ANALISIS FRAMEWORK T-POT DAN SIEM SEBAGAI SISTEM DETEKSI INTRUSI SERTA NOTIFIKASI *REAL-TIME* MELALUI TELEGRAM

MUHAMMAD KAHFI DARMAWAN

NIM. 2210511007

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

2026

ANALISIS FRAMEWORK T-POT DAN SIEM SEBAGAI SISTEM DETEKSI INTRUSI SERTA NOTIFIKASI *REAL-TIME* MELALUI TELEGRAM

MUHAMMAD KAHFI DARMAWAN
NIM. 2210511007

SKRIPSI
Sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer

PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA
2026

ABSTRAK

Meningkatnya ancaman serangan siber terhadap infrastruktur jaringan menuntut adanya sistem deteksi intrusi yang mampu merespons secara cepat dan konsisten. Penelitian ini bertujuan untuk membangun, mengimplementasikan, dan mengevaluasi sistem deteksi intrusi berbasis framework T-Pot yang terintegrasi dengan Security Information and Event Management (SIEM) menggunakan Elastic Stack, serta mekanisme notifikasi real-time melalui Telegram. Sistem yang dibangun memanfaatkan tiga komponen utama T-Pot, yaitu Cowrie sebagai SSH honeypot, Dionaea sebagai honeypot multi-protokol, dan Suricata sebagai Intrusion Detection System (IDS), yang dihubungkan dengan ElastAlert2 sebagai rule-based alerting engine. Sebagai kontribusi tambahan, dikembangkan script malware_vt_checker.py untuk melakukan enrichment otomatis terhadap sampel malware menggunakan VirusTotal API.

Evaluasi sistem dilakukan melalui dua tahap pengujian. Pengujian organik selama 16 hari efektif menghasilkan 6.332.283 events dari 28.224 alamat IP unik di 163 negara, termasuk pendeteksian 1.062 sampel malware dengan 198 hash unik, di mana 98,56% terklasifikasi sebagai malicious oleh VirusTotal. Pengujian terkontrol dilakukan dengan 150 iterasi yang mencakup lima skenario, yaitu brute force SSH, port scanning, DDoS/SYN flood, malware upload dengan VirusTotal, dan malware upload tanpa VirusTotal. Metrik yang diukur meliputi Mean Time to Detect (MTTD) sebagai indikator kecepatan notifikasi end-to-end dan success rate sebagai indikator konsistensi notifikasi.

Hasil pengujian menunjukkan bahwa MTTD rata-rata keseluruhan sebesar 24,902 detik dengan success rate 100% dari seluruh iterasi. Per skenario, MTTD terendah dicapai oleh skenario malware tanpa VirusTotal (15,067 detik), diikuti brute force (18,786 detik), port scanning (22,769 detik), dan DDoS (28,703 detik). Skenario malware dengan VirusTotal menghasilkan MTTD 39,185 detik akibat overhead enrichment API eksternal. Analisis bottleneck menunjukkan bahwa segmen T2→T3 (ElastAlert polling) mendominasi latency pada empat skenario pertama dengan kontribusi 92–98%, sedangkan bottleneck pada skenario malware dengan VirusTotal berada pada segmen T1→T2 (enrichment VirusTotal, rata-rata 24,185 detik). Seluruh hipotesis terpenuhi: H1 terpenuhi secara parsial (4 dari 5 skenario memenuhi target MTTD $\leq$ 30 detik), H2 terpenuhi penuh (success rate 100%), dan H3 terpenuhi melalui bukti peningkatan kualitas informasi keamanan dari event mentah menjadi alert terstruktur dengan enrichment GeoIP, klasifikasi signature, dan analisis threat intelligence.

Kata Kunci: *honeypot, T-Pot, SIEM, Elastic Stack, ElastAlert, intrusion detection system, MTTD, notifikasi real-time, Telegram, VirusTotal, Cowrie, Dionaea, Suricata*

ABSTRACT

The increasing threat of cyber attacks against network infrastructure demands an intrusion detection system capable of responding rapidly and consistently. This research aims to build, implement, and evaluate an intrusion detection system based on the T-Pot framework integrated with Security Information and Event Management (SIEM) using Elastic Stack, along with a real-time notification mechanism through Telegram. The system utilizes three core T-Pot components — Cowrie as an SSH honeypot, Dionaea as a multi-protocol honeypot, and Suricata as an Intrusion Detection System (IDS) — connected to ElastAlert2 as a rule-based alerting engine. As an additional contribution, the malware_vt_checker.py script was developed to perform automated enrichment of malware samples using the VirusTotal API.

System evaluation was conducted in two phases. Organic testing over 16 effective days captured 6,332,283 events from 28,224 unique IP addresses across 163 countries, including the detection of 1,062 malware samples with 198 unique hashes, of which 98.56% were classified as malicious by VirusTotal. Controlled testing was performed with 150 iterations across five scenarios: SSH brute force, port scanning, DDoS/SYN flood, malware upload with VirusTotal, and malware upload without VirusTotal. Metrics measured include Mean Time to Detect (MTTD) as an indicator of end-to-end notification speed and success rate as an indicator of notification consistency.

Results show an overall average MTTD of 24.902 seconds with a 100% success rate across all iterations. Per scenario, the lowest MTTD was achieved by malware without VirusTotal (15.067 seconds), followed by brute force (18.786 seconds), port scanning (22.769 seconds), and DDoS (28.703 seconds). The malware scenario with VirusTotal yielded an MTTD of 39.185 seconds due to external API enrichment overhead. Bottleneck analysis revealed that the T2→T3 segment (ElastAlert polling) dominates latency in four of five scenarios, contributing 92–98% of total MTTD, while the bottleneck in the malware with VirusTotal scenario shifts to the T1→T2 segment (VirusTotal enrichment, averaging 24.185 seconds). All hypotheses were confirmed: H1 was partially fulfilled (4 of 5 scenarios met the MTTD ≤ 30 second target), H2 was fully fulfilled (100% success rate), and H3 was confirmed through evidence of improved security information quality — transforming raw events into structured alerts enriched with GeoIP context, signature classification, and threat intelligence analysis.

Keywords: *honeypot, T-Pot, SIEM, Elastic Stack, ElastAlert, intrusion detection system, MTTD, real-time notification, Telegram, VirusTotal, Cowrie, Dionaea, Suricata*

LEMBAR PERSETUJUAN SKRIPSI

LEMBAR PERSETUJUAN

Yang bertanda tangan di bawah ini:
Nama : Muhammad Kahfi Darmawan
NIM : 2210511007
Program Studi : Informatika Program Sarjana/~~Sistem Informasi Program Sarjana/Sains Data Program Sarjana/Sistem Informasi Program Diploma~~ (*Coret yang tidak perlu)

Jenis Tugas Akhir : Skripsi / ~~Proyek / Artikel Publikasi~~ (*Coret yang tidak perlu)

Judul Proposal Tugas Akhir : ANALISIS FRAMEWORK T-POT DAN SIEM SEBAGAI SISTEM DETEKSI INTRUSI SERTA NOTIFIKASI REAL-TIME MELALUI TELEGRAM

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

Jakarta, 27 April 2026

Menyetujui,

Dosen Pembimbing 1,	Dosen Pembimbing 2,
Ditandatangani secara digital oleh: Henki Bayu Seta Verifikasi di disign.upnvj.ac.id	Ditandatangani secara digital oleh Hamonangan Kinantan Prabu Verifikasi di disign.upnvj.ac.id
Henki Bayu Seta, S.Kom., M.TI	Hamonangan Kinantan P., S.T, MT
NIDN. 0309118104	NIDN. 0002088502

Mengetahui,

Koordinator Program Studi,

Ditandatangani secara digital oleh Ridwan Raafi'udin
Verifikasi di disign.upnvj.ac.id

Dr. Ridwan Raafi'udin, S.Kom., M.Kom
NIDN. 002058804

LEMBAR PENGESAHAN SKRIPSI

LEMBAR PENGESAHAN

Judul	:	Analisis Framework T-Pot dan SIEM sebagai Sistem Deteksi Intrusi serta Notifikasi *Real-Time* melalui Telegram
Nama	:	Muhammad Kahfi Darmawan
NIM	:	2210511007
Program Studi	:	S1 Informatika

Disetujui oleh :

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

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

Pembimbing 1:
Henki Bayu Seta, S.Kom, MTI.

Pembimbing 2:
Hamonangan Kinantan Prabu, 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 :
22 Mei 2026

PERNYATAAN ORISINALITAS

PERNYATAAN ORISINALITAS

Tugas akhir ini adalah hasil karya saya sendiri dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan benar

Nama	:	Muhammad Kahfi Darmawan
NIM	:	2210511007
Tanggal	:	24 Juli 2026
Judul Skripsi	:	**ANALISIS FRAMEWORK T-POT DAN SIEM SEBAGAI SISTEM DETEKSI INTRUSI SERTA NOTIFIKASI REAL-TIME MELALUI TELEGRAM**

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

Jakarta, 24 Juli 2026

Yang menyatakan.

Muhammad Kahfi Darmawan

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional "Veteran" Jakarta, saya yang bertanda tangan di bawah ini.

Nama	:	Muhammad Kahfi Darmawan
NIM	:	2210511007
Fakultas	:	Ilmu Komputer
Program Studi	:	S-1 Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan karya ilmiah saya kepada Universitas Pembangunan Nasional "Veteran" Jakarta Hak Bebas Non-Eksklusif (*Non-Exclusive Royalty Free Right*) untuk publikasi dengan judul:

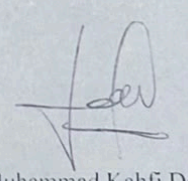
ANALISIS FRAMEWORK T-POT DAN SIEM SEBAGAI SISTEM DETEKSI INTRUSI SERTA NOTIFIKASI REAL-TIME MELALUI TELEGRAM

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional "Veteran" Jakarta berhak menyimpan, mengalih media atau memformatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasi artikel ilmiah selama tetap mencantumkan nama saya sebagai penulis atau pencipta dan sebagai pemilik Hak Cipta.

Dengan pernyataan ini saya buat dengan sebenarnya.

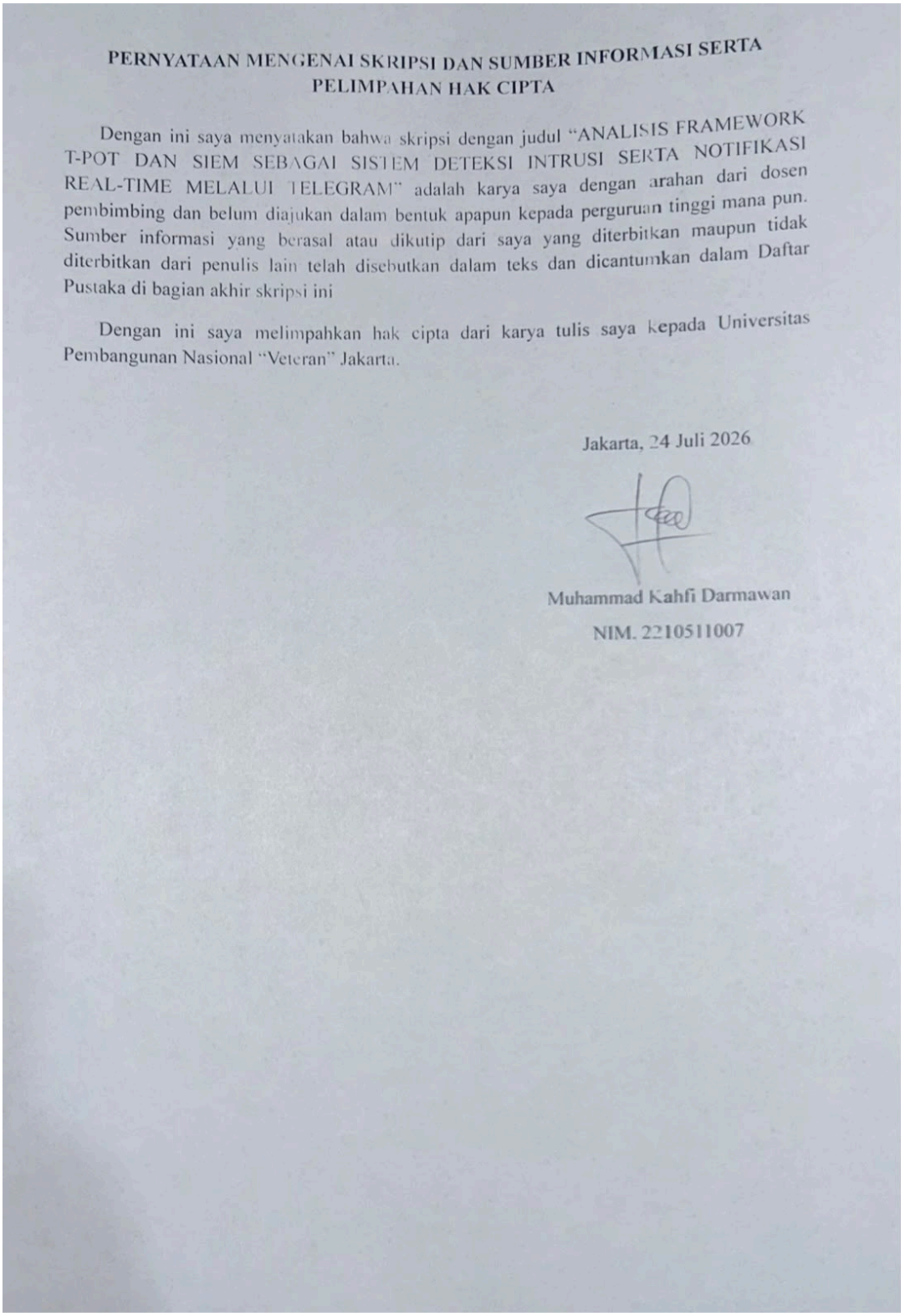
Dibuat di : Jakarta
Pada tanggal : 24 Juli 2026

Yang menyatakan,



Muhammad Kahfi Darmawan

PERNYATAAN MENGENAI SKRIPSI DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA



PERNYATAAN MENGENAI SKRIPSI DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA

Dengan ini saya menyatakan bahwa skripsi dengan judul "ANALISIS FRAMEWORK T-POT DAN SIEM SEBAGAI SISTEM DETEKSI INTRUSI SERTA NOTIFIKASI REAL-TIME MELALUI TELEGRAM" adalah karya saya dengan arahan dari dosen pembimbing dan belum diajukan dalam bentuk apapun kepada perguruan tinggi mana pun. Sumber informasi yang berasal atau dikutip dari saya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka di bagian akhir skripsi ini

Dengan ini saya melimpahkan hak cipta dari karya tulis saya kepada Universitas Pembangunan Nasional "Veteran" Jakarta.

Jakarta, 24 Juli 2026

Muhammad Kahfi Darmawan

NIM. 2210511007

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat, karunia, serta kesempatan yang diberikan, sehingga penulis dapat menyelesaikan Tugas Akhir yang berjudul “Analisis Framework T-Pot dan SIEM sebagai Sistem Deteksi Intrusi serta Notifikasi Real-Time melalui Telegram” dengan baik.

Penyusunan Tugas Akhir ini dilakukan sebagai salah satu syarat untuk menyelesaikan pendidikan pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta. Dalam proses penyusunannya, penulis menyadari bahwa banyak pihak yang turut berperan, baik melalui bimbingan, dukungan, maupun bantuan secara langsung maupun tidak langsung.

Oleh karena itu, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Allah SWT, atas segala nikmat, kesehatan, serta kemudahan yang diberikan sehingga penulis dapat menyelesaikan Tugas Akhir ini hingga akhir.
2. Prof. Dr. Ir. Supriyanto, ST., M.Sc., IPM, selaku Dekan Fakultas Ilmu Komputer UPN Veteran Jakarta yang telah menyediakan lingkungan akademik yang mendukung proses pembelajaran dan pengembangan diri mahasiswa.
3. Dr. Ridwan Raafi'udin, S.Kom., M.Kom., selaku Ketua Program Studi S1 Informatika yang telah memberikan arahan serta kebijakan yang membantu kelancaran proses studi penulis.
4. Bapak Henki Bayu Seta, S.Kom., M.TI., selaku Dosen Pembimbing I yang telah memberikan banyak masukan, arahan, serta wawasan dalam proses penyusunan penelitian ini.
5. Bapak Hamonangan Kinantan Prabu, S.T., M.T., selaku Dosen Pembimbing II yang dengan penuh kesabaran membimbing serta membantu penulis dalam menyempurnakan penelitian ini.
6. Bapak Muhammad Panji Muslim, S.Pd., M.Kom., selaku Dosen Pembimbing Akademik yang senantiasa memberikan dukungan dan arahan selama masa perkuliahan.
7. Seluruh dosen dan staf Fakultas Ilmu Komputer yang telah memberikan ilmu, pengalaman, serta bantuan selama penulis menempuh pendidikan.

8. Kedua orang tua tercinta, Bapak Fachri Darmawan dan Ibu Evi Nurhayati, yang selalu memberikan doa, dukungan, serta motivasi tanpa henti sehingga penulis dapat menyelesaikan studi ini.
9. Elsya Putri Ramadhani, yang selalu hadir memberikan semangat, dukungan, serta menjadi tempat berbagi cerita dalam setiap proses yang dilalui penulis selama penyusunan Tugas Akhir ini.
10. Diri penulis sendiri yang telah berusaha bertahan, belajar, dan terus melangkah hingga mampu menyelesaikan tahap ini.

Penulis menyadari bahwa Tugas Akhir ini masih memiliki banyak kekurangan, baik dari segi isi maupun penyajian. Oleh karena itu, penulis sangat terbuka terhadap kritik dan saran yang membangun demi perbaikan di masa mendatang. Semoga penelitian ini dapat memberikan manfaat dan kontribusi, khususnya dalam bidang keamanan siber.

Akhir kata, penulis mengucapkan terima kasih kepada semua pihak yang telah membantu, dan semoga segala kebaikan yang diberikan mendapatkan balasan yang setimpal dari Allah SWT.

Jakarta, 29 April 2026

Muhammad Kahfi Darmawan

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

DAFTAR RUMUS