



**RANCANGAN DAN ANALISIS KINERJA HONEYPOT
UNTUK KEAMANAN JARINGAN MENGGUNAKAN
ALGORITMA KNN**

**TUGAS AKHIR
SKRIPSI**

GREGORIAN IVOLITO RAMADHANI SANDA

41521010068

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2026**



**RANCANGAN DAN ANALISIS KINERJA HONEYPOT
UNTUK KEAMANAN JARINGAN MENGGUNAKAN
ALGORITMA KNN**

**TUGAS AKHIR
SKRIPSI**

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana

**GREGORIAN IVOLITO RAMADHANI SANDA
41521010068**

**UNIVERSITAS
MERCU BUANA**

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2026**

HALAMAN PERNYATAAN KARYA SENDIRI

Saya yang bertanda tangan di bawah ini:

Nama : Gregorian Ivolito Ramadhani Sanda

NIM : 41521010068

Fakultas/Program Studi : Fakultas Ilmu Komputer / Teknik Informatika

Menyatakan dengan sebenar-benarnya bahwa Tugas Akhir berjudul:

“Rancangan Dan Analisis Kinerja Honeypot Untuk Keamanan Jaringan Menggunakan Algoritma KNN” adalah hasil karya saya sendiri, tidak mengandung unsur plagiarisme, pelanggaran hak cipta, atau konten ilegal dalam bentuk apapun dan tidak melanggar hukum atau hak pihak manapun.

Apabila di kemudian hari ditemukan pelanggaran terhadap pernyataan ini, saya bersedia menanggung seluruh konsekuensi hukum dan membebaskan Universitas Mercu Buana dari segala bentuk tuntutan hukum dan saya siap mendapatkan sanksi akademis yang berlaku di Universitas Mercu Buana.

Demikian pernyataan ini saya buat dengan sebenar-benarnya untuk digunakan sebagaimana mestinya.

UNIVERSITAS
MERCU BUANA

Jakarta, 18 Agustus 2026



Gregorian Ivolito Ramadhani Sanda

PERNYATAAN SIMILARITY CHECK
/SIMILARITY CHECK STATEMENT

Saya yang bertanda tangan dibawah ini menyatakan, bahwa karya ilmiah yang ditulis oleh
/The undersigned, hereby declare that the scientific work written by

Nama /Name : GREGORIAN IVOLITO RAMADHANI
SANDA
NIM /Student ID Number : 41521010068
Program Studi /Study Program : Teknik Informatika

Dengan Judul Tugas Akhir

/The title:

“RANCANGAN DAN ANALISIS KINERJA HONEYPOT UNTUK KEAMANAN JARINGAN MENGGUNAKAN ALGORITMA KNN”

telah dilakukan pengecekan *similarity* dengan sistem Turnitin pada tanggal:

/Similarity checks have been carried out with the Turnitin system on the date:

22 Agustus 2026

dengan nilai persentase sebesar :

/with a percentage value of:

30%

dinyatakan memenuhi standar sesuai dengan ketentuan berlaku di **Fakultas Ilmu Komputer** Universitas Mercu Buana. */declared to meet standards in accordance with applicable regulations at the Faculty of Computer Science, Universitas Mercu Buana.*

File hasil cek similarity turnitin:

/Turnitin similarity report file

https://drive.google.com/file/d/1EZ5uuNlnPnqbKKSOQr4bMFb9i-0XlrDf/view?usp=drive_link



Jakarta, 22 Agustus 2026
Admin Turnitin Fasilkom UMB



Agung Prawoto

Agung Prawoto, S.Kom., B.Sc

NIK : 322970503

Fakultas Ilmu Komputer

KAMPUS MENARA BHAKTI

Jl. Raya Meruya Selatan No. 1 Kembangan, Jakarta Barat 11650

Telp. 021-5840816 (Hunting), Psw : 5700 Fax. 021-5840813

<http://www.mercubuana.ac.id>, e-mail : fasilkom@mercubuana.ac.id

HALAMAN PENGESAHAN

Tugas Akhir ini diajukan oleh:

Nama : GREGORIAN IVOLITO RAMADHANI SANDA
NIM : 41521010068
Fakultas/Program Studi : Fakultas Ilmu Komputer / Teknik Informatika
Judul Tugas Akhir : Rancangan dan Analisis Kinerja Honeypot Untuk
Keamanan Jaringan Menggunakan Algoritma KNN

Telah berhasil dipertahankan pada sidang tanggal 18 Agustus 2026 dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer Universitas Mercu Buana.

Disahkan oleh:

Dosen Pembimbing



Saruni Dwiasnati, ST, MM, M.Kom
NIDN/NUPTK: 0325128802

Jakarta, 18 Agustus 2026
Mengetahui,

Dekan Fakultas Ilmu Komputer

Ketua Program Studi
Teknik Informatika



MERCU BUANA

Dr. Bambang Jokonowo, S.Si., MTI
NIDN/NUPTK: 0320037002

Dr. Hadi Santoso, S.Kom., M.Kom
NIDN/NUPTK: 0225067701

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan Tugas Akhir ini. Penulisan Tugas Akhir ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Teknik Informatika pada Fakultas Ilmu Komputer Universitas Mercu Buana. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan Tugas Akhir ini, sangatlah sulit bagi saya untuk menyelesaikan Tugas Akhir ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Andi Adriansyah, M.Eng. selaku Rektor Universitas Mercu Buana.
2. Bapak Dr. Bambang Jokonowo, S.Si., MTI selaku Dekan Fakultas Ilmu Komputer.
3. Bapak Dr. Hadi Santoso, S.Kom., M.Kom. selaku Ketua Program Studi Teknik Informatika Universitas Mercu Buana.
4. Ibu Saruni Dwiasnati, ST, MM, M.Kom selaku dosen pembimbing TA yang telah memberikan pengarahan, motivasi, menyediakan waktu, tenaga, dan pikiran sehingga selama pembuatan proposal penelitian ini terjadwal dengan baik.
5. Kedua Orang Tua saya yang selalu mensupport dan mendukung saya selama menjalani masa studi sebagai mahasiswa Universitas Mercubuana.
6. Semua Teman di Pusat Pelatihan Kerja Daerah Jakarta Pusat yang selalu peduli dan mendukung saya selama ini
7. Semua teman kuliah yang selalu berbagi informasi dan memberikan dukungan dalam bentuk yang berbeda-beda.

Akhir kata, saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga Tugas Akhir ini membawa manfaat bagi pengembangan ilmu.

Jakarta, 18 Agustus 2026

Gregorian Ivolito Ramadhani Sanda

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR DI REPOSITORI UMB

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR DI REPOSITORI UMB

Sebagai sivitas akademik Universitas Mercu Buana, saya yang bertanda tangan di bawah ini:

Nama : Gregorian Ivolito Ramadhani Sanda
NIM : 41521010068
Fakultas/Program Studi : Fakultas Ilmu Komputer / Teknik Informatika
Judul Laporan Skripsi : Rancangan Dan Analisis Kinerja Honeypot Untuk
Keamanan Jaringan Menggunakan Algoritma KNN

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 Tugas Akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

UNIVERSITAS
MERCU BUANA

Jakarta, 18 Agustus 2026

Yang menyatakan,



Gregorian Ivolito Ramadhani Sanda

RANCANGAN DAN ANALISIS KINERJA HONEYPOT UNTUK KEAMANAN JARINGAN MENGGUNAKAN ALGORITMA KNN

GREGORIAN IVOLITO RAMADHANI SANDA

ABSTRAK

keamanan siber menjadi salah satu aspek kritis dalam era digital yang terus berkembang. Serangan cyber semakin canggih dan beragam, sehingga diperlukan metode deteksi dini untuk mengidentifikasi ancaman sebelum menyebabkan kerusakan. Semakin pesatnya perkembangan teknologi digital diikuti dengan meningkatnya risiko serangan siber yang dapat mengganggu stabilitas dan keamanan sistem jaringan. Serangan seperti DDoS, brute force, hingga penyebaran malware menjadi tantangan yang nyata bagi berbagai sektor. Dalam menghadapi situasi ini, honeypot hadir sebagai pendekatan strategis yang mampu memancing serangan untuk kemudian dianalisis tanpa mengganggu sistem utama. Penelitian ini bertujuan untuk mengeksplorasi efektivitas honeypot dalam mengidentifikasi pola serangan, yang kemudian dianalisis menggunakan algoritma K-Nearest Neighbor (KNN) untuk mengelompokkan jenis-jenis serangan yang terekam. Proses simulasi dilakukan dalam lingkungan virtual menggunakan sistem operasi Ubuntu sebagai target dan Kali Linux sebagai pelaku serangan. Dengan pendekatan gabungan antara metode kualitatif dan kuantitatif, penelitian ini berupaya memahami pola serangan sekaligus mengevaluasi performa klasifikasi data menggunakan KNN. Hasilnya menunjukkan bahwa kombinasi honeypot dan KNN dapat memberikan gambaran yang lebih jelas dan akurat mengenai aktivitas mencurigakan dalam jaringan. Temuan ini diharapkan dapat memperkaya pemahaman tentang sistem pertahanan siber dan menjadi referensi dalam pengembangan sistem deteksi serangan berbasis data.

Kata Kunci: Honeypot, Serangan Siber, Keamanan Jaringan, KNN, Analisis Data, Virtualisasi

DESIGN AND PERFORMANCE ANALYSIS OF A HONEYPOT FOR NETWORK SECURITY USING THE KNN ALGORITHM

GREGORIAN IVOLITO RAMADHANI SANDA

ABSTRACT

Cybersecurity has become a critical aspect of the rapidly evolving digital era. Cyberattacks are growing more sophisticated and diverse, necessitating early detection methods to identify threats before they cause significant damage. The rapid advancement of digital technology has brought along a growing threat of cyberattacks that can compromise the stability and security of network systems. Attacks such as Distributed Denial of Service (DDoS), brute force, and malware distribution have become increasingly common and dangerous. To address these challenges, honeypots serve as an effective defensive mechanism by attracting and recording malicious activities without exposing the real system to risk. This study examines the implementation of a honeypot system to detect attack patterns, which are subsequently analyzed using the K-Nearest Neighbor (KNN) algorithm to classify various types of network attacks. The simulation is conducted in a virtual environment, with Ubuntu used as the target server and Kali Linux as the attacker. By combining qualitative and quantitative research approaches, this study aims to understand attack behaviors while also evaluating the classification performance of KNN. The results demonstrate that integrating honeypots with KNN can provide accurate insights into network threats. These findings contribute to the development of smarter and more responsive cybersecurity detection systems.

Keywords: Honeypot, Cyberattack, Network Security, KNN, Data Analysis, Virtual Environment

UNIVERSITAS
MERCU BUANA

DAFTAR ISI

HALAMAN SAMPUL.....	0
HALAMAN JUDUL.....	i
HALAMAN PERNYATAAN KARYA SENDIRI	ii
HALAMAN SURAT KETERANGAN HASIL UJI TURNITIN	iii
HALAMAN PENGESAHAN.....	iv
KATA PENGANTAR.....	v
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR DI REPOSITORI UMB.....	vi
ABSTRAK.....	vii
ABSTRACT.....	viii
DAFTAR ISI	ix
DAFTAR TABEL	xi
DAFTAR GAMBAR	xii
DAFTAR LAMPIRAN.....	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah	2
1.3 Tujuan Penelitian.....	3
1.4 Manfaat Penelitian.....	3
1.5 Batasan Masalah.....	4
BAB II TINJAUAN PUSTAKA.....	5
2.1 Penelitian Terdahulu.....	5
2.2 Teori Utama.....	18
2.2.1 Honeypot.....	18
2.2.2 Virtualisasi.....	19
2.2.3 Distributed Denial of Service (DDoS)	19
2.2.4 Port Scanning.....	19
2.2.5 Brute Force.....	20
2.2.6 Malware.....	20
2.3 Teori Pendukung.....	21
2.3.1 Algoritma KNN	21
2.4 Gap Penelitian.....	22
BAB III METODE PENELITIAN	23
3.1 Jenis Penelitian.....	23
3.2 Desain Penelitian	23
3.3 Pengumpulan Data.....	25
3.4 Analisis Data.....	25
3.5 Tahapan Penelitian	26
BAB IV PEMBAHASAN.....	29
4.1 Lingkungan Penelitian.....	29
4.2 Topologi jaringan.....	29
4.3 Perancangan Sistem	30
4.3.1 Instalasi Honeypot T-pot.....	30
4.3.2 Alur kerja sistem.....	31

4.4 Pengujian Sistem	32
4.4.1 Nmap	33
4.4.2 Metasploit	34
4.4.3 Mirai	38
4.3.4 Hping3	40
4.3.5 Hammer.py	41
4.5 Pengumpulan dan Persiapan Data	42
4.5.1 Sumber Data	42
4.5.2 Pembersihan Data	43
4.5.3 Pelabelan Data	45
4.5.4 Normalisasi Data	46
4.6 Implementasi algoritma KNN	46
4.6.1 Import Library	47
4.6.2 Split Data	48
4.6.3 Menentukan Nilai K	48
4.6.4 Menghitung Jarak	49
4.6.5 Voting mayoritas	50
4.7 Evaluasi Kinerja Honeypot	52
4.7.1 Akurasi	53
4.7.2 Precision	54
4.7.3 Recall	54
4.7.4 F1-score	55
4.7.5 Confusion Matrix	56
BAB V KESIMPULAN DAN SARAN	58
5.1 Kesimpulan	58
5.2 Saran	59
DAFTAR PUSTAKA	60
LAMPIRAN	63

DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu.....	5
Tabel 4.1 Confusion Matrix.....	57



DAFTAR GAMBAR

Gambar 3.1	Desain Penelitian.....	11
Gambar 3.2	Alur Tahapan Penelitian.....	26
Gambar 4.1	Topologi Virtualbox.....	29
Gambar 4.2	Tampilan Login t-pot.....	30
Gambar 4.3	Tampilan t-pot map.....	31
Gambar 4.4	Alur Kerja Sistem.....	31
Gambar 4.5	Flowchart Nmap Attack.....	33
Gambar 4.6	Tampilan penyerangan Nmap 1.....	33
Gambar 4.7	Tampilan penyerangan Nmap 2.....	34
Gambar 4.9	Alur kerja Brute Force SSH.....	34
Gambar 4.10	Alur kerja Brute Force Telnet.....	35
Gambar 4.11	Tampilan Brute Force Attack SSH 1.....	35
Gambar 4.12	Tampilan Brute Force Attack SSH 2.....	36
Gambar 4.13	Tampilan login port 22.....	36
Gambar 4.14	Tampilan Brute Force Attack Telnet 1.....	37
Gambar 4.15	Tampilan Brute Force Attack Telnet 2.....	37
Gambar 4.16	Tampilan Login Telnet.....	38
Gambar 4.17	Alur kerja Malware Attack.....	38
Gambar 4.18	Tampilan Login Putty.....	39
Gambar 4.19	Tampilan Malware Attack.....	39
Gambar 4.20	Alur Kerja DOS.....	40
Gambar 4.21	Tampilan Dos Attack.....	40
Gambar 4.22	Tampilan Wireshark Dos Attack.....	41
Gambar 4.23	Tampilan DDOS Attack.....	41
Gambar 4.24	Tampilan Wireshark DDOS.....	42
Gambar 4.25	Tampilan Reports kibana.....	43
Gambar 4.26	Tampilan Import Dataset.....	43
Gambar 4.27	Tampilan menghapus data duplikat.....	44
Gambar 4.28	Tampilan menghapus data tidak relevan.....	44
Gambar 4.29	Tampilan Data cleansing.....	45
Gambar 4.30	Tampilan labeling data.....	46
Gambar 4.31	Tampilan normalisasi data.....	46
Gambar 4.32	Import Library.....	47
Gambar 4.33	Tampilan Split data.....	47
Gambar 4.34	Tampilan Akurasi Nilai K.....	49
Gambar 4.35	Tampilan Uji Data Baru.....	51
Gambar 4.36	Tampilan Posisi data Baru.....	52
Gambar 4.37	Tampilan Hasil Perhitungan Akurasi.....	53
Gambar 4.38	Tampilan Hasil Perhitungan Precision.....	54
Gambar 4.39	Tampilan Hasil Perhitungan Recall.....	55
Gambar 4.40	Tampilan Hasil Perhitungan F1-Score.....	56
Gambar 4.41	Tampilan Hasil Perhitungan Confusion Matrix.....	57

DAFTAR LAMPIRAN

Lampiran 1. Kartu Asistensi.....	63
Lampiran 2. Curriculum Vitae.....	64
Lampiran 3. Surat Pernyataan & Pengalihan HAKI.....	65
Lampiran 4. Sertifikat BNSP.....	67

