BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi *Internet of Things* (IoT) telah mendorong adopsi perangkat pintar secara masif di berbagai sektor, mulai dari industri (*Industrial IoT*/IIoT) hingga layanan kesehatan. Cisco Annual Internet Report (2023) memproyeksikan bahwa jumlah perangkat IoT yang terhubung secara global akan mencapai 29,3 miliar pada tahun 2023, meningkat signifikan dari 11,3 miliar pada tahun 2018 [1]. Seiring dengan pertumbuhan eksponensial tersebut, laporan SonicWall (2023) mencatat bahwa volume serangan siber yang menargetkan perangkat IoT juga melonjak drastis, dengan lebih dari 112 juta serangan terdeteksi secara global sepanjang tahun 2023 [2]. Keterbatasan sumber daya komputasi pada mayoritas perangkat *edge* menjadikan jaringan IoT rentan terhadap berbagai eksploitasi, mulai dari penyadapan data (*sniffing*) hingga pengambilalihan perangkat menjadi jaringan *botnet* untuk melancarkan serangan *Distributed Denial of Service* (DDoS) [3].

Peningkatan konektivitas ini membuka celah keamanan yang serius. Tinjauan sistematis yang dilakukan oleh Almowsawi (2024) menyoroti bahwa dalam rentang tahun 2020 hingga 2024, ancaman terhadap ekosistem IoT semakin kompleks, menuntut adanya kerangka kerja keamanan generasi baru yang berbasis kecerdasan buatan [4]. Hal ini diperkuat oleh Pang dan Li (2024) yang menyatakan bahwa metode keamanan konvensional seringkali gagal menangani serangan siber modern yang dinamis pada jaringan IoT [5]. Sektor-sektor kritis sangat rentan terhadap serangan ini. Mohy-Eddine *et al.* (2023) menekankan bahwa pada *Industrial IoT* (IIoT), integritas data adalah hal mutlak, dan serangan intrusi dapat berakibat fatal pada operasional industri [6]. Serupa dengan itu, Gelenbe *et al.* (2024) menemukan bahwa pada *Health IoT* dan *Internet of Vehicles* (IoV), serangan terdistribusi dapat membahayakan keselamatan pengguna, sehingga diperlukan algoritma deteksi yang mampu belajar secara mandiri (*self-supervised*) [7].

Untuk mengatasi kerentanan pada pengiriman data, diperlukan pendekatan keamanan berlapis. Sebagai pertahanan utama kerahasiaan data, *Advanced Encryption Standard* (AES) digunakan karena efisiensinya. Atmoko (2023) dalam analisis komparatifnya membuktikan bahwa AES memiliki kinerja yang jauh lebih unggul dibandingkan *Data Encryption Standard* (DES), baik dari sisi kecepatan enkripsi maupun dekripsi [8]. Selain itu, AES dinilai lebih aman karena mampu menghasilkan kunci enkripsi yang lebih kuat dan tahan terhadap upaya pembongkaran paksa [8]. Namun, tantangan tetap ada karena banyak perangkat IoT memiliki keterbatasan daya dan memori (*resource-constrained*). Jouhari dan Guizani (2024) mencatat bahwa solusi keamanan untuk perangkat semacam ini tidak boleh membebani kinerja perangkat secara berlebihan, namun tetap harus andal dalam menangkal serangan [9].

Mengingat enkripsi saja tidak dapat mencegah anomali perilaku jaringan, diperlukan *Intrusion Detection System* (IDS) yang cerdas. *Long Short-Term Memory* (LSTM), sebuah arsitektur dari *Deep Learning*, terbukti efektif untuk kasus ini. Saurabh *et al.* (2022) mengusulkan model berbasis LSTM (LBDMIDS) yang secara signifikan meningkatkan kemampuan deteksi intrusi pada jaringan IoT dibandingkan metode tradisional [10]. Keunggulan utama LSTM terletak pada kemampuannya menangani data *time-series* dan dependensi jangka panjang, sebagaimana dijelaskan oleh Lu *et al.* (2024) yang mengembangkan metode deteksi anomali berbasis frekuensi dan LSTM [11]. Bahkan pada infrastruktur kompleks seperti *smart grid*, integrasi LSTM terbukti mampu mendeteksi anomali dengan akurasi tinggi melalui pendekatan pembelajaran terfederasi (*federated learning*) [12].

Penelitian terbaru oleh Gueriani, Kheddar, dan Mazari (2024) menjadi landasan kuat efektivitas metode ini [13]. Dalam penelitian mereka, pengujian menggunakan *dataset* modern menunjukkan bahwa pendekatan berbasis LSTM mampu mencapai performa deteksi yang superior [13]. Meskipun demikian,

tantangan dalam penerapan *Deep Learning* seperti yang dibahas oleh Cevallos *et al.* (2023) adalah kompleksitas komputasi, sehingga diperlukan optimasi model agar tetap relevan untuk diimplementasikan pada perangkat dengan sumber daya terbatas [14]. TensorFlow Lite hadir sebagai solusi optimasi model *machine learning* untuk perangkat *edge* melalui teknik seperti kuantisasi dan pruning, yang mampu mengurangi ukuran model dan mempercepat inferensi tanpa mengorbankan akurasi secara signifikan [15][16].

Meskipun beberapa penelitian terdahulu telah berhasil mengembangkan *Intrusion Detection System* (IDS) berbasis *Deep Learning* seperti LSTM dengan tingkat akurasi yang tinggi, fokus utama masih bertumpu murni pada aspek deteksi ancaman. Hingga saat ini, masih terdapat *research gap* di mana belum ada penelitian yang mengintegrasikan kemampuan deteksi anomali tersebut dengan algoritma enkripsi standar industri seperti AES-128 dalam satu *pipeline* yang sama, sekaligus mengoptimasinya untuk dapat dieksekusi secara efisien pada perangkat *edge* IoT yang memiliki keterbatasan daya komputasi dan memori. Oleh karena itu, kebaruan (*novelty*) penelitian ini terletak pada integrasi tiga lapis keamanan (enkripsi AES-128 untuk kerahasiaan data + deteksi anomali berbasis LSTM untuk identifikasi serangan + optimasi TensorFlow Lite untuk efisiensi di perangkat *edge*) yang belum ditemukan dalam literatur yang ada, serta implementasi *end-to-end* pada lingkungan simulasi perangkat *edge* dengan mempertimbangkan keterbatasan sumber daya.

Berdasarkan paparan tersebut, penelitian ini mengusulkan integrasi enkripsi AES-128 untuk proteksi *payload* dan deteksi anomali berbasis *Deep Learning* LSTM yang dioptimasi menggunakan TensorFlow Lite. Pendekatan ini bertujuan untuk menutup celah keamanan yang disebutkan dalam studi-studi di atas dengan menciptakan sistem pertahanan yang tidak hanya merahasiakan data, tetapi juga efisien dan cerdas dalam mengenali pola serangan baru pada perangkat yang memiliki sumber daya terbatas.

1.2 Rumusan Masalah

1. Bagaimana mengimplementasikan algoritma enkripsi AES-128 untuk mengamankan transmisi data pada simulasi perangkat IoT?
2. Bagaimana membangun model *Deep Learning* berbasis LSTM yang akurat untuk mendeteksi anomali pada data *traffic* jaringan IoT?
3. Bagaimana akurasi model *Deep Learning* LSTM dalam mendeteksi anomali pada trafik jaringan IoT menggunakan *dataset* CICIoT2023 setelah dilakukan optimasi dengan TensorFlow Lite?
4. Bagaimana dampak implementasi integrasi antara enkripsi data AES-128 dan inferensi deteksi anomali terhadap latensi total sistem pada lingkungan simulasi *edge device* IoT?

1.3 Batasan Masalah

Beberapa batasan masalah yang bertujuan untuk menghindari pembahasan yang lebih luas pada penelitian ini antara lain:

1. Fokus penelitian adalah pada keamanan data (*data security*) yang mencakup aspek kerahasiaan (menggunakan AES) dan deteksi intrusi (menggunakan LSTM).
2. Algoritma enkripsi yang digunakan adalah AES dengan panjang kunci 128-bit, diterapkan pada *payload* data sensor sebelum transmisi. Manajemen kunci (*key management*) diasumsikan sudah aman dan tidak dibahas secara mendalam.
3. Model LSTM digunakan untuk klasifikasi biner (Normal vs Anomali) menggunakan *dataset benchmark* CICIoT2023, tidak mencakup klasifikasi jenis serangan secara spesifik (*multiclass classification*).

4. Pengujian sistem dilakukan menggunakan *dataset benchmark* CICIoT2023 untuk pelatihan model, serta data simulasi (*dummy sensor data*) yang dibangkitkan secara *real-time* pada lingkungan virtual untuk pengujian integrasi.
5. Analisis efisiensi daya dan waktu komputasi perangkat keras dilakukan secara komparatif teoritis berdasarkan hasil eksekusi simulasi, bukan pengukuran fisik menggunakan alat ukur daya.
6. Implementasi sistem dibagi menjadi dua tahap yaitu pelatihan model (*training*) dilakukan di lingkungan Google Colab, sedangkan pengujian integrasi sistem (enkripsi dan deteksi) disimulasikan menggunakan *Virtual Machine* (VM) Raspberry Pi OS sebagai representasi perangkat IoT (*edge device*) dan PC *Host* sebagai server.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Merancang mekanisme simulasi pengiriman data aman pada perangkat IoT menggunakan algoritma enkripsi AES-128.
2. Mengembangkan dan mengoptimasi model *Deep Learning* LSTM menggunakan TensorFlow Lite untuk mendeteksi anomali trafik jaringan IoT dengan target akurasi F1-Score minimal 95% pada kelas Normal menggunakan *dataset benchmark* CICIoT2023.
3. Menganalisis dampak implementasi integrasi antara enkripsi AES-128 dan inferensi model LSTM terhadap latensi total dan efisiensi komputasi sistem pada simulasi perangkat *edge* IoT.

1.5 Manfaat Penelitian

Beberapa manfaat dilaksanakannya penelitian ini antara lain:

1. Mendukung peningkatan keamanan pada lingkungan berbasis IoT dengan solusi yang efisien dan terjangkau
2. Memberikan kontribusi terhadap pengembangan sistem keamanan IoT berbasis *Deep Learning*.
3. Menjadi referensi implementasi sistem keamanan IoT dengan pendekatan gabungan enkripsi dan deteksi anomali yang teroptimasi untuk perangkat *edge*.

1.6 Sistematika Penulisan

Susunan penulisan naskah penelitian ini dilakukan menggunakan sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN, Menguraikan latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan laporan.

BAB II TINJAUAN PUSTAKA, Membahas teori-teori dasar yang mendukung penelitian, meliputi konsep *Internet of Things* (IoT), kriptografi AES, intrusi jaringan, algoritma *Long Short-Term Memory* (LSTM), TensorFlow Lite, serta studi literatur terdahulu yang relevan.

BAB III METODE PENELITIAN, Menjelaskan tahapan penelitian mulai dari pengumpulan *dataset*, *preprocessing* data, perancangan skema enkripsi, arsitektur model LSTM, hingga skenario pengujian dan evaluasi model.

BAB IV HASIL DAN PEMBAHASAN, Menyajikan hasil implementasi sistem, analisis performa model (Akurasi, Presisi, *Recall*, *F1-Score*), hasil enkripsi/dekripsi, serta pembahasan mengenai temuan penelitian.

BAB V PENUTUP, Berisi kesimpulan dari seluruh rangkaian penelitian dan saran-saran konstruktif untuk pengembangan penelitian selanjutnya.