SISTEM KEAMANAN DATA IOT BERBASIS ENKRIPSI AES-128 DAN DETEKSI ANOMALI LSTM DENGAN OPTIMASI TENSORFLOW LITE PADA PERANGKAT EDGE

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Informatika

disusun oleh

YUNUS EKA PRASETYANTO

22.11.4976

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

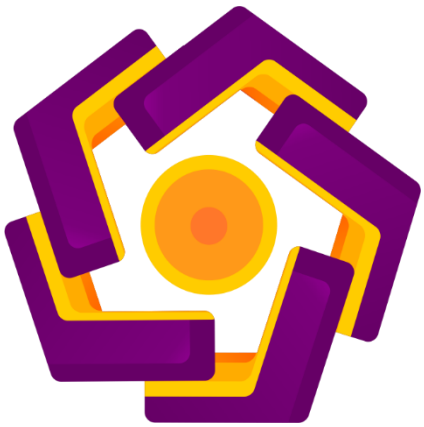
2026

SISTEM KEAMANAN DATA IOT BERBASIS ENKRIPSI AES-128 DAN DETEKSI ANOMALI LSTM DENGAN OPTIMASI TENSORFLOW LITE PADA PERANGKAT EDGE

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Informatika



disusun oleh

YUNUS EKA PRASETYANTO

22.11.4976

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

HALAMAN PERSETUJUAN

SKRIPSI

SISTEM KEAMANAN DATA IOT BERBASIS ENKRIPSI AES-128 DAN DETEKSI ANOMALI LSTM DENGAN OPTIMASI TENSORFLOW LITE PADA PERANGKAT EDGE

yang disusun dan diajukan oleh

Yunus Eka Prasetyanto

22.11.4976

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 26 Februari 2026

Dosen Pembimbing,

Muhammad Tofa Nurcholis, M.Kom
NIK. 190302281

HALAMAN PENGESAHAN

SKRIPSI

SISTEM KEAMANAN DATA IOT BERBASIS ENKRIPSI AES-128 DAN DETEKSI ANOMALI LSTM DENGAN OPTIMASI TENSORFLOW LITE PADA PERANGKAT EDGE

yang disusun dan diajukan oleh

Yunus Eka Prasetyanto

22.11.4976

Telah dipertahankan di depan Dewan Penguji
pada tanggal 26 Februari 2026

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Yudi Sutanto, M.Kom **NIK. 190302039**	
Andika Agus Slameto, M.Kom **NIK. 190302109**	
Muhammad Tofa Nurcholis, M.Kom **NIK. 190302281**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 26 Februari 2026

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Yunus Eka Prasetyanto
NIM : 22.11.4976

Menyatakan bahwa Skripsi dengan judul berikut:

Sistem Keamanan Data IoT Berbasis Enkripsi AES-128 dan Deteksi Anomali LSTM dengan Optimasi TensorFlow Lite pada Perangkat Edge

Dosen Pembimbing : Muhammad Tofa Nurcholis, M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 26 Februari 2026

Yang Menyatakan,

Yunus Eka Prasetyanto

HALAMAN PERSEMBAHAN

Skripsi ini disusun dan dipersembahkan sebagai bentuk tanggung jawab akademik penulis kepada berbagai pihak yang telah memberikan kontribusi dan dukungan selama proses pendidikan dan penyusunan skripsi.

Pertama, skripsi ini penulis persembahkan kepada orang tua dan keluarga yang senantiasa memberikan dukungan, perhatian, serta doa yang berkesinambungan, sehingga penulis dapat menyelesaikan seluruh tahapan studi dengan baik. Dukungan tersebut menjadi motivasi utama bagi penulis dalam menghadapi berbagai tantangan selama proses penyusunan skripsi.

Selanjutnya, skripsi ini penulis persembahkan kepada Bapak Muhammad Tofa Nurcholis, M.Kom selaku dosen pembimbing serta seluruh dosen Program Studi Informatika Fakultas Ilmu Komputer Universitas Amikom Yogyakarta yang telah memberikan bimbingan akademik, arahan, serta ilmu pengetahuan yang sangat bermanfaat bagi penulis.

Skripsi ini juga penulis persembahkan kepada almamater Universitas Amikom Yogyakarta sebagai institusi pendidikan yang telah menyediakan sarana, prasarana, serta lingkungan akademik yang mendukung pengembangan pengetahuan dan kemampuan penulis selama masa studi.

Akhir kata, skripsi ini dipersembahkan sebagai bentuk kontribusi akademik penulis bagi pengembangan ilmu pengetahuan, khususnya di bidang informatika, serta sebagai salah satu hasil dari proses pembelajaran yang telah ditempuh.

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Sistem Keamanan Data IoT Berbasis Enkripsi AES-128 dan Deteksi Anomali LSTM dengan Optimasi TensorFlow Lite pada Perangkat Edge" dengan baik. Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana pada Program Studi Informatika Fakultas Ilmu Komputer Universitas Amikom Yogyakarta. Pada kesempatan ini penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Orang tua dan keluarga penulis yang senantiasa memberikan doa, motivasi, dukungan moral, serta semangat yang tidak ternilai harganya.
2. Bapak Muhammad Tofa Nurcholis, M.Kom selaku Dosen Pembimbing yang telah meluangkan waktu, tenaga, dan pikiran dalam memberikan bimbingan, arahan, serta masukan selama proses penyusunan skripsi ini.
3. Ibu Eli Pujiastuti, M.Kom selaku Ketua Program Studi Informatika Fakultas Ilmu Komputer Universitas Amikom Yogyakara.
4. Bapak Tim Dosen Penguji yang telah memberikan evaluasi, saran, dan masukan yang membangun demi penyempurnaan skripsi ini.
5. Seluruh dosen dan staf Fakultas Ilmu Komputer Universitas Amikom Yogyakarta yang telah memberikan ilmu pengetahuan serta pelayanan akademik selama penulis menempuh pendidikan.

Penulis menyadari bahwa skripsi ini masih memiliki keterbatasan dan jauh dari kesempurnaan. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang bersifat membangun guna penyempurnaan di masa yang akan datang. Akhir kata, penulis berharap skripsi ini dapat memberikan manfaat bagi pengembangan ilmu pengetahuan, khususnya di bidang keamanan data dan teknologi Internet of Things.

Yogyakarta, 29 September 2025

Penulis

DAFTAR ISI

HALAMAN JUDUL i
HALAMAN PERSETUJUAN ii
HALAMAN PENGESAHAN iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI iv
HALAMAN PERSEMBAHAN v
KATA PENGANTAR vi
DAFTAR ISI vii
DAFTAR TABEL ix
DAFTAR GAMBAR x
DAFTAR LAMPIRAN xi
DAFTAR LAMBANG DAN SINGKATAN xii
DAFTAR ISTILAH xvi
INTISARI xxxi
ABSTRACT xxxii
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 4
1.3 Batasan Masalah 4
1.4 Tujuan Penelitian 5
1.5 Manfaat Penelitian 5
1.6 Sistematika Penulisan 6
BAB II TINJAUAN PUSTAKA 7
2.1 Studi Literatur 7
2.2 Dasar Teori 13
2.2.1 Internet of Things (IoT) 13
2.2.2 Keamanan Data pada IoT 14
2.2.3 Advanced Encryption Standard (AES) 14
2.2.4 Deteksi Anomali dalam Keamanan IoT 16
2.2.5 Long Short-Term Memory (LSTM) 17
2.2.6 Optimasi Model pada Edge Device (TensorFlow Lite) 19
2.2.7 Dataset CICIoT2023 23
BAB III METODE PENELITIAN 26

3.1 Objek Penelitian 26
3.2 Alur Penelitian 26
3.3 Tahapan Penelitian 28
3.3.1 Akuisisi Data 28
3.3.2 Preprocessing Data 28
3.3.3 Pelatihan Model 30
3.3.4 Perancangan Simulasi 31
3.3.5 Implementasi dan Pengujian 34
3.3.6 Evaluasi dan Analisis 35
3.4 Alat dan Bahan 35
3.4.1 Bahan Penelitian (Dataset) 35
3.4.2 Alat (Instrumen Pengembangan) 36
BAB IV HASIL DAN PEMBAHASAN 37
4.1 Akuisisi Data 37
4.2 Preprocessing Data 38
4.2.1 Data Cleaning dan Label Encoding 38
4.2.2 Handling Imbalanced Data 38
4.2.3 Normalisasi dan Reshaping 39
4.3 Pelatihan Model 40
4.3.1 Arsitektur Model LSTM 40
4.4 Perancangan Simulasi 42
4.4.1 Simulasi, Konversi, dan Optimasi Model TFLite 42
4.5 Implementasi dan Pengujian Sistem 43
4.5.1 Pengujian Modul Kriptografi Terisolasi (VM 32-bit) 43
4.5.2 Penyesuaian Lingkungan untuk Integrasi TFLite 45
4.5.3 Hasil Eksekusi Sistem Terintegrasi End-to-End (Google Colab 64-bit) 45
4.6 Evaluasi dan Analisis 48
4.6.1 Analisis Metrik Klasifikasi 48
4.6.2 Analisis Efisiensi Komputasi (Komparasi Model .h5 dan .tflite) 51
BAB V PENUTUP 55
5.1 Kesimpulan 55
5.2 Saran 57
REFERENSI 58
LAMPIRAN 61

DAFTAR TABEL

Tabel 2.1 Keaslian Penelitian 10
Tabel 2.2 Klasifikasi Fitur dalam *Dataset* CICIoT2023..... 25
Tabel 3.1 Spesifikasi Teknis AES 34
Tabel 3.2 Daftar Alat Pengembangan.....36
Tabel 4.1 Spesifikasi *Hyperparameter* 40
Tabel 4.2 Laporan Klasifikasi.....50
Tabel 4.3 Ringkasan Statistik Latensi Inferensi dari Lima Kali Pengujian 54

DAFTAR GAMBAR

Gambar 2.1 CIA Triad 14
Gambar 2.2 Struktur Blok Enkripsi AES 16
Gambar 2.3 Arsitektur Dasar LSTM 19
Gambar 2.4 Topologi Jaringan Pengambilan Data 24
Gambar 3.1 Alur Penelitian 27
Gambar 3.2 Arsitektur Sistem *Training* di Cloud 32
Gambar 3.3 Instansi Linux berarsitektur 64-bit (Google Colab) 33
Gambar 3.4 Arsitektur Sistem Implementasi di VM Raspberry Pi 33
Gambar 4.1 Proses Akuisisi Data 37
Gambar 4.2 *Preprocessing* Data Awal 38
Gambar 4.3 Distribusi Data Setelah SMOTE 39
Gambar 4.4 Normalisasi dan *Reshaping* 39
Gambar 4.5 Arsitektur Model LSTM 40
Gambar 4.6 Kode eksekusi teknik *Stratified Data Splitting* 41
Gambar 4.7 Proses Pelatihan Model LSTM 41
Gambar 4.8 Grafik Riwayat Pelatihan Model 42
Gambar 4.9 Konversi Model Format .h5 ke .tflite 43
Gambar 4.10 Hasil Pengujian Modul Kriptografi AES-128 pada VM 32-bit 44
Gambar 4.11 Log Sistem Integrasi AES dan TFLite *End-to-End* 46
Gambar 4.12 *Confusion Matrix* 48
Gambar 4.13 *Output* Kode Laporan Klasifikasi 49
Gambar 4.14 Hasil Pengujian Latensi Komparatif Run 1 51
Gambar 4.15 Hasil Pengujian Latensi Komparatif Run 2 52
Gambar 4.16 Hasil Pengujian Latensi Komparatif Run 3 52
Gambar 4.17 Hasil Pengujian Latensi Komparatif Run 4 53
Gambar 4.18 Hasil Pengujian Latensi Komparatif Run 5 53

DAFTAR LAMPIRAN

Lampiran 1 Kode Pelatihan Model LSTM dan Konversi TFLite 61
Lampiran 2 Kode Pengujian Modul Kriptografi AES-128 pada VM 32-Bit.....66
Lampiran 3 Kode Simulasi Integrasi AES dan TFLite End-to-End 67

DAFTAR LAMBANG DAN SINGKATAN

ACK	Acknowledgment Flag (TCP)
AES	Advanced Encryption Standard
AI	Artificial Intelligence
ARP	Address Resolution Protocol
BiLSTM	Bidirectional Long Short-Term Memory
CBC	Cipher Block Chaining
CIA	Confidentiality, Integrity, Availability
CNN	Convolutional Neural Network
CoAP	Constrained Application Protocol
CWR	Congestion Window Reduced Flag (TCP)
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DDoS	Distributed Denial of Service
ECDH	Elliptic-Curve Diffie–Hellman
ECE	ECN-Echo Flag (TCP)

ESP32	Espressif Systems 32-bit Microcontroller
FFT	Fast Fourier Transform
FIN	Finish Flag (TCP)
FN	False Negative
FP	False Positive
GPU	Graphics Processing Unit
GRU	Gated Recurrent Unit
HDF5	Hierarchical Data Format version 5 (.h5)
HTTP	Hypertext Transfer Protocol
IAT	Inter-Arrival Time
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IIoT	Industrial Internet of Things
IoT	Internet of Things
IoV	Internet of Vehicles
IPsec	Internet Protocol Security
IPv	Internet Protocol version

IRC	Internet Relay Chat
IV	Initialization Vector
LLC	Logical Link Control
LSTM	Long Short-Term Memory
MITM	Man In The Middle
MQTT	Message Queuing Telemetry Transport
NaN	Not a Number
NIST	National Institute of Standards and Technology
PC	Personal Computer
PKCS7	Public-Key Cryptography Standards #7
PSH	Push Flag (TCP)
RNN	Recurrent Neural Network
RSA	Rivest–Shamir–Adleman
RST	Reset Flag (TCP)
SBC	Single Board Computer
SENet	Squeeze-and-Excitation Network
SMTP	Simple Mail Transfer Protocol

SMOTE	Synthetic Minority Over-sampling Technique
SQL	Structured Query Language
SSH	Secure Shell
SVM	Support Vector Machine
SYN	Synchronize Flag (TCP)
TCP	Transmission Control Protocol
TFLite	TensorFlow Lite
TLS	Transport Layer Security
UDP	User Datagram Protocol
VM	Virtual Machine
XSS	Cross-Site Scripting

DAFTAR ISTILAH

Accuracy	Proporsi prediksi yang benar secara keseluruhan.
Actuator (Aktuator)	Perangkat mekanis atau elektrik yang mengubah sinyal kontrol menjadi gerakan mekanis atau tindakan fisik dalam sistem IoT.
Adam (Adaptive Moment Estimation)	Algoritma optimasi algoritma *machine learning* yang sangat efisien dalam memperbarui bobot jaringan secara adaptif selama pelatihan.
Anomaly Detection	Proses identifikasi pola dalam data yang menyimpang dari perilaku normal.
Application Layer	Lapisan dalam model arsitektur jaringan tempat aplikasi pengguna beroperasi.
At-rest	Status data yang sedang disimpan dalam media penyimpanan.
Attention Mechanism	Komponen dalam model *deep learning* yang memungkinkan jaringan untuk memfokuskan perhatian pada bagian spesifik dari data *input*.
Autoencoder	Jenis jaringan saraf tiruan yang digunakan untuk pembelajaran representasi data, sering dipakai untuk deteksi anomali.
Batch Size	Jumlah sampel data latih yang diproses dalam satu kali iterasi sebelum model memperbarui parameter bobotnya.

Benchmark	Tolok ukur atau standar yang digunakan untuk membandingkan kinerja suatu sistem atau model.
Benign	Istilah untuk klasifikasi data atau trafik jaringan yang bersifat normal (bukan serangan).
Binary Crossentropy	Fungsi kerugian (*loss function*) yang umum digunakan dalam masalah klasifikasi dua kelas (biner) untuk mengukur seberapa jauh prediksi model dari label sebenarnya.
Block Cipher	Algoritma kriptografi yang mengenkripsi data dalam blok-blok berukuran tetap.
Botnet	Sekumpulan perangkat yang terhubung ke internet dan telah disusupi oleh *malware*, digunakan secara bersamaan oleh penyerang untuk melakukan tugas otomatis seperti serangan DDoS.
Bottleneck	Titik kemacetan dalam suatu sistem komputasi atau jaringan yang memperlambat kinerja keseluruhan aliran data.
Brute-force Attack	Metode serangan kriptografi dengan mencoba semua kombinasi kunci yang mungkin hingga menemukan kunci yang benar.
CIA Triad	Model kerangka kerja inti dalam keamanan informasi yang terdiri dari *Confidentiality*, *Integrity*, dan *Availability*.
Cipher Block Chaining (CBC)	Mode operasi algoritma *block cipher* di mana setiap blok *plaintext* di-XOR dengan blok *ciphertext* sebelumnya sebelum dienkripsi..
Ciphertext	Data atau informasi yang telah diubah melalui enkripsi menjadi bentuk tidak terbaca.

Cloud	Model komputasi yang menyediakan sumber daya (seperti server, penyimpanan) melalui internet.
Concatenation	Operasi penggabungan dua atau lebih vektor/untaian data menjadi satu kesatuan.
Confidentiality	Aspek keamanan informasi yang menjamin data hanya dapat diakses oleh pihak yang berwenang.
Confusion Matrix	Tabel yang menggambarkan performa model klasifikasi.
Covariance	Ukuran statistik yang menunjukkan hubungan linear antara dua variabel.
Data Cleaning	Proses menghapus, memperbaiki, atau mengatur data yang tidak lengkap, rusak, atau duplikat (termasuk nilai *null*/NaN).
Data in Transit	Data yang sedang dalam proses pengiriman atau bergerak melalui jaringan dari satu titik ke titik lain.
Data Leakage	Kebocoran data dalam *machine learning* di mana informasi dari luar set data latih (seperti data uji) ikut memengaruhi pelatihan model, menghasilkan evaluasi yang bias atau tidak valid.
Data Plane	Bagian dari arsitektur jaringan yang bertugas meneruskan atau membawa *payload* data pengguna.
Data Preprocessing	Tahap persiapan dan transformasi data mentah sebelum diproses oleh model.
Data Security	Praktik melindungi informasi digital dari akses yang tidak sah, korupsi, atau pencurian.

Data Tampering	Serangan yang bertujuan mengubah data secara tidak sah.
Deep Learning	Sub-bidang *machine learning* yang menggunakan jaringan saraf dengan banyak lapisan (*neural networks*).
Defense in Depth	Strategi keamanan berlapis yang menggunakan beberapa mekanisme pertahanan untuk melindungi aset informasi.
Dense Output Layer	Lapisan terakhir dalam jaringan saraf yang terhubung penuh (*fully connected*) dan bertugas menghasilkan nilai prediksi akhir.
Deployment Environment	Lingkungan di mana sistem lunak atau model diimplementasikan secara aktual untuk dijalankan.
Difusi	Sifat dalam kriptografi di mana perubahan kecil pada *plaintext* menyebabkan perubahan besar pada *ciphertext*.
Drate (Destination Rate)	Laju transfer data ke perangkat tujuan (*destination*).
Dropout Layer	Teknik dalam *deep learning* yang secara acak mengabaikan (mematikan) sebagian neuron selama pelatihan untuk mencegah *overfitting*.
Dummy Data	Data tiruan atau buatan yang digunakan untuk keperluan pengujian simulasi dan tidak merepresentasikan data asli.
Dynamic Key Exchange	Mekanisme pertukaran kunci kriptografi secara dinamis dan otomatis antara dua pihak yang berkomunikasi untuk meningkatkan keamanan.

Dynamic Range Quantization	Teknik kuantisasi model *machine learning* di mana bobot dikuantisasi pasca-pelatihan dari *floating-point* ke *integer*, namun aktivasi dikuantisasi secara dinamis selama proses inferensi berjalan.
Edge Device	Perangkat keras yang berada di ujung jaringan (dekat sumber data) yang bertugas mengumpulkan atau memproses data sebelum dikirim ke server pusat.
Element-wise Multiplication	Operasi matematika di mana setiap elemen dalam satu matriks/vektor dikalikan dengan elemen pada posisi yang sama di matriks/vektor lain.
Embedded System	Sistem komputer khusus yang dirancang untuk melakukan satu atau beberapa fungsi dedikasi tertentu.
Encoding Kategorikal (Label Encoding)	Teknik mengubah data kategori (teks) menjadi bentuk numerik biner atau bilangan bulat.
Encryption	Proses mengamankan informasi dengan mengubah data asli (*plaintext*) menjadi bentuk tersandi (*ciphertext*).
End-to-End Encryption	Sistem komunikasi di mana hanya orang yang berkomunikasi yang dapat membaca pesannya.
End-to-End Latency	Total waktu pemrosesan dari ujung awal pengiriman hingga ujung akhir penerimaan atau pemrosesan hasil.
Ensemble Model	Teknik yang menggabungkan beberapa model *machine learning* untuk meningkatkan performa prediksi.
Epoch	Satu siklus penuh di mana keseluruhan *dataset* pelatihan telah dilewatkan maju dan mundur melalui jaringan saraf.

Exploding Gradient	Masalah dalam pelatihan jaringan saraf di mana nilai gradien menjadi terlalu besar, menyebabkan model menjadi tidak stabil.
False Alarm	Peringatan palsu yang dihasilkan sistem ketika mendeteksi aktivitas jaringan normal sebagai sebuah serangan (sinonim dengan *False Positive*).
False Negative	Hasil prediksi yang salah di mana sistem mengidentifikasi aktivitas berbahaya/serangan sebagai aktivitas normal.
False Positive	Hasil prediksi yang salah di mana sistem mengidentifikasi aktivitas normal sebagai ancaman atau anomali.
Feature Engineering	Proses manipulasi variabel data mentah untuk meningkatkan performa model.
Feature Selection	Proses memilih *subset* fitur paling relevan dari *dataset* untuk meningkatkan performa model dan mengurangi beban komputasi.
Federated Learning	Paradigma *machine learning* di mana model dilatih secara terdesentralisasi di banyak perangkat.
Floating-point	Format representasi angka dalam komputer yang dapat merepresentasikan bilangan real (misal: *float32*).
Flood (TCP/UDP/ICMP)	Teknik serangan DoS/DDoS dengan membanjiri server target menggunakan paket data masif.
Flow	Sekumpulan paket yang berbagi karakteristik umum seperti alamat IP sumber/tujuan.

Flow Duration	Durasi total dari suatu aliran komunikasi (*flow*) antara sumber dan tujuan.
Forget Gate	Gerbang arsitektur LSTM untuk menentukan informasi masa lalu mana yang harus dibuang dari *memory cell*.
Framework	Kerangka kerja perangkat lunak yang menyediakan struktur dasar (contoh: TensorFlow, Keras).
Full Integer Quantization	Teknik kuantisasi di mana seluruh bobot dan aktivasi matematika dalam model dikonversi sepenuhnya ke format *integer* (bilangan bulat) untuk mempercepat komputasi pada perangkat tanpa unit *floating-point*.
Gap	Kesenjangan atau celah yang belum terisi dalam suatu bidang penelitian atau pengetahuan.
Gateway	Perangkat atau titik koneksi jaringan yang menjembatani jalur komunikasi antara dua jaringan dengan protokol yang berbeda.
Header Length	Panjang bagian *header* dari sebuah paket data jaringan.
Hidden State	Vektor dalam *Recurrent Neural Network* yang menyimpan memori jangka pendek.
Hybrid System	Sistem yang dibangun dengan mengintegrasikan dua pendekatan atau teknologi yang berbeda.
Imbalanced Dataset	Kondisi dalam *dataset* klasifikasi di mana jumlah sampel pada satu kelas jauh lebih banyak atau lebih sedikit dibandingkan kelas lainnya.

In-transit	Status data yang sedang dikirimkan melalui jaringan.
Initialization Vector (IV)	Blok data acak yang digunakan bersama kunci rahasia untuk memulai proses enkripsi agar pola *ciphertext* tidak berulang.
Input Gate	Gerbang dalam arsitektur LSTM yang menentukan informasi baru untuk dimasukkan ke *memory cell*.
Input Layer	Lapisan paling awal pada *neural network* yang bertugas menerima data mentah.
Integer	Tipe data numerik yang merepresentasikan bilangan bulat (misal: *int8*).
Integrity	Aspek keamanan informasi yang menjamin keakuratan dan kelengkapan data.
Intrusion	Aktivitas tidak sah atau berbahaya yang memasuki/mengganggu sistem.
Intrusion Detection	Proses memantau kejadian dalam sistem atau jaringan untuk mengidentifikasi pelanggaran keamanan.
Key (Kunci)	Deretan bit yang digunakan oleh algoritma kriptografi untuk mengenkripsi/mendekripsi data.
Key Generation (Keygen)	Proses menghasilkan kunci kriptografi.
Key Management	Pengelolaan kunci kriptografi dalam sistem keamanan.
Learning Privacy	Konsep perlindungan data di mana model dilatih tanpa mengekspos data mentah (*privacy-preserving*).

Library	Kumpulan kode/fungsi siap pakai dalam pemrograman.
Lightweight	Sifat dari model atau algoritma yang dirancang agar ringan dan efisien sumber daya.
Lossless	Proses kompresi atau transformasi data yang memungkinkan pemulihan data asli secara utuh tanpa ada informasi yang hilang.
Machine Learning	Bidang ilmu yang memberi kemampuan pada komputer untuk belajar dari data.
Malicious	Istilah untuk perangkat lunak, trafik, atau tindakan yang bersifat merusak, berbahaya, atau bermuatan serangan.
Memory Cell	Unit fundamental dalam jaringan LSTM yang berfungsi menyimpan informasi.
Metric	Ukuran kuantitatif untuk mengevaluasi performa model.
Min-Max Scaling (Normalization)	Metode normalisasi yang mengubah skala nilai fitur ke rentang tertentu, biasanya [0, 1].
Multiclass Classification	Klasifikasi di mana data dikelompokkan ke dalam lebih dari dua kelas berbeda.
Native Deployment	Implementasi sistem, perangkat lunak, atau model secara langsung pada lingkungan perangkat keras asli (fisik) tanpa melalui lapisan simulasi atau virtualisasi.
Network Layer	Lapisan dalam arsitektur IoT yang menangani transmisi dan perutean data.

Network Plane	Bagian dari arsitektur jaringan yang mengelola perutean, manajemen lalu lintas, dan topologi jaringan secara keseluruhan.
Network Traffic	Volume data yang dikirim dan diterima melalui suatu jaringan.
Online Learning	Pelatihan model di mana data diproses berurutan dan model diperbarui bertahap.
Operation Folding	Teknik optimasi selama konversi model *machine learning* yang menggabungkan beberapa operasi matematika menjadi satu instruksi sederhana untuk mempercepat pemrosesan.
Output Gate	Gerbang dalam LSTM yang mengontrol informasi untuk diteruskan sebagai *output*.
Overfitting	Kondisi di mana model *machine learning* terlalu mengingat data latih sehingga kehilangan kemampuannya untuk memprediksi data baru secara akurat.
Overhead	Beban komputasi tambahan (seperti memori atau waktu pemrosesan) yang dibutuhkan oleh sebuah sistem untuk menjalankan tugas-tugas pendukung di luar fungsi utamanya.
Packet	Unit dasar data yang ditransmisikan melalui jaringan.
Padding	Penambahan bit ekstra (biasanya ke dalam blok terakhir data) agar panjang data memenuhi ukuran blok algoritma enkripsi (seperti PKCS7).
Payload	Bagian muatan inti dari paket data yang dikirimkan melalui jaringan.

Perception Layer	Lapisan terbawah arsitektur IoT yang terdiri dari sensor fisik.
Permutation (Permutasi)	Operasi dalam kriptografi untuk mengubah urutan atau posisi unit data.
Plaintext	Data informasi dalam bentuk asli sebelum dienkripsi.
Plotting	Proses membuat grafik atau visualisasi data.
Port Scan	Teknik untuk menemukan *port* terbuka pada sistem target.
Power Consumption	Jumlah energi listrik (daya) yang dikonsumsi oleh perangkat keras selama beroperasi, menjadi metrik penting dalam sistem IoT.
Precision	Proporsi prediksi positif yang benar di antara semua prediksi positif.
Prediction	Fase penggunaan model terlatih untuk membuat prediksi pada data baru.
Protocol Type	Jenis protokol komunikasi (misal: TCP, UDP).
Pruning	Teknik pemangkasan dalam *deep learning* yang menghapus bobot atau neuron yang tidak terlalu signifikan untuk mengurangi ukuran model tanpa mengorbankan akurasi secara drastis.
Quantization (Kuantisasi)	Teknik optimasi model dengan mengurangi presisi angka bobot model (misal *float32* ke *int8*) agar inferensi lebih cepat.

Random Sampling	Teknik pengambilan sampel data secara acak sehingga setiap unit data memiliki probabilitas yang sama untuk terpilih.
Rate	Laju transfer data (misal: bit per detik).
Real-time	Pemrosesan data yang merespons secara langsung tanpa jeda yang signifikan.
Recall	Proporsi kasus positif yang berhasil diidentifikasi oleh model (Sensitivitas).
Reconnaissance (Recon)	Tahap di mana penyerang mengumpulkan informasi dan memindai celah keamanan target.
Record	Satu unit baris data dalam kumpulan data.
Reinforcement Learning	Paradigma *machine learning* berbasis imbalan (*reward*).
Reshaping	Proses mengubah struktur dimensi array data agar sesuai dengan format *input* yang diminta oleh algoritma (misal: data 2D menjadi 3D).
Resource-constrained	Kondisi keterbatasan sumber daya pada perangkat keras (daya, memori, komputasi).
Round Key	Kunci turunan untuk digunakan pada setiap ronde enkripsi.
Rounds (Ronde)	Siklus transformasi yang diulang dalam *block cipher*.

Runtime	Lingkungan komputasi di mana sebuah program atau model dieksekusi secara nyata.
Security Posture	Tingkat kesiapan postur keamanan siber suatu organisasi.
Self-supervised	Pembelajaran di mana model belajar dari data tak berlabel dengan menghasilkan labelnya sendiri.
Semi-supervised Learning	Pembelajaran yang menggunakan sedikit data berlabel dan banyak data tidak berlabel.
Sigmoid	Fungsi aktivasi matematika yang memetakan *input* ke rentang 0 dan 1.
Sliding Window	Teknik segmentasi data deret waktu menjadi sekuens berurutan yang saling tumpang tindih untuk keperluan pelatihan model.
Smart Grid	Jaringan listrik cerdas berteknologi digital.
Sniffing	Teknik memantau dan menangkap paket data di jaringan.
Speedup	Metrik yang menunjukkan rasio peningkatan kecepatan pemrosesan model sebelum dan sesudah dioptimasi.
Spoofing	Serangan di mana penyerang menyamar sebagai sistem yang sah.
SQL Injection	Serangan web dengan menyisipkan perintah SQL berbahaya.

Srate (Source Rate)	Laju transfer data dari perangkat sumber (*source*).
State	Representasi sementara blok data dalam AES.
Stratified Data Splitting	Teknik pembagian *dataset* (misal untuk latih dan uji) yang memastikan bahwa proporsi antar kelas (misal kelas normal dan serangan) tetap seimbang dan mewakili populasi aslinya.
Substitution (Substitusi)	Operasi di mana satu unit data diganti dengan unit lainnya.
Substitution-box (S-Box)	Tabel pencarian untuk substitusi non-linier.
Supervised Learning	Pembelajaran menggunakan pasangan *input* dan target yang sudah memiliki label.
Symmetric Key Cryptography	Kriptografi menggunakan kunci yang sama untuk enkripsi dan dekripsi.
Testing Data (Data Uji)	*Subset* data yang dipisahkan dari data latih, digunakan secara khusus untuk mengevaluasi kinerja akhir dari model yang telah dilatih.
Three-way Handshake	Proses tiga langkah untuk membangun koneksi TCP.
Threshold	Nilai batas untuk mengambil keputusan klasifikasi.
Time-Series	Deretan data titik yang dicatat berdasarkan urutan waktu.

Timestep	Satu langkah waktu dalam pemrosesan deret waktu.
Training Environment	Infrastruktur komputasi yang didedikasikan untuk melatih model arsitektur sistem.
Training	Proses melatih model agar mengenali pola.
Unsupervised Learning	Pembelajaran pada data tanpa label untuk menemukan pola tersembunyi.
Vanishing Gradient	Masalah di mana nilai gradien menjadi mendekati nol sehingga model sulit belajar.
Variance	Sebaran data dari nilai rata-rata.
XOR (Exclusive OR)	Operasi logika yang benar jika kedua *input* berbeda.
Zero-day Attack	Serangan yang mengeksploitasi kerentanan yang belum diketahui pembuat perangkat lunak.

INTISARI

Keamanan jaringan pada ekosistem *Internet of Things* (IoT) menjadi isu krusial seiring meningkatnya perangkat terhubung dengan sumber daya komputasi terbatas. Ancaman seperti penyadapan data dan serangan intrusi membahayakan integritas sistem, sementara metode deteksi konvensional kerap membebani kinerja perangkat. Penelitian ini mengusulkan sistem keamanan bertingkat yang menggabungkan kriptografi AES-128 untuk kerahasiaan data dan *Intrusion Detection System* (IDS) berbasis *Long Short-Term Memory* (LSTM) untuk deteksi anomali. Model LSTM dilatih menggunakan *dataset* CICIoT2023 dengan teknik SMOTE pada data latih untuk menyeimbangkan kelas (rasio awal normal:serangan 1:41), kemudian dioptimasi menggunakan kuantisasi dinamis TensorFlow Lite (TFLite) agar efisien dijalankan di perangkat *edge*. Pengujian dilakukan dengan mensimulasikan enkripsi secara terisolasi pada VM 32-bit dan pengujian integrasi inferensi pada lingkungan 64-bit.

Hasil penelitian menunjukkan model mampu mencapai akurasi keseluruhan sebesar 99%, dengan kemampuan mengenali kelas normal yang sangat baik (*Recall* 0,99 dan *F1-score* 0,83). Konversi ke format TFLite berhasil mempercepat waktu inferensi rata-rata hingga 134,3 kali lipat (dari 113,85 ms pada model standar menjadi 0,848 ms) tanpa mengorbankan performa deteksi. Proses enkripsi AES-128 berjalan sangat efisien dengan latensi di bawah 1 ms. Secara akumulatif, integrasi sistem keamanan enkripsi dan deteksi anomali (*end-to-end*) ini hanya menambah total beban latensi sekitar 1,0 ms, yang sangat memenuhi standar *real-time* untuk aplikasi IoT (umumnya < 100 ms). Penelitian ini membuktikan bahwa kombinasi enkripsi simetris dan deteksi anomali berbasis kecerdasan buatan yang dioptimasi sangat layak diimplementasikan pada ekosistem perangkat *edge* yang terbatas, meskipun implementasi langsung pada perangkat keras fisik masih disarankan untuk pengujian selanjutnya.

Kata kunci: IoT, LSTM, TensorFlow Lite, Deteksi Anomali, Enkripsi AES-128.

ABSTRACT

Network security in the Internet of Things (IoT) ecosystem has become critical due to the proliferation of resource-constrained connected devices. Threats such as data sniffing and intrusion attacks jeopardize system integrity, while conventional detection methods often burden device performance. This study proposes a defense-in-depth mechanism combining AES-128 cryptography for data confidentiality and a Long Short-Term Memory (LSTM)-based Intrusion Detection System (IDS) for anomaly detection. The LSTM model was trained on the CICIoT2023 dataset using SMOTE on the training set to address class imbalance (initial normal:attack ratio of 1:41), and subsequently optimized with TensorFlow Lite (TFLite) dynamic range quantization for efficient edge deployment. Experiments were conducted by simulating isolated encryption on a 32-bit VM and integrated inference on a 64-bit environment.

The results show that the model achieves an overall accuracy of 99%, with an excellent ability to recognize the normal class (Recall of 0.99 and F1-score of 0.83). Conversion to the TFLite format successfully accelerates average inference time by 134.3 times (from 113.85 ms in the standard model to 0.848 ms) without sacrificing detection performance. The AES-128 encryption process runs highly efficiently with a latency of under 1 ms. Cumulatively, the end-to-end integration of the encryption and anomaly detection security systems adds a total latency burden of only about 1.0 ms, which easily meets the real-time standard for IoT applications (typically < 100 ms). This research demonstrates that the combination of symmetric encryption and optimized AI-based anomaly detection is highly feasible for implementation in resource-constrained edge ecosystems, although direct implementation on physical hardware is still recommended for future evaluation.

Keyword: *IoT, LSTM, TensorFlow Lite, Anomaly Detection, AES-128 Encryption.*