikan bimbingan, arahan, dan masukan yang sangat berarti selama proses pengerjaan skripsi.
4. Kedua orang tua dan keluarga tercinta, atas segala doa, dukungan moral dan materi, serta semangat yang selalu menyertai setiap langkah penulis
5. Teman-teman terdekat: Cahyo Pamungkas, Purnama Sari, Romiza Farrel, dan Kevin , atas motivasi, bantuan, dan kebersamaannya selama proses ini.
6. Teman-teman IF01, atas kebersamaan, motivasi, dan bantuan yang diberikan selama masa studi dan penyusunan skripsi ini.

Penulis menyadari bahwa skripsi ini masih memiliki kekurangan. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan. Semoga karya ini dapat memberikan manfaat, khususnya dalam bidang keamanan jaringan komputer.

Yogyakarta, 16 Juli 2025

Penulis

DAFTAR ISI

(gunakan tools table of content pada menu references di Word)

Daftar Isi

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR LAMBANG DAN SINGKATAN

ML	: Machine Learning
LR	: Logistic Regression
RF	: Random Forest
KNN	: K-Nearest Neighbors
IDS	: Intrusion Detection System
NSL-KDD	: Network Security Layer – Knowledge Discovery in Database
UNSW-NB15	: University of New South Wales – Network Botnet
AI	: Artificial Intelligence
SVM	: Support Vector Machines
NB	: Naïve Bayes

DAFTAR ISTILAH

Pearson Correlation	: Mengukur hubungan dua variable
Dataset	: Kumpulan semua data yang digunakan
Preprocessing	: Tahap persiapan data seblum masuk ke model
Cross-Validation	: Teknik uji model yang lebih andal untuk performa umum
Metrik Evaluasi	: Ukuran untuk menilai kinerja model
SMOTETomek	: Teknik penyeimbangan data
GridSearchCV	: Cari kombinasi parameter terbaik
Machine Learning	: Pembelajaran mesin dari data
Model	: Hasil dari proses training
Training	: Proses mengajari model dengan cara memberi data
Testing	: Proses menguji performa akhir model
Feature	: Atribut yang digunakan untuk membuat prediksi
Label	: Nilai output yang ingin kita prediksi
Overfitting	: Kondisi Ketika model terlalu hafal dengan data latih
Underfitting	: Kondisi Ketika model terlalu sederhana
Trade-off	: Mengorbankan satu hal untuk mendapatkan hal lain

INTISARI

Keamanan jaringan komputer semakin penting seiring dengan meningkatnya jumlah perangkat dan kompleksitas infrastruktur jaringan. Serangan seperti *Denial of Service (DoS), Remote to Local (R2L), User to Root (U2R),* dan *Probe* menjadi ancaman serius yang perlu dideteksi sedini mungkin. Metode deteksi tradisional berbasis *signature* memiliki keterbatasan dalam menghadapi serangan baru yang belum terdokumentasi. Oleh karena itu, pendekatan berbasis *heuristic-based* digunakan untuk mendeteksi anomali secara proaktif.

Penelitian ini menggunakan lima algoritma *Machine Learning*, yaitu *Logistic Regression*, *Random Forest, Support Vector Machine (SVM), Naïve Bayes, dan K-Nearest Neighbors (KNN)* untuk mengidentifikasi serangan siber. Dua dataset yang digunakan adalah *NSL-KDD* dan *UNSW-NB15* yang mencerminkan berbagai jenis serangan dan lalu lintas jaringan. Proses penelitian mencakup pra-pemrosesan data, pembagian data, penyeimbangan data menggunakan *SMOTETomek*, pelatihan model, dan optimasi dengan *GridSearchCV*.

Pada *NSL-KDD biner*, Akurasi *Random Forest* mencapai 100%, *SVM* 99%, *KNN* 100% dengan recall 99%, *Logistic Regression* 95%, dan *Naive Bayes* 89%. Pada *UNSW-NB15* biner, *Random Forest* 99%, *KNN* 97%, *SVM* 96%, *Logistic Regression* 95%, dan *Naive Bayes* 90%. Untuk multi-kelas *NSL-KDD*, Akurasi *Random Forest* 100%, *SVM* 99%, *KNN* 99%, *Logistic Regression* 94%, dan *Naive Bayes* 74%. Pada multi-kelas *UNSW-NB15*, *Random Forest* 85%, *KNN* 81%, *SVM* 77%, *Logistic Regression* 73%, dan *Naive Bayes* 60%. Hasil ini menunjukkan *Random Forest* sebagai model paling andal untuk pengembangan sistem deteksi dini serangan jaringan.

Kata kunci: Machine Learning, Deteksi Anomali, Serangan Siber, NSL-KDD, UNSW-NB15

ABSTRACT

The importance of computer network security is increasing along with the rise of connected devices and network complexity. Attacks such as Denial of Service (DoS), Remote to Local (R2L), User to Root (U2R), and Probe pose serious threats that must be detected early. Traditional signature-based detection methods are limited in identifying new and undocumented threats. Therefore, a heuristic-based approach is proposed to detect anomalies proactively.

This study employs five Machine Learning algorithms: Support Vector Machine (SVM), Random Forest, Naïve Bayes, K-Nearest Neighbors (KNN), and Logistic Regression to identify cyber attacks. Two datasets, NSL-KDD and UNSW-NB15, are used due to their variety of attack types and network traffic representation. The methodology includes data preprocessing, data splitting, class balancing with SMOTETomek, model training, and optimization using GridSearchCV.

In NSL-KDD binary, accuracy Random Forest achieved 100%, SVM 99%, KNN 100% with 99% recall, Logistic Regression 95%, and Naive Bayes 89%. In UNSW-NB15 binary, Random Forest reached 99%, KNN 97%, SVM 96%, Logistic Regression 95%, and Naive Bayes 90%. For NSL-KDD multi-class, Random Forest obtained 100%, SVM 99%, KNN 99%, Logistic Regression 94%, and Naive Bayes 74%. In UNSW-NB15 multi-class, accuracy Random Forest scored 85%, KNN 81%, SVM 77%, Logistic Regression 73%, and Naive Bayes 60%. These results highlight Random Forest as the most reliable model for developing early intrusion detection systems.

.

Keyword**:** Machine Learning, Anomaly Detection, Cyber Attack, NSL-KDD, UNSW-NB15