BAB I
PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi *Internet of Things* (IoT) telah membawa transformasi besar pada sistem pencahayaan cerdas (*smart lighting*), yang kini menjadi salah satu segmen dengan pertumbuhan tercepat dalam ekosistem IoT. Pada tahun 2024, nilai pasar global *smart lighting* mencapai USD 22,45 miliar dan diproyeksikan meningkat hingga USD 165,89 miliar pada tahun 2034, dengan tingkat pertumbuhan tahunan rata-rata (*Compound Annual Growth Rate* / CAGR) sebesar 22,14% [1]. Pertumbuhan ini menunjukkan peningkatan kebutuhan akan solusi pencahayaan yang efisien energi sekaligus mendukung otomasi bangunan pintar.

Namun, laju pertumbuhan tersebut tidak diimbangi oleh peningkatan investasi pada aspek keamanan sistemnya. Berdasarkan laporan Dataintelo, pasar keamanan untuk protokol konektivitas kritis seperti ZigBee hanya mencatat CAGR sebesar 13,7% [2]. Perbedaan laju pertumbuhan sebesar 8,44% antara sektor *smart lighting* dan pasar keamanan ZigBee mengindikasikan adanya kesenjangan dalam adopsi teknologi dan penguatan mekanisme perlindungan datanya. Fenomena ini dikenal sebagai *Security Debt Bomb*, yaitu akumulasi risiko keamanan yang timbul akibat meningkatnya jumlah perangkat IoT tanpa disertai mekanisme perlindungan yang memadai. Kondisi ini diperparah oleh laporan yang menyebutkan bahwa serangan *malware* terhadap perangkat IoT meningkat hingga 107% sepanjang tahun 2024 [3].

Laporan *Verizon's Data Breach Investigations Report* juga mencatat bahwa satu dari tiga pelanggaran data kini melibatkan perangkat IoT [4]. Berbagai penelitian memperlihatkan kerentanan nyata dalam sistem *smart lighting*. Ronen et al. menemukan adanya *extended functionality attacks* pada perangkat *smart lighting*, di mana penyerang dapat mengeksploitasi saluran komunikasi ZigBee untuk menyebarkan malware antarperangkat tanpa koneksi internet [5]. Studi lain oleh Husein et al menunjukkan bahwa jaringan ZigBee pada sistem *smart lighting* juga dapat dieksploitasi melalui serangan berbasis MQTT, yang berpotensi mengompromikan sistem kendali pencahayaan secara menyeluruh [6]. Selain itu,

pada tahun 2020, *Check Point Research* mengonfirmasi kerentanan CVE-2020-6007 pada *Philips Hue Bridge* yang memungkinkan eksekusi kode jarak jauh melalui celah *heap-based buffer overflow* [7].

Analisis forensik yang dilakukan oleh Ahmed dan Khan terhadap beberapa lampu pintar komersial menemukan berbagai "*hidden dangers*", termasuk transmisi data tidak terenkripsi serta protokol autentikasi lemah yang berpotensi dimanfaatkan untuk intersepsi data [8]. Temuan-temuan tersebut memperlihatkan bahwa sebagian besar implementasi *smart lighting* saat ini belum memiliki mekanisme pengamanan data yang memadai, terutama dalam proses transmisi log sensor dan komunikasi antarperangkat.

Masalah keamanan pada sistem IoT semakin kompleks karena keterbatasan sumber daya perangkat keras yang digunakan. Algoritma kriptografi konvensional seperti AES dan SHA memang kuat secara teoritis, tetapi memiliki kebutuhan daya, ruang penyimpanan, dan kompleksitas komputasi yang tinggi, sehingga kurang efisien untuk perangkat *embedded* seperti mikrokontroler pada sistem *smart lighting*. Oleh karena itu, dibutuhkan pendekatan *lightweight cryptography*, yaitu algoritma kriptografi yang dirancang untuk perangkat dengan keterbatasan sumber daya namun tetap menjaga keamanan data. Salah satu algoritma yang menonjol adalah PRESENT cipher [9].

Algoritma PRESENT merupakan *block cipher* ringan dengan ukuran blok 64-bit dan Panjang kunci 80-bit atau 128-bit. Berdasarkan penelitian oleh Kumar et al., PRESENT termasuk algoritma yang efisien dalam hal kecepatan eksekusi, konsumsi daya, serta ketahanan terhadap kriptanalisis, menjadikannya kandidat yang sesuai untuk aplikasi IoT. menjadikannya kandidat yang sesuai untuk implementasi pada perangkat *smart lighting* dengan keterbatan memori dan daya komputasi [10]. Penerapan PRESENT pada sistem *smart lighting* diharapkan dapat menjamin keamanan data tanpa mengorbankan performa sistem.

Dalam konteks lokal, PT. Solusindo Bintang Pratama (SBP) sebagai perusahaan penyedia layanan internet (*Internet Service Provider*) dengan merk *Comet Broadband* Wi-Fi, menghadapi tantangan terkait efisiensi energi dan keamanan data pada area gudang penyimpanan. Berdasarkan hasil wawancara dengan pengelola gudang, sistem pecahayaan yang digunakan masih bersifat

konvensional, di mana lampu sering dibiarkan menyala meskipun tidak ada aktivitas. Kondisi ini tidak hanya menyebabkan pemborosan energi listrik, tetapi juga menimbulkan risiko keamanan, mengingat gudang tersebut menyimpan barang-barang inventaris berharga milik perusahaan.

Selain aspek efisiensi, data aktivitas gudang yang dihasilkan oleh sensor pada sistem pencahyaan memiliki nilai sensitif yang seringkali tidak disadari. Fenomena *security debt bomb* berpotensi berdampak pada sistem ini, mengingat sistem pencahayaan yang belum dilengkapi mekanisme pengamanan data dapat menjadi bagian dari akumulasi risiko keamanan IoT. Data dari sensor PIR dapat mengungkap pola aktivitas fisik gudang, seperti jam-jam tinggi aktivitas, periode ketika gudang tidak diawasi, serta kebiasaan penggunaan ruang penyimpanan. Informasi semacam ini dapat dimanfaatkan oleh pihak tidak berwenang untuk merencanakan aktivitas berbahaya, sehingga perlindungan data menjadi sama pentingnya dengan otomatisasi pencahyaan itu sendiri. Hal ini menunjukkan bahwa penerapan *smart lighting* tanpa mekanisme keamanan yang memadai justru dapat menciptakan celah baru di lingkungan industri.

Oleh sebab itu, dibutuhkan sistem *smart lighting* otomatis berbasis IoT yang tidak hanya mampu mengatur pencahayaan secara efisien, tetapi juga memastikan keamanan data yang ditransmisikan. Pada penelitian ini, sistem akan diimplementasikan menggunakan mikrokontroler ESP32 dan sensor PIR dengan penerapan algoritma enkripsi PRESENT-80 secara langsung di sisi perangkat IoT. Artinya, data sensor dienkripsi terlebih dahulu di mikrokontroler sebelum dikirimkan ke server lokal. Enkripsi ini penting untuk melindungi informasi sensitif terkait pola aktivitas gudang dari risiko intersepsi atau manipulasi melalui jaringan Wi-Fi yang rentan, baik pada jam operasional maupun di luar jam kerja. Pendekatan tersebut bertujuan menjaga kerahasiaan dan integritas data, sekaligus mencegah eksploitasi pola data oleh pihak tidak berwenang, seperti yang diidentifikasi dalam kerentanana MQTT pada sistem *smart lighting* [6].

Dengan demikian, sistem yang dikembangkan tidak hanya berkontribusi pada efisiensi energi, tetapi juga memperkuat aspek keamanan informasi di lingkungan industry. Sejalan dengan proyeksi pertumbuhan pasar *smart lighting* kawasan Asia-Pasifik yang mencapai CAGR 19,8% [10], kebutuhan akan sistem

pencahayaan yang aman dan efisien semakin mendesak. Oleh karena itu, penelitian ini dilakukan untuk merancang, mengimplementasikan, dan menganalisis sistem *smart lighting* berbasis IoT dengan algoritma PRESENT guna memastikan keamanan data dan integritas informasi pada gudang PT. Solusindo Bintang Pratama.

B. Perumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana merancang sistem *smart lighting* berbasis IoT yang mampu mendeteksi aktivitas di gudang PT. SBP secara *real-time*?
2. Bagaimana implementasi algoritma PRESENT-80 pada sisi perangkat IoT untuk menjamin kerahasiaan dan integritas data sensor yang merepresentasikan pola aktivitas gudang?
3. Bagaimana efektivitas algoritma PRESENT dalam mengamankan transmisi data dari serangan *Man-in-the-Middle* (MitM) dan *Eavesdropping*?

C. Batasan Penelitian

Untuk menjaga penelitian tetap terarah dan terukur, maka ditetapkan beberapa batasan masalah sebagai berikut:

1. Penelitian difokuskan pada implementasi keamanan transmisi data sensor PIR pada sistem *smart lighting* di gudang PT. Solusindo Bintang Pratama.
2. Sistem menggunakan mikrokontroler ESP32 dengan protokol komunikasi Wi-Fi untuk pengiriman data ke server lokal.
3. Lingkungan pengujian menggunakan koneksi Wi-Fi yang dikondisikan stabil untuk menjaga eksperimen tetap terkontrol. Aspek seperti mekanisme *retry*, *packet loss*, atau operasi *offline* tidak menjadi fokus penelitian karena berada diluar ruang lingkup pengujian algoritma PRESENT.
4. Pengujian dilakukan hanya pada kondisi sistem dialiri listrik PLN. Aspek ketahanan sistem saat pemadaman listrik atau penggunaan

baterai cadangan tidak menjadi bahan evaluasi penelitian ini.

5. Analisis difokuskan pada performa enkripsi (waktu eksekusi dan *throughput*) serta efektivitas keamanan data, sedangkan pengujian fungsi dasar (deteksi gerakan dan kontrol lampu) hanya dilakukan sebagai validasi sistem.
6. Sensor PIR digunakan sebagai penghasil data aktivitas, sementara karakteristik teknis sensor tidak dianalisis karena penelitian difokuskan pada aspek keamanan data pada ESP32 menggunakan algoritma PRESENT-80.
7. Algoritma kriptografi yang digunakan adalah PRESENT-80 tanpa perbandingan dengan algoritma lain.
8. Evaluasi efektivitas algoritma PRESENT dilakukan melalui simulasi dua jenis serangan umum pada jaringan IoT, yaitu *Eavesdropping* dan *Man-in-the-Middle* (MitM).

D. Tujuan Penelitian

Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem *smart lighting* berbasis *Internet of Things* (IoT) pada gudang PT. Solusindo Bintang Pratama dengan memanfaatkan sensor PIR dan mikrokontroler ESP32 untuk mendeteksi aktivitas secara *real-time* dan mengendalikan nyala lampu secara otomatis. Selain itu, penelitian ini bertujuan untuk menerapkan algoritma kriptografi ringan PRESENT-80 dengan mode *Counter* (CTR) pada sisi perangkat IoT guna menjamin kerahasiaan dan integritas data sensor sebelum dikirimkan melalui jaringan Wi-Fi. Penelitian ini juga bertujuan untuk menganalisis performa enkripsi serta mengevaluasi efektivitas algoritma PRESENT-80 dalam menghadapi serangan *Eavesdropping* dan *Man-in-the-Middle*, sekaligus memvalidasi fungsionalitas sistem secara keseluruhan.

E. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Bagi penulis, memberikan pengalaman praktis dalam merancang dan mengimplementasikan sistem IoT dengan penerapan *lightweight cryptography*, khususnya algoritma PRESENT, serta memperdalam

pemahaman mengenai analisis keamanan data pada perangkat IoT dengan keterbatasan sumber daya.

2. Bagi pembaca, menjadi referensi ilmiah dalam pengembangan sistem otomasi berbasis IoT yang mengintegrasikan keamanan data melalui algoritma kriptografi ringan, serta dapat digunakan sebagai dasar untuk penelitian lanjutan terkait efisiensi dan perlindungan data pada perangkat IoT.
3. Bagi industri (PT. Solusindo Bintang Pratama), hasil penelitian ini diharapkan memberikan solusi praktis berupa sistem *smart lighting* otomatis dengan enkripsi PRESENT-80 yang mampu melindungi informasi sensitif terkait pola aktivitas dan monitoring fasilitas dari potensi ancaman siber.

F. Keaslian Penelitian

Tabel 1. Perbandingan keaslian penelitian

	Firdaus dkk., 2021 [11].	Tran Anh Khoa dkk., 2020 [12].	Penelitian Ini
Judul	Implementasi Algoritma PRESENT untuk Proses Enkripsi pada Modul Komunikasi LoRa	*Designing Efficient Smart Home Management with IoT Smart Lighting: A Case Study*	Implementasi dan Analisis Keamanan Data Sistem *Smart Lighting* Menggunakan Algoritma PRESENT: Studi Kasus Gudang PT. Solusindo Bintang Pratama
Metode	Eksperimen / Implementasi Sistem	Rancang Bangun Sistem IoT	Eksperimen Rekayasa / *Design Science Research*
Platform / Teknologi	Mikrokontroler LoRa, Algoritma PRESENT	ESP8266, Raspberry Pi, SHA-256	ESP32, Sensor PIR, Wi-Fi, Algoritma PRESENT-80
Persamaan	Sama-sama menggunakan algoritma PRESENT sebagai mekanisme enkripsi data IoT untuk menjaga	Sama-sama mengembangkan sistem *smart lighting* berbasis IoT dengan perhatian pada	-

	keamanan komunikasi	keamanan komunikasi data	
Perbedaan	Menggunakan jaringan LoRa, bukan Wi-Fi; tidak menerapkan sistem *smart lighting*; tidak ada analisis terhadap serangan keamanan	Menggunakan algoritma SHA-256 (kriptografi berat) untuk autentikasi, bukan PRESENT; tidak mengenkripsi data sensor	Sedangkan penelitian ini menggunakan algoritma PRESENT-80 sebagai enkripsi data sensor pada sistem *smart lighting* industri (gudang) dan menguji keamanan terhadap serangan MitM & *Eavesdropping*
Keterangan	Fokus pada efisiensi enkripsi di jaringan LoRa, menjadi dasar bahwa PRESENT cocok untuk IoT	Fokus pada autentikasi perangkat dan pengguna, belum membahas enkripsi data sensor secara menyeluruh	Penelitian ini memiliki keaslian pada penerapan nyata, analisis keamanan data, dan penggunaan LWC yang efisien untuk perangkat IoT