SISTEM ANALISIS DAN KLASIFIKASI RISIKO MALICIOUS TRAFFIC PADA LOG HONEYPOT MENGGUNAKAN ALGORITMA RANDOM FOREST

FARHANI AMANAH

NIM. 2210511021

PROGRAM STUDI S1 INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA

JAKARTA

2026

SISTEM ANALISIS DAN KLASIFIKASI RISIKO MALICIOUS TRAFFIC PADA LOG HONEYPOT MENGGUNAKAN ALGORITMA RANDOM FOREST

FARHANI AMANAH

NIM. 2210511021

SKRIPSI

Diajukan Sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Komputer

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA

JAKARTA

2026

LEMBAR PERNYATAAN ORISINALITAS

PERNYATAAN ORISINALITAS

Tugas Akhir ini adalah hasil karya sendiri dan semua sumber baik yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Farhani Amanah

NIM : 2210511021

Tanggal : 26 Juli 2026

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 26 Juli 2026

Yang Menyatakan,

Farhani Amanah

Dipindai dengan CamScanner

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademika Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan di bawah ini :

Nama : Farhani Amanah

NIM : 2210511021

Fakultas : Ilmu Komputer

Program Studi : S1 Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non eksklusif (Non-exclusive Royalty Free Right) atas skripsi saya yang berjudul :

SISTEM ANALISIS DAN KLASIFIKASI RISIKO MALICIOUS TRAFFIC PADA LOG HONEYPOT MENGGUNAKAN ALGORITMA RANDOM FOREST

Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/memformatkan, mengelola dalam bentuk pangkalan data (basis data), merawat dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di Jakarta
Pada tanggal 26 Juli 2026
Yang Menyatakan,

Farhani Amanah

Dipindai dengan CamScanner

LEMBAR PERSETUJUAN SIDANG

LEMBAR PERSETUJUAN

Yang bertanda tangan di bawah ini:

Nama	: Farhani Amanah
NIM	: 2210511021
Program Studi	: Informatika Program Sarjana/~~Sistem Informasi Program Sarjana/Sains Data Program Sarjana/Sistem Informasi Program Diploma~~ (*Coret yang tidak perlu)
Judul Tugas Akhir	: Sistem Analisis dan Klasifikasi Risiko Malicious Traffic pada Log Honeypot menggunakan Algoritma Random Forest

Dinyatakan telah memenuhi syarat dan menyetujui untuk mengikuti ujian sidang Tugas Akhir.

Jakarta, 2026

Menyetujui,

Dosen Pembimbing I,	Dosen Pembimbing II,
Prof. Dr. Ir. Supriyanto, M.Sc., IPM.	Kharisma Wiati Gusti, M.T.
NIP. 197605082003121002	NIP. 199006192022032007

Mengetahui,
Koordinator Program Studi,

Dr. Ridwan Raafi'udin, M.Kom.
NIP. 198805022021211001

CS Dipindai dengan CamScanner

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

Judul	:	Sistem Analisis dan Klasifikasi Risiko Malicious Traffic pada Log Honeypot Menggunakan Algoritma Random Forest
Nama	:	Farhani Amanah
NIM	:	2210511021

Disetujui oleh :

Penguji 1:
Dr. Widya Cholil, M.I.T.

Penguji 2:
Anis Fitri Nur Masruriyah, S.Kom., M.Kom.

Pembimbing 1:
Prof. Dr. Ir. Supriyanto, S.T., M.Sc., IPM.

Pembimbing 2:
Kharisma Wiati Gusti, S.T., M.T.

Diketahui oleh:

Koordinator Program Studi:
Dr. Ridwan Raafi'udin, S.Kom., M.Kom.
NIP. 198805022021211001

Dekan Fakultas Ilmu Komputer
Prof. Dr. Ir. Supriyanto, S.T., M.Sc., IPM.
NIP. 197605082003121002

Tanggal Ujian Tugas Akhir
9 Juli 2026

Dipindai dengan CamScanner

ABSTRAK

Semakin meningkatnya ancaman siber mengakibatkan jumlah dan kompleksitas *malicious traffic* yang terekam di *honeypot* semakin tinggi sehingga diperlukan mekanisme analisis yang dapat mengidentifikasi tingkat risiko serangan secara terukur. Penelitian ini bertujuan membangun sistem analisis dan klasifikasi risiko *malicious traffic* pada log *honeypot* menggunakan algoritma *Random Forest*. Dataset yang digunakan berasal dari log *Honeypot* yang merekam aktivitas autentikasi dan interaksi penyerang. Tahapan penelitian meliputi *preprocessing data*, *feature engineering*, pembentukan label risiko menggunakan *pseudo labeling* berdasarkan *framework MITRE ATT&CK* dan *NIST SP* 800-30, penanganan ketidakseimbangan data menggunakan *Synthetic Minority Oversampling Technique (SMOTE)*, serta evaluasi model menggunakan *Stratified* 5-*Fold Cross Validation.* Hasil penelitian menunjukkan bahwa model *Random Forest* mampu mengklasifikasikan *malicious traffic* ke dalam kategori *Low Risk* dan *High Risk* dengan nilai *accuracy* sebesar 99,40%, *precision* sebesar 95,28%, *recall* sebesar 99,02%, *F1-score* sebesar 97,12%, dan *ROC-AUC* sebesar 99,95%. Selanjutnya model diimplementasikan ke dalam dashboard berbasis web untuk menampilkan hasil analisis, klasifikasi risiko, attack indication, dan security recommendation secara interaktif. Hasil penelitian menunjukkan bahwa kombinasi log *honeypot* dan *Random Forest* efektif digunakan untuk mendukung analisis risiko ancaman siber berdasarkan karakteristik perilaku serangan.

Kata kunci: *malicious traffic, honeypot, Random Forest,* klasifikasi risiko*,* keamanan siber

ABSTRACT

The increasing volume and sophistication of cyber threats have resulted in a growing amount of malicious traffic recorded by honeypots, creating the need for a mechanism capable of identifying attack risk levels in a measurable manner. This study aims to develop a risk analysis and classification system for malicious traffic based on honeypot logs using the Random Forest algorithm. The dataset was obtained from honeypot logs that record authentication activities and attacker interactions. The research process consisted of data preprocessing, feature engineering, risk label generation using pseudo labeling based on the MITRE ATT&CK framework and NIST SP 800-30, data balancing using the Synthetic Minority Oversampling Technique (SMOTE), and model evaluation through Stratified 5-Fold Cross Validation. The results show that the Random Forest model successfully classified malicious traffic into Low Risk and High Risk categories, achieving an accuracy of 99,40%, precision of 95,28%, recall of 99,02%, F1-score of 97,12%, and ROC-AUC of 99,95%. The model was subsequently implemented in a web-based dashboard to provide interactive analysis results, risk classification, attack indications, and security recommendations. These findings demonstrate that the combination of honeypot logs and Random Forest is effective in supporting cyber threat risk analysis based on attack behavior characteristics.

Keywords: malicious traffic, honeypot, Random Forest, risk classification, cybersecurity

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR RUMUS

DAFTAR LAMPIRAN

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa, atas segala rahmat-Nya sehingga Tugas Akhir ini berhasil diselesaikan. Tugas Akhir ini dilakukan dalam bentuk Skripsi. Tugas Akhir ini dilakukan sejak bulan September 2025 sampai bulan April 2026 dengan judul "Sistem Analisis dan Klasifikasi Risiko *Malicious Traffic* Pada Log *Honeypot* menggunakan Algoritma *Random Forest*".

Terima kasih penulis ucapkan kepada:

1. Bapak Hasan Basri dan Ibu Fatimah Zahara selaku Ayah dan Bunda dari penulis yang senantiasa memberikan *effort* yang sangat luar biasa kepada penulis, dukungan moral, doa, serta motivasi yang tiada henti.
2. Bapak Prof. Dr. Ir. Supriyanto, M.Sc., IPM. selaku Dekan Fakultas Ilmu Komputer sekaligus dosen pembimbing, dan Ibu Kharisma Wiati Gusti, M.T. selaku dosen pembimbing yang telah memberikan arahan, bimbingan, dan saran kepada penulis selama proses penyusunan skripsi ini.
3. Bapak Dr. Ridwan Raafi'udin, S.Kom, M.Kom. selaku Ketua Program Studi Informatika.
4. Bapak Basuki Erwin Setiyadi, S.S.T.TP., M.Si. selaku narasumber dari Direktorat Operasi Keamanan Siber (D21) Badan Siber dan Sandi Negara (BSSN), serta Badan Siber dan Sandi Negara (BSSN) yang telah memberikan tanggapan, informasi, dan jawaban atas pertanyaan penelitian yang diajukan penulis sehingga dapat mendukung penyusunan skripsi ini.

Semoga Tugas Akhir ini bermanfaat bagi pihak yang membutuhkan dan bagi kemajuan ilmu pengetahuan.

Jakarta, 26 Juli 2026

Farhani Amanah