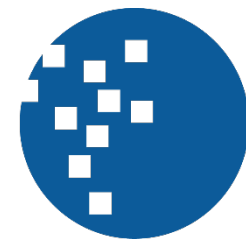


**DETEKSI RAGAM SERANGAN SSH
BERDASARKAN LOG AUTENTIKASI
MENGUNAKAN LONG SHORT-TERM MEMORY**



UMN

UNIVERSITAS
MULTIMEDIA
NUSANTARA

Tugas Akhir

Bintang Timurlangit

00000053806

**PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG**

2025

**DETEKSI RAGAM SERANGAN SSH
BERDASARKAN LOG AUTENTIKASI
MENGUNAKAN LONG SHORT-TERM MEMORY**



Diajukan sebagai Salah Satu Syarat untuk Memperoleh
Gelar Sarjana Teknik

Bintang Timurlangit

00000053806

**PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG**

2025

HALAMAN PERNYATAAN TIDAK PLAGIAT

Dengan ini saya,

Nama : Bintang Timurlangit

Nomor Induk Mahasiswa : 00000053806

Program Studi : Teknik Komputer

Skripsi dengan judul:

DETEKSI RAGAM SERANGAN SSH
BERDASARKAN LOG AUTENTIKASI
MENGUNAKAN LONG SHORT-TERM MEMORY

Merupakan hasil karya saya sendiri bukan plagiat dari laporan karya tulis ilmiah yang ditulis oleh orang lain, dan semua sumber, baik yang dikutip maupun dirujuk, telah saya nyatakan dengan benar serta dicantumkan di Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan/penyimpangan, baik dalam pelaksanaan maupun dalam penulisan laporan karya tulis ilmiah, saya bersedia menerima konsekuensi dinyatakan TIDAK LULUS untuk mata kuliah yang telah saya tempuh.

Tangerang, 28 November 2025



Bintang Timurlangit

HALAMAN PERSETUJUAN

Tugas Akhir dengan Judul

Deteksi Ragam Serangan SSH Berdasarkan Log Autentikasi
Menggunakan Long Short-Term Memory

Oleh

Nama : Bintang Timurlangit

NIM : 00000053806

Program Studi : Teknik Komputer

Fakultas : Teknik dan Informatika

Telah disetujui untuk diajukan pada

Sidang Tugas Akhir Universitas Multimedia Nusantara

Tangerang, 5 Januari 2026

Pembimbing



Hargyo T. N. Ignatius, Ph.D.
NIDN.0317048101

Ketua Program Studi Teknik Komputer



Samuel Hutagalung, M. T. I
NIDN.034038902

HALAMAN PENGESAHAN

Tugas Akhir dengan Judul

Deteksi Ragam Serangan SSH Berdasarkan Log Autentikasi
Menggunakan Long Short-Term Memory

Oleh

Nama : Bintang Timurlangit
NIM : 00000053806
Program Studi : Teknik Komputer
Fakultas : Teknik dan Informatika

Telah diujikan pada hari Kamis, 8 Januari 2026

Pukul 13.00 s.d 15.00 dan dinyatakan

LULUS

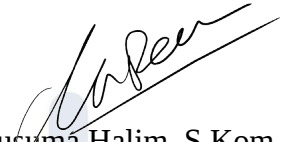
Dengan susunan penguji sebagai berikut.

Ketua Sidang

Penguji



Nabila Husna Shabrina S.T., M.T.
NIDN.0321099301



Dareen Kusuma Halim, S.Kom., M.Eng.Sc.
NIDN.0317129202

Pembimbing



Hargyo T. N. Ignatius, Ph.D.
NIDN.0317048101

Ketua Program Studi Teknik Komputer



Samuel Hutagalung, M. T. I.
NIDN.0304038902

HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH

Yang bertanda tangan di bawah ini:

Nama : Bintang Timurlangit
NIM : 00000053806
Program Studi : Teknik Komputer
Jenjang : S1
Judul Karya Ilmiah : Deteksi Ragam Serangan SSH Berdasarkan Log Autentikasi Menggunakan Long Short-Term Memory

Menyatakan dengan sesungguhnya bahwa saya bersedia (**pilih salah satu**):

- ☒ Saya bersedia memberikan izin sepenuhnya kepada Universitas Multimedia Nusantara untuk mempublikasikan hasil karya ilmiah saya ke dalam repositori Knowledge Center sehingga dapat diakses oleh Sivitas Akademika UMN/Publik. Saya menyatakan bahwa karya ilmiah yang saya buat tidak mengandung data yang bersifat konfidensial.
- ☐ Saya tidak bersedia mempublikasikan hasil karya ilmiah ini ke dalam repositori Knowledge Center, dikarenakan: dalam proses pengajuan publikasi ke jurnal/konferensi nasional/internasional (dibuktikan dengan *letter of acceptance*) **.
- ☐ Lainnya, pilih salah satu:
 - ☐ Hanya dapat diakses secara internal Universitas Multimedia Nusantara
 - ☐ Embargo publikasi karya ilmiah dalam kurun waktu 3 tahun.

Tangerang, 5 Januari 2026



Bintang Timurlangit

* Pilih salah satu

** Jika tidak bisa membuktikan LoA jurnal/HKI, saya bersedia mengizinkan penuh karya ilmiah saya untuk dipublikasikan ke KC UMN dan menjadi hak institusi UMN.

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas segala rahmat, karunia, dan petunjuk-Nya sehingga penulis dapat menyelesaikan tugas akhir yang berjudul *“Deteksi Ragam Serangan SSH Berdasarkan Log Autentikasi Menggunakan Long Short-Term Memory”*. Tugas akhir ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana pada Program Studi Teknik Komputer di Universitas Multimedia Nusantara.

Pencapaian ini tidak terlepas dari dukungan, bantuan, dan bimbingan berbagai pihak sejak awal masa perkuliahan hingga pada tahap akhir penyusunan tugas akhir ini. Tanpa kontribusi dan kebaikan yang penulis terima, laporan ini tidak akan terselesaikan sebagaimana adanya, bahkan mungkin tidak pernah menjadi kenyataan. Sebagai pengingat sekaligus penghormatan atas perjalanan ini, penulis menyisipkan sebuah kutipan yang senantiasa meneguhkan langkah:

“Perjalanan manusia selalu lebih bermakna ketika dijalani bersama; sebab kemajuan tidak lahir dari langkah tunggal, melainkan dari dorongan, kepedulian, dan ruang tumbuh yang kita saling berikan.”

Dengan penuh rasa hormat, penulis menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Dr. Ir. Andrey Andoko, M.Sc., selaku Rektor Universitas Multimedia Nusantara.
2. Dr. Eng. Niki Prastomo, S.T., M.Sc., selaku Dekan Fakultas Universitas Multimedia Nusantara.
3. Samuel Hutagalung, M. T. I., selaku Ketua Program Studi Universitas Multimedia Nusantara.
4. Hargyo T. N. Ignatius, Ph.D., sebagai Pembimbing pertama yang telah memberikan bimbingan, arahan, dan motivasi atas terselesainya tugas akhir ini.

5. PT Maro Anugrah Jaya, sebagai perusahaan yang telah berkenan untuk memberikan data dan informasi yang menjadi bahan utama dalam penelitian ini.
6. Keluarga saya tercinta yang telah memberikan bantuan dukungan material dan moral, sehingga penulis dapat menyelesaikan tugas akhir ini.
7. Vania Jiang, S.I.Kom, yang selalu memberikan semangat dukungan, dan mengingatkan untuk menyelesaikan tugas akhir ini.
8. Gilbert Zaini, S.T., Christoper John Aranda, S.T., dan Richard Tandean, S.T., yang telah memberikan dukungan dan mengajarkan saya tentang pembelajaran mesin.
9. Dan seluruh pihak lain yang tidak dapat disebutkan satu per satu, namun kontribusinya memiliki peran penting dalam kelancaran proses penelitian dan penyusunan tugas akhir ini.

Penulis berharap semoga karya ilmiah ini dapat dijadikan sebagai referensi dan bahan pembelajaran yang bermanfaat bagi pembaca. Penulis juga menyadari bahwa tugas akhir ini masih memiliki berbagai kekurangan. Oleh karena itu, penulis sangat terbuka terhadap setiap masukan, kritik, dan saran dari berbagai pihak guna memperbaiki dan menyempurnakan karya-karya serupa di masa yang akan datang.

Tangerang, 5 Januari 2026



Bintang Timurlangit

DETEKSI RAGAM SERANGAN SSH BERDASARKAN LOG AUTENTIKASI MENGUNAKAN LONG SHORT-TERM MEMORY

Bintang Timurlangit

ABSTRAK

Serangan SSH *slow-rate* merupakan ancaman yang sulit terdeteksi oleh sistem keamanan berbasis aturan seperti Fail2Ban karena pola percobaannya dilakukan secara perlahan dan tersebar dalam rentang waktu panjang, sehingga tidak melewati ambang batas deteksi berbasis frekuensi. Kondisi ini ditemukan pada infrastruktur server PT Maro Anugrah Jaya. Untuk mengatasi permasalahan tersebut, penelitian ini mengembangkan sistem deteksi intrusi berbasis pembelajaran mesin menggunakan algoritma *Long Short-Term Memory* (LSTM) yang mampu mengenali pola perilaku temporal. Model dilatih menggunakan dataset log autentikasi yang telah direkayasa menjadi sekuens berdasar jendela waktu, kemudian diuji pada data uji serta diimplementasikan dalam aplikasi bernama SSHGuard yang berjalan secara *real-time* pada lingkungan server Linux. Evaluasi model menunjukkan performa yang baik dengan akurasi sebesar 92,38% pada pengujian dataset latihan dan 94,18% saat diimplementasikan dalam sistem nyata. Hasil pengujian aplikasi menunjukkan adanya penurunan signifikan pada tingkat *false negative*, di mana Fail2Ban gagal mendeteksi 403 aktivitas serangan (*false negative*), sedangkan SSHGuard berhasil mendeteksi seluruh aktivitas serangan pada dataset pengujian tanpa menghasilkan *false negative*. Selain itu, SSHGuard mengidentifikasi 1.063 alamat IP sebagai serangan, jauh lebih tinggi dibandingkan Fail2Ban yang hanya memblokir 598 alamat IP. Pendekatan LSTM mampu meningkatkan efektivitas deteksi serangan SSH *slow-rate* yang sebelumnya tidak tertangani oleh sistem berbasis aturan.

Kata kunci: SSH, *slow-rate*, LSTM, deteksi intrusi, analisa log

DETECTION OF SSH ATTACK CLASSES BASED ON AUTHENTICATION LOGS USING LONG SHORT-TERM MEMORY

Bintang Timurlangit

ABSTRACT (English)

Slow-rate SSH attacks are a stealthy threat that is difficult to detect using rule-based security systems such as Fail2Ban, as their login attempts are spread across long time intervals and do not exceed frequency-based detection thresholds. This issue is also found in the server infrastructure of PT Maro Anugrah Jaya. To address this problem, this research proposes a machine learning-based intrusion detection system using a Long Short-Term Memory (LSTM) model capable of learning temporal behavioural patterns. The model was trained using authentication logs that were converted into time-windowed sequences, and subsequently evaluated through testing and deployed in a real-time application called SSHGuard on a Linux server environment. Model evaluation demonstrated strong performance with an accuracy of 92.38% on test data and 94.18% when deployed in a real operational environment. Application-level testing demonstrates a significant reduction in the false negative rate, where Fail2Ban failed to detect 403 attack activities (false negatives), while SSHGuard successfully detected all attack activities in the evaluation dataset without producing any false negatives. In addition, SSHGuard identified 1,063 IP addresses as attacks, significantly higher than Fail2Ban, which blocked only 598 IP addresses. The results indicate that the LSTM-based approach effectively improves the detection of slow-rate SSH attacks that conventional rule-based systems fail to identify.

Keywords: SSH, slow-rate attack, LSTM, intrusion detection, log analysis

DAFTAR ISI

HALAMAN PERNYATAAN TIDAK PLAGIAT	ii
HALAMAN PERSETUJUAN	iii
HALAMAN PENGESAHAN	iv
HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH	v
ABSTRAK	viii
<i>ABSTRACT (English)</i>	ix
DAFTAR ISI	x
DAFTAR TABEL	xiii
DAFTAR GAMBAR	xiv
DAFTAR LAMPIRAN	xvii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Pertanyaan Penelitian	5
1.3 Batasan Penelitian	6
1.4 Tujuan Penelitian	7
1.5 Manfaat Penelitian	7
1.6 Sistematika Penulisan	8
BAB II TINJAUAN PUSTAKA	9
2.1 Penelitian Terdahulu	Error! Bookmark not defined.
2.1.1 <i>SSH and FTP brute-force Attacks Detection in Computer Network: LSTM and Machine Learning Approaches</i>	9
2.1.2 <i>HTTP Low and Slow DoS Attack Detection using LSTM</i>	10
2.1.3 <i>On the Detection Capabilities of Signature-Based Intrusion Detection System in the Context of Web Attacks</i>	11
2.1.4 <i>Transferability of Machine Learning Models Learned from Public Intrusion Detection Datasets: The CICIDS2017 Case Study</i>	12
2.1.5 <i>Evaluation of Cluster Based Anomaly Detection</i>	13
2.2 Virtualisasi Proxmox	14
2.3 Protokol Secure Shell (SSH)	15
2.4 Serangan Brute-Force	18
2.4.1 Serangan Frekuensi Tinggi	19

2.4.2	Serangan dengan Teknik <i>Slow-Rate</i>	19
2.5	Deteksi Serangan Berbasis Aturan (<i>Rule Based</i>)	20
2.6	<i>Long Short-Term Memory</i> (LSTM)	22
BAB III METODE PENELITIAN		25
3.1	Metode Penelitian	25
3.2	Perancangan Model	27
3.2.1	Pengumpulan Dataset	27
3.2.2	Prapemrosesan Data	28
3.2.3	Perancangan Fitur	31
3.2.4	Pelabelan Data	36
3.2.5	Persiapan Data	39
3.2.6	Pelatihan Model	42
3.2.7	Evaluasi Model	46
3.3	Perancangan Aplikasi	50
3.3.1	Arsitektur Aplikasi	50
3.3.2	Integrasi Model dan Konfigurasi	57
3.3.3	Layanan Sistem dan CLI	57
3.3.4	Pengemasan Aplikasi	59
3.3.5	Distribusi Aplikasi	60
3.3.6	Evaluasi Aplikasi	61
BAB IV IMPLEMENTASI DAN PENGUJIAN		65
4.1	Spesifikasi Sistem	66
4.1.1	Spesifikasi Hardware Komputer Penulis	66
4.1.2	Spesifikasi Hardware Laptop Penulis	66
4.1.3	Spesifikasi Hardware Pengujian	66
4.2	Implementasi Model	67
4.2.1	Pengumpulan Dataset	67
4.2.2	Prapemrosesan Data	69
4.2.3	Perancangan Fitur	74
4.2.4	Pelabelan Data	77
4.2.5	Persiapan Data	85
4.2.6	Pelatihan Model	90

4.2.7	Ekspor Model	91
4.3	Implementasi Aplikasi	92
4.3.1	Modul Utama	92
4.3.2	Layanan Sistem dan CLI	97
4.3.3	Pengemasan Aplikasi	98
4.3.4	Distribusi Aplikasi	99
4.3.5	Instalasi	100
4.4	Pengujian & Analisis	101
4.4.1	Evaluasi Model	101
4.4.2	Evaluasi Aplikasi	110
4.5	Limitasi	116
4.5.1	Ketergantungan pada Pola Perilaku Temporal	116
4.5.2	Rotasi Alamat IP oleh Penyerang	116
BAB V SIMPULAN DAN SARAN		117
5.1	Simpulan	117
5.2	Saran	118
DAFTAR PUSTAKA		119
LAMPIRAN		124



DAFTAR TABEL

Tabel 3.1 Fitur Statistik Dasar	32
Tabel 3.2 <i>Hyperparameter</i> Model	43
Tabel 3.3 Parameter <i>Callback</i> EarlyStopping.....	44
Tabel 3.4 Parameter <i>Callback</i> ReduceLROnPlateau	45
Tabel 3.5 Perintah Deteksi dalam Aplikasi.....	58
Tabel 3.6 Spesifikasi LXC <i>Container</i>	61
Tabel 3.7 Parameter SSH pada LXC <i>Container</i>	61
Tabel 4.1 Pola Regex untuk Klasifikasi Peristiwa	71
Tabel 4.2 Nilai Statistik Prediksi <i>Slow-Rate</i>	109
Tabel 4.3 Nilai Statistik Prediksi Fast Attack	110
Tabel 4.4 Hasil Pengujian <i>Coverage</i>	111
Tabel 4.5 Hasil Pengujian terhadap Metrik Evaluasi Standar.....	112



DAFTAR GAMBAR

Gambar 1.1 Grafik Percobaan Serangan SSH.....	2
Gambar 1.2 Grafik Percobaan Serangan SSH yang dilewatkan Fail2Ban.....	3
Gambar 2.1 Arsitektur Internal Proxmox.	14
Gambar 2.2 Tampilan Web Antarmuka Proxmox	15
Gambar 2.3 Alur Kerja Protokol SSH	16
Gambar 2.4 Alur Kerja Fail2Ban.....	21
Gambar 2.5 Struktur Dasar Unit LSTM.....	23
Gambar 3.1 Metode Penelitian.....	25
Gambar 3.2 Arsitektur Aplikasi	50
Gambar 3.3 Alur Kerja Aplikasi	52
Gambar 4.1 Lokasi Tempat Log Autentikasi.....	67
Gambar 4.2 Isi dari Berkas Log Autentikasi Proxmox.....	68
Gambar 4.3 Repositori LogHub pada situs GitHub.....	68
Gambar 4.4 Hasil Unduhan Log Autentikasi LogHub.....	69
Gambar 4.5 Pola Regex untuk Ekstraksi Fitur pada Log.....	70
Gambar 4.6 Kelas YearRollover	70
Gambar 4.7 Fungsi ‘expand_message_repeat()’	72
Gambar 4.8 Sintaks untuk Memasukkan Informasi ke DataFrame	73
Gambar 4.9 Ekspor Data Hasil <i>Parsing</i>	73
Gambar 4.10 Hasil .parquet Seluruh Peristiwa.....	73
Gambar 4.11 Memuat Data Log Hasil <i>Parsing</i>	74
Gambar 4.12 Agregasi Data Berdasarkan IP dan Jendela Waktu.....	74
Gambar 4.13 Perhitungan Fitur Volume dan Frekuensi Aktivitas Autentikasi	75
Gambar 4.14 Perhitungan Fitur Temporal Aktivitas Autentikasi	75
Gambar 4.15 Perhitungan Fitur Keragaman <i>Username</i>	76
Gambar 4.16 Pembersihan dan Normalisasi Fitur	76
Gambar 4.17 Sintaks <i>Clustering</i> dengan DBSCAN	77
Gambar 4.18 Hasil <i>Clustering</i> DBSCAN	78
Gambar 4.19 Analisa Statistik Per-Cluster	79
Gambar 4.20 Hubungan Nilai Median Antar Percobaan Login.....	81

Gambar 4.21 Hubungan Nilai Median Antar Durasi Aktivitas Autentikasi	82
Gambar 4.22 Hubungan Durasi Aktivitas Autentikasi Antar Jumlah Percobaan Login Gagal.....	83
Gambar 4.23 Sintaks Pembentukan Sekuen	85
Gambar 4.24 Hasil Pembentukan Jendela.....	85
Gambar 4.25 Hasil Pemisahan Data Latih dan Uji	86
Gambar 4.26 Sintaks Penyeimbangan Kelas	87
Gambar 4.27 Hasil Penyeimbangan Kelas pada Data Latih	88
Gambar 4.28 Sintaks Normalisasi dan <i>One-Hot Encoding</i>	89
Gambar 4.29 Hasil Pembentukan Data Latih dan Uji.....	89
Gambar 4.30 Inisialisasi Model	90
Gambar 4.31 <i>Callback</i> ReduceLROnPlateau.....	91
Gambar 4.32 <i>Callback</i> EarlyStopping	91
Gambar 4.33 Fungsi Ekspor Model	92
Gambar 4.34 Mekanisme <i>Tailing</i>	92
Gambar 4.35 Fungsi <i>Parse Line</i>	93
Gambar 4.36 Inisialisasi Artefak dan Model	93
Gambar 4.37 Inferensi dan Prediksi Kelas.....	94
Gambar 4.38 Inisialisasi Modul Manajemen <i>Firewall</i>	95
Gambar 4.39 Mekanisme Pemblokiran IP	96
Gambar 4.40 Fungsi Pembersihan IP	96
Gambar 4.41 Definisi Layanan Aplikasi.....	97
Gambar 4.42 Proses Pengemasan Aplikasi.....	99
Gambar 4.43 Repositori Aplikasi di GitHub.....	99
Gambar 4.44 Perintah Instalasi Aplikasi.....	100
Gambar 4.45 Status SSHGuard Berhasil Di-Instal.	100
Gambar 4.46 Kurva <i>Training Loss</i> dan <i>Validation Loss</i>	101
Gambar 4.47 Kurva <i>Training Accuracy</i> dan <i>Validation Accuracy</i>	102
Gambar 4.48 Laporan Klasifikasi Pelatihan Model.....	103
Gambar 4.49 Kurva ROC <i>One-vs-Rest</i>	104
Gambar 4.50 Kurva ROC <i>Macro</i> dan <i>Micro Average</i>	105

Gambar 4.51 Hasil <i>Confusion Matrix</i> Model.....	106
Gambar 4.52 Distribusi Prediksi dan Tingkat Kepercayaan.....	108
Gambar 4.53 Halaman situs SecRepo.....	111
Gambar 4.54 Hasil <i>Confusion Matrix</i> pada Fail2Ban.....	114
Gambar 4.55 Hasil <i>Confusion Matrix</i> pada SSHGuard	115



UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

DAFTAR LAMPIRAN

Lampiran A – Turnitin	124
Lampiran B – Konsultasi Bimbingan.....	132
Lampiran C – Daftar Penggunaan AI	134



UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA