

**ANALISIS KINERJA ALGORITMA LONG SHORT-TERM MEMORY
DALAM DETEKSI INTRUSI JARINGAN
BERBASIS LOG HONEYPOT COWRIE SSH**



RENDY SAHRASAD

2210511132

**PROGRAM STUDI S1 INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA**

2026

**ANALISIS KINERJA ALGORITMA LONG SHORT-TERM MEMORY
DALAM DETEKSI INTRUSI JARINGAN
BERBASIS LOG HONEYPOT COWRIE SSH**

**RENDY SAHRASAD
NIM. 2210511132**

**PROGRAM STUDI S1 INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA
2026**

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

Judul : Analisis Kinerja Algoritma Long Short-Term Memory dalam Deteksi Intrusi Jaringan Berbasis Log Honeypot Cowrie SSH
Nama : Rendy Sahrasad
NIM : 2210511132
Program Studi : Program Sarjana Informatika

Disetujui oleh:

Penguji 1:

Dr. Noor Falih, S.Kom, MT
NIP. 198907152018031001



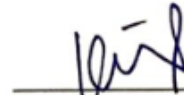
Penguji 2:

Novi Trisman Hadi, S.Pd., M.Kom.
NIP. 199211032022031007



Pembimbing 1:

Prof. Dr. Ir. Supriyanto, ST., M.Sc., IPM
NIP. 197605082003121002



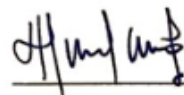
Pembimbing 2:

Hamonangan Kinantan Prabu, M.T.
NIP. 198508022020121003



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:

21 Juli 2026

**PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK
KEPENTINGAN AKADEMIS**

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

Nama : Rendy Sahrasad
NIM : 2210511132
Fakultas : 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:

Analisis Kinerja Algoritma Long Short-Term Memory dalam Deteksi Intrusi Jaringan Berbasis Log Honeypot Cowrie SSH

Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional "Veteran" Jakarta berhak menyimpan, mengalih media atau 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.

Jakarta
21 Juli 2026
Yang menyatakan,



Rendy Sahrasad

**PERSYARATAN MENGENAI SKRIPSI DAN SUMBER INFORMASI SERTA
PELIMPAHAN HAK CIPTA**

Dengan ini saya menyatakan bahwa skripsi dengan judul "Analisis Kinerja Algoritma Long Short-Term Memory dalam Deteksi Intrusi Jaringan Berbasis Log HoneyPot Cowrie SSH" adalah karya saya dengan arahan dari dosen pembimbing dan belum diajukan atau dikutip dari karya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka di bagian akhir proposal ini.

Jakarta, 21 Juli 2026



Rendy Sahrasad
2210511132

**Analisis Kinerja Algoritma *Long Short-Term Memory* dalam Deteksi
Intrusi Jaringan Berbasis Log Honeypot Cowrie SSH
Rendy Sahrasad**

ABSTRAK

Peningkatan aktivitas jaringan komputer menuntut adanya sistem deteksi intrusi yang mampu mengenali pola aktivitas mencurigakan secara terstruktur. Penelitian ini bertujuan mengimplementasikan model *Network Intrusion Detection System* (NIDS) berbasis *Long Short-Term Memory* (LSTM) untuk mengklasifikasikan aktivitas pada log *honeypot* Cowrie SSH. Data log diproses melalui seleksi data Cowrie SSH, pembersihan data, pembentukan *event sequence* berdasarkan *session*, pembentukan label *multiclass*, *feature engineering*, penghapusan fitur yang berpotensi menyebabkan *data leakage* dan *proxy label*, *tokenization*, *padding*, serta pembagian data latih, validasi, dan uji. Kelas klasifikasi yang digunakan terdiri dari *normal*, *scan_probe*, dan *brute_force*. Model LSTM dievaluasi menggunakan metrik *accuracy*, *precision*, *recall*, *F1-score*, dan *confusion matrix*. Hasil evaluasi menunjukkan bahwa model memperoleh *accuracy* sebesar 99,30%, dengan *macro average* dan *weighted average precision*, *recall*, serta *F1-score* sebesar 99,30%. Selain evaluasi model, penelitian ini mengintegrasikan model ke dalam prototipe *dashboard* NIDS berbasis Flask, MongoDB, dan Docker. Hasil pengujian menunjukkan bahwa sistem mampu membaca log Cowrie SSH, membentuk token *session*, melakukan prediksi, menyimpan hasil, dan menampilkan klasifikasi dengan status pencatatan *LOGGED*. Sistem yang dikembangkan bersifat *detection-only* tanpa pemblokiran otomatis.

Kata Kunci: Cowrie SSH, *Honeypot*, *Long Short-Term Memory* (LSTM), *Multiclass*, *Network Intrusion Detection System* (NIDS).

**Performance Analysis of Long Short-Term Memory for Network
Intrusion Detection Based on Cowrie SSH Honeypot Logs**
Rendy Sahrasad

ABSTRACT

The increasing use of computer networks requires an intrusion detection system capable of identifying suspicious activity patterns in a structured manner. This study aims to implement a Long Short-Term Memory (LSTM)-based Network Intrusion Detection System (NIDS) model to classify activities in Cowrie SSH honeypot logs. The log data were processed through Cowrie SSH data selection, data cleaning, session-based event sequence formation, multiclass label construction, feature engineering, removal of features causing data leakage and proxy labels, tokenization, padding, and data splitting into training, validation, and testing sets. The target classification categories consist of normal, scan_probe, and brute_force. The LSTM model was evaluated using accuracy, precision, recall, F1-score, and a confusion matrix. The evaluation results show that the model achieved an accuracy of 99.30%, with macro average and weighted average precision, recall, and F1-score values of 99.30%. In addition, the model was integrated into a NIDS dashboard prototype using Flask, MongoDB, and Docker. The testing results demonstrate that the system can read Cowrie SSH logs, generate session tokens, perform predictions, store results, and display classifications with a LOGGED status. The developed system operates as a detection-only mechanism and does not perform automatic blocking.

Keywords: *Cowrie SSH, Honeypot, Long Short-Term Memory (LSTM), Multiclass, Network Intrusion Detection System (NIDS).*

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT, Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan penyusunan Tugas Akhir ini dengan baik. Skripsi ini disusun sebagai salah satu persyaratan untuk memperoleh gelar Sarjana Komputer pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta dengan judul “Analisis Kinerja Algoritma *Long Short-Term Memory* dalam Deteksi Intrusi Jaringan Berbasis Log HoneyPot Cowrie SSH”

Penyusunan Tugas Akhir ini tidak terlepas dari bantuan, dukungan, serta bimbingan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan rasa terima kasih dan penghargaan yang setinggi-tingginya kepada:

1. Kedua orang tua serta seluruh keluarga penulis yang senantiasa memberikan doa, kasih sayang, dukungan moral maupun materil, serta menjadi sumber motivasi utama dalam menyelesaikan studi.
2. Bapak Prof. Dr. Ir. Supriyanto, S.T., M.Sc., IPM, selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta sekaligus Pembimbing I, yang telah memberikan arahan, bimbingan, serta masukan yang sangat berharga selama proses penyusunan skripsi.
3. Bapak Hamonangan Kinantan P., S.T., M.T., selaku Pembimbing II, atas saran, pandangan, bimbingan teknis, dan evaluasi yang konstruktif dalam penyempurnaan penelitian ini.
4. Bapak Dr. Ridwan Raafi'udin, S.Kom., M.Kom., selaku Koordinator Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta, atas arahan dan bimbingan yang diberikan selama penulis menempuh pendidikan.
5. Teman-teman dan rekan seperjuangan mahasiswa Informatika angkatan 2022 yang telah menjadi tempat berdiskusi, bertukar pikiran, serta saling memberikan dukungan selama proses pengerjaan Tugas Akhir ini.

Penulis menyadari bahwa Tugas Akhir ini masih memiliki keterbatasan dan belum sepenuhnya sempurna. Oleh karena itu, penulis mengharapkan kritik dan saran yang bersifat membangun demi perbaikan di masa yang akan datang. Semoga hasil penelitian ini dapat memberikan manfaat dan kontribusi bagi pengembangan ilmu pengetahuan, khususnya di bidang Informatika.

Jakarta, 13 Juli 2026

Rendy Sahrasad

DAFTAR ISI

KATA PENGANTAR	viii
DAFTAR ISI.....	ix
DAFTAR GAMBAR	xii
DAFTAR TABEL	xiii
DAFTAR RUMUS	xv
BAB 1. PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah.....	3
1.3. Batasan Masalah	3
1.4. Tujuan dan Manfaat Penelitian	4
1.4.1. Tujuan Penelitian	4
1.4.2. Manfaat Penelitian	4
1.5. Sistematika Penulisan	5
BAB 2. TINJAUAN PUSTAKA	6
2.1. Keamanan Jaringan.....	6
2.2. Ancaman Jaringan.....	6
2.3. Pertahanan Jaringan	6
2.4. Intrusion Detection System.....	7
2.4.1. Jenis Intrusion Detection System (IDS)	8
2.4.1.1. Host Intrusion Detection System (HIDS)	8
2.4.1.2. Network Intrusion Detection System (NIDS)	8
2.5. Deep Learning & Recurrent Neural Network (RNN).....	9
2.5.1. Long Short-Term Memory (LSTM)	10
2.6. Honeypot.....	12
2.7. Pre-processing Data	13
2.8. Data Cleaning	13
2.9. Log Berbasis Event Sequence dan Session.....	13
2.10. Data Leakage dan Proxy Label	14
2.11. Tokenization dan Padding Data	15
2.12. Feature Scaling	15

2.13.	Evaluasi Model	16
2.14.	Tensorflow	17
2.15.	<i>Rapid Application Development (RAD)</i>	17
2.16.	Python	18
2.17.	Implementasi Sistem Dashboard	18
2.17.1.	Flask	19
2.17.2.	Keras.....	19
2.17.3.	Docker	20
2.17.4.	MongoDB.....	20
2.18.	Penelitian Terdahulu	21
BAB 3. METODE PENELITIAN.....		27
3.1.	Tahapan Penelitian.....	27
3.1.1.	Identifikasi Masalah	29
3.1.2.	Studi Literatur.....	29
3.1.3.	Pengumpulan Data	29
3.1.4.	Preprocessing Data	32
3.1.5.	Pengembangan Model	38
3.1.6.	Evaluasi Model.....	39
3.1.7.	Rancangan Awal Sistem Web	39
3.1.8.	Implementasi Sistem Web.....	41
3.1.9.	Pengujian Sistem Web.....	42
3.2.	Perangkat Penelitian	42
3.2.1.	Perangkat Keras	42
BAB 4. HASIL DAN PEMBAHASAN.....		43
4.1.	Hasil Identifikasi Dataset Mentah.....	43
4.1.1.	Struktur Dataset Mentah.....	43
4.1.2.	Jumlah Data dan Distribusi Awal.....	44
4.1.3.	Hasil Seleksi Log Cowrie SSH	45
4.1.4.	Karakteristik Log Cowrie SSH	46
4.2.	Hasil Preprocessing Data	47
4.2.1.	Seleksi Data Cowrie SSH.....	48
4.2.2.	Pembentukan Event Behavior Session.....	48

4.2.3.	Pembentukan Label Multiclass	49
4.2.4.	Hasil Feature Engineering	49
4.2.5.	Penghapusan Fitur Data Leakage dan Proxy Label .	50
4.2.6.	Pembentukan Dataset	53
4.2.7.	Tokenisasi dan Padding Event Sequence	54
4.2.8.	Pembentukan Tensor Input LSTM.....	56
4.3.	Pelatihan Model LSTM	56
4.3.1.	Arsitektur Model LSTM.....	57
4.3.2.	Konfigurasi Training Model.....	59
4.3.3.	Proses dan Hasil Training	60
4.3.4.	Penyimpanan Model dan Komponen Preprocessing	63
4.4.	Evaluasi Model	64
4.4.1.	Accuracy, Precision, Recall, dan F1-Score	64
4.4.2.	Confusion Matrix	65
4.4.3.	Analisis Hasil Prediksi per Kelas	66
4.5.	Implementasi Dashboard	68
4.5.1.	Arsitektur Sistem Dashboard	68
4.5.2.	Integrasi Model LSTM dengan Dashboard.....	69
4.5.3.	Tampilan dan Fitur Dashboard.....	70
4.5.4.	Pembacaan Log Cowrie pada Dashboard.....	72
4.6.	Pengujian Sistem.....	74
4.6.1.	Lingkup Pengujian Docker.....	74
4.6.2.	Skenario Pengujian Scan Probe.....	75
4.6.3.	Skenario Pengujian Brute Force.....	77
4.6.4.	Skenario Pengujian Normal	79
4.6.5.	Perbandingan Prediksi Model dengan Log Aktual ..	81
4.6.6.	Analisis Hasil Pengujian Sistem	83
4.6.7.	Keterbatasan Pengujian Sistem	84
BAB 5.	PENUTUP	85
5.1.	Kesimpulan	85
5.2.	Saran	85
DAFTAR	PUSTAKA	87

DAFTAR GAMBAR

Gambar 2.1 Intrusion Detection System Concept.....	8
Gambar 2.2 Arsitektur <i>Recurrent Neural Network</i>	10
Gambar 2.3 Proses Algoritma LSTM	11
Gambar 2.4 Model RAD	17
Gambar 3.1 Alur Tahapan Penelitian.....	28
Gambar 3.2 Collection Honeypot UPN	30
Gambar 3.3 UML Rancangan Awal Sistem Web	40
Gambar 4.2 Alur Pembentukan Dataset Final	52
Gambar 4.3 Arsitektur Model LSTM Multiclass.....	58
Gambar 4.5 Grafik Training Loss dan Validation Loss.....	63
Gambar 4.6 Heatmap Confusion Matrix.....	66
Gambar 4.8 Tampilan Overview Dashboard	71
Gambar 4.9 Tampilan Recent Predictions	72
Gambar 4.10 UML Sequence Diagram Pengujian Scan Probe.....	76
Gambar 4.11 UML Sequence Diagram Pengujian Brute Force.....	78
Gambar 4.12 UML Sequence Diagram Pengujian Normal	80

DAFTAR TABEL

Tabel 3.1 Rincian Atribut Dataset Cowrie SSH	31
Tabel 3.2 Tabel Tahapan Preprocessing Data.....	32
Tabel 3.3 Tabel Kelas Label Multiclass.....	34
Tabel 3.4 Tabel Fitur Dataset Final.....	35
Tabel 3.5 Tabel Fitur Yang Tidak Digunakan sebagai Input Model	36
Tabel 4.1 Event Behavior Sequence	43
Tabel 4.2 Ringkasan Dataset Mentah.....	45
Tabel 4.3 Event Cowrie SSH yang digunakan.....	45
Tabel 4.4 Karakteristik Umum Log Cowrie SSH	47
Tabel 4.5 Hasil Seleksi Data Cowrie SSH	48
Tabel 4.6 Tabel Mapping Label Multiclass	49
Tabel 4.7 Kolom Dataset Hasil Feature Engineering.....	50
Tabel 4.8 Input dan Target Model LSTM.....	50
Tabel 4.9 Input dan Target Model LSTM.....	51
Tabel 4.10 Distribusi Dataset Sebelum Penyeimbangan	53
Tabel 4.11 Distribusi Dataset Final.....	53
Tabel 4.12 Mapping Token Event.....	54
Tabel 4.13 Contoh Tokenisasi dan Padding Event Sequence	55
Tabel 4.14 Bentuk Tensor Input Model LSTM	56
Tabel 4.15 Ringkasan Arsitektur Model LSTM	57
Tabel 4.16 Ringkasan Arsitektur Model LSTM	60
Tabel 4.17 Hasil Training Model LSTM	60
Tabel 4.18 Komponen yang disimpan setelah pelatihan.....	63
Tabel 4.19 Hasil Evaluasi Model LSTM	64
Tabel 4.20 Confusion Matrix Model LSTM	65
Tabel 4.21 Ringkasan Analisis Prediksi per Kelas	67
Tabel 4.22 Ringkasan Analisis Prediksi per Kelas	68
Tabel 4.23 Alur Integrasi Model.....	69
Tabel 4.24 Fitur Dashboard.....	71
Tabel 4.25 Mapping Token yang Ditampilkan pada Dashboard	73
Tabel 4.26 Contoh Hasil Pembacaan Log pada Dashboard.....	73

Tabel 4.27 Lingkungan Pengujian Sistem	75
Tabel 4.28 Skenario Pengujian Scan Probe	76
Tabel 4.29 Hasil Pengujian Scan Probe	77
Tabel 4.30 Skenario Pengujian Brute Force	78
Tabel 4.31 Hasil Pengujian Brute Force	79
Tabel 4.32 Skenario Pengujian Normal	80
Tabel 4.33 Hasil Pengujian Normal	81
Tabel 4.34 Perbandingan Hasil Prediksi Model dengan Log Aktual.....	82

DAFTAR RUMUS

Rumus 2.5.1 Forget Gate	11
Rumus 2.5.2 Input Gate	11
Rumus 2.5.3 Input Gate	11
Rumus 2.5.4 Cell State	11
Rumus 2.5.5 Output Gate.....	12
Rumus 2.5.6 Output Gate	12