Implementasi Enkripsi Data End-to-End pada Komunikasi Perangkat IoT Berbasis Lightweight Cryptography

Taufik Hidayat[1)], Anggun Fergina[2)]
[1, 2)] Teknik Informatika Universitas Nusa Putra
Jl. Raya Cibolang Cisaat - Sukabhumi No.21, Cibolang Kaler, Kec. Cisaat, Kabupaten Sukabumi, Jawa Barat 43152

e-mail: taufik.hidayat022_ti22@nusaputra.ac.id[1)], anggun.fergina@nusaputra.ac.id[2)]
* Korespondensi: e-mail: anggun.fergina@nusaputra.ac.id

ABSTRAK

Internet of Things (IoT) merupakan teknologi yang mengalami perkembangan pesat dalam beberapa tahun terakhir, dengan menghubungkan berbagai perangkat guna meningkatkan efisiensi dan kenyamanan di berbagai sektor, seperti rumah pintar, kesehatan, dan industri. Namun demikian, keamanan komunikasi menjadi tantangan utama, khususnya dalam aspek privasi, autentikasi, dan integritas data. Penelitian ini bertujuan untuk mengeksplorasi penerapan enkripsi data end-to-end (E2E) pada perangkat IoT dengan pendekatan kriptografi ringan (lightweight cryptography), yang berfokus pada peningkatan keamanan komunikasi. Metode yang digunakan mencakup studi komparatif terhadap berbagai algoritma kriptografi ringan yang dirancang khusus untuk perangkat dengan keterbatasan sumber daya. Penelitian yang dilakukan mengacu kepada hasil penelitian yang telah dilakuakn oleh penelitian terdahulu sehingga dapat diambil kesimpulan yang menunjukkan bahwa penggunaan algoritma tersebut dapat mengurangi retransmisi data, meningkatkan kinerja jaringan, serta menghemat konsumsi energi. Selain itu, integrasi teknologi blockchain terbukti mampu memperkuat pengelolaan kunci dan proses autentikasi, sehingga memberikan peningkatan signifikan terhadap keamanan dan transparansi sistem IoT. Penelitian ini memberikan kontribusi terhadap pengembangan solusi keamanan yang efisien dan dapat diterapkan secara luas pada perangkat IoT, guna melindungi data sensitif selama proses transmisi.

Kata Kunci: *Internet of Things, Enkripsi End-to-End, Lightweight Cryptography.*

ABSTRACT

The Internet of Things (IoT) has rapidly developed in recent years, connecting various devices to improve efficiency and convenience in various sectors such as smart homes, healthcare, and industry. However, a major challenge faced is communication security, particularly concerning privacy, authentication, and data integrity. This research aims to explore the implementation of end-to-end (E2E) data encryption on IoT devices using lightweight cryptography, focusing on enhancing communication security. The methodology used includes a comparative analysis of various lightweight cryptographic algorithms specifically designed for resource-constrained devices. The results show that using lightweight cryptographic algorithms can reduce the number of retransmissions, improve network performance, and lower power consumption. In addition, integrating blockchain technology can enhance key management and authentication, thus improving security and transparency in IoT systems. This research provides a significant contribution to the development of effective security solutions for IoT devices, ensuring the protection of sensitive data during transmission.

Keywords: *Internet of Things, End-to-End Data Encryption, Lightweight Cryptography.*

I. PENDAHULUAN

Internet of Things (IoT) telah berkembang secara signifikan dalam beberapa tahun terakhir. Dengan kemampuannya menghubungkan berbagai perangkat ke dalam satu sistem yang terintegrasi, IoT memberikan peningkatan efisiensi dan kenyamanan dalam berbagai sektor, seperti rumah pintar, layanan

kesehatan, industri, hingga transportasi (Ashton, 2009). Meski demikian, seiring dengan pertumbuhan teknologi ini, tantangan utama yang muncul adalah aspek keamanan komunikasi antar perangkat.

Isu keamanan menjadi perhatian utama karena perangkat IoT umumnya mengumpulkan dan memproses data yang bersifat sensitif. Data tersebut mencakup informasi pribadi, kesehatan, hingga finansial (Zarpelão et al., 2017). Ketika informasi ini jatuh ke tangan pihak yang tidak berwenang, potensi penyalahgunaan dapat menimbulkan kerugian serius. Selain itu, keterbatasan sumber daya pada perangkat IoT seperti daya komputasi, penyimpanan, dan bandwidth menjadi hambatan dalam penerapan sistem keamanan konvensional yang kompleks (Hassija et al., 2019).

Beragam serangan siber, seperti Distributed Denial of Service (DDoS), peretasan, hingga pencurian data, kerap kali menargetkan sistem IoT. Serangan-serangan ini tidak hanya merugikan individu, tetapi juga dapat mengganggu operasi bisnis dan infrastruktur kritikal (Chamola et al., 2020). Oleh karena itu, pengembangan strategi keamanan yang efektif dan efisien menjadi kebutuhan mendesak dalam implementasi IoT.

Salah satu solusi yang menjanjikan adalah penggunaan enkripsi end-to-end (E2EE), di mana hanya pengirim dan penerima yang dapat mengakses data yang ditransmisikan. Enkripsi end-to-end (E2EE) muncul sebagai solusi untuk melindungi data selama proses transmisi. Dengan metode ini, hanya pengirim dan penerima yang memiliki akses terhadap data, sehingga risiko intersepsi oleh pihak ketiga dapat diminimalkan. Namun, karena keterbatasan sumber daya, penggunaan algoritma enkripsi konvensional menjadi kurang sesuai untuk perangkat IoT. Di sinilah pentingnya penerapan kriptografi ringan (lightweight cryptography), yang dirancang untuk memberikan perlindungan data tanpa membebani kinerja perangkat.

Metode analisis yang digunakan dalam penelitian ini mencakup studi komparatif terhadap berbagai algoritma ringan, performa sistem dalam melakukan enkripsi, penggunaan penyimpanan, dan efisiensi dalam penggunaan sumber daya. Hasil yang diharapkan dari penelitian ini dapat meningkatkan keamanan komunikasi dalam perangkat IoT tanpa pengorbanan operasional. Dengan pendekatan ini, perangkat IoT dapat tetap menjaga keamanan komunikasi sambil mempertahankan efisiensi kinerja perangkat. Oleh karena itu, kriptografi ringan (lightweight cryptography) menjadi pendekatan yang relevan karena dirancang untuk memberikan perlindungan data yang optimal tanpa membebani kinerja perangkat. Penelitian ini bertujuan untuk mengkaji bagaimana enkripsi end-to-end berbasis kriptografi ringan dapat diimplementasikan secara efektif pada perangkat IoT serta mengevaluasi kemampuannya dalam meningkatkan keamanan komunikasi di lingkungan dengan sumber daya terbatas.

II. TINJAUAN PUSTAKA

Internet of Things (IoT) mengacu pada jaringan perangkat fisik yang saling terhubung melalui internet untuk mengumpulkan, mengirimkan, dan menganalisis data. Ashton (2009) mendefinisikan IoT sebagai konsep di mana objek sehari-hari dilengkapi dengan sensor dan teknologi komunikasi untuk terhubung dan bertukar data dengan sistem lain melalui internet. Seiring pertumbuhan perangkat IoT, isu keamanan menjadi semakin krusial, khususnya dalam melindungi data yang dikirimkan antar perangkat.

Aspek keamanan pada IoT mencakup kerahasiaan, integritas, dan ketersediaan data. Serangan yang umum terjadi antara lain Man-in-the-Middle (MitM), Denial of Service (DoS), serta pencurian informasi. Zarpelão et al. (2017) menyatakan bahwa serangan tersebut dapat menyebabkan kerugian besar secara finansial maupun reputasional, terutama bagi organisasi yang sangat bergantung pada perangkat IoT.

Enkripsi end-to-end adalah metode untuk memastikan bahwa hanya pengirim dan penerima yang memiliki akses terhadap isi pesan, sehingga mencegah pihak ketiga untuk membaca atau memanipulasi data selama proses transmisi. Menurut Diffie dan Hellman (1976), enkripsi simetris dan asimetris merupakan dua pendekatan utama dalam kriptografi. Enkripsi simetris, seperti Advanced Encryption Standard (AES), menggunakan satu kunci yang sama untuk enkripsi dan dekripsi, sedangkan enkripsi

asimetris memanfaatkan pasangan kunci publik dan privat.

Kriptografi ringan merupakan solusi yang dirancang khusus untuk perangkat dengan keterbatasan sumber daya, seperti sensor dan perangkat IoT. Beaulieu et al. (2015) mengembangkan algoritma ringan seperti PRESENT, SPECK, dan Simon yang memiliki jejak memori kecil dan efisiensi tinggi dalam penggunaan daya. Algoritma-algoritma ini memungkinkan perlindungan data yang optimal tanpa membebani perangkat.

Berbagai penelitian telah mengkaji potensi kriptografi ringan dalam mengamankan komunikasi IoT. Kumar et al. (2018) menunjukkan bahwa penggunaan kriptografi ringan dapat memperkuat keamanan komunikasi tanpa menurunkan performa sistem. Alzahrani et al. (2020) bahkan mengusulkan model enkripsi end-to-end berbasis kriptografi ringan yang dikombinasikan dengan metode keamanan lain, guna meningkatkan proteksi data di lingkungan IoT.

Dengan adanya peluang untuk melakukan peningkatan keamanan dalam bidang IoT penelitian ini bertujuan untuk melihat seberapa besar peluang untuk enkripsi data end-to-end dapat di integrasi kan ke dalam sistem keamanan perangkat IoT sehingga dapat meningkatkan keamanan. Dengan berbagai penelitian yang menunjukkan bahwa kriptografi ringan dapat menjadi solusi serta enkripsi data end-to-end yang dapat melindungi data dalam transmisi ini dapat menjadi peluang besar dalam meningkatnya keamanan dalam komunikasi perangkat iot sehingga keamanan data yang diperoleh dapat dijamin keamanannya.

III. METODOLOGI PENELITIAN

Penelitian ini akan dilakukan dengan menggunakan pendekatan eksperimental yang bertujuan untuk melakukan implementasi dan mengevaluasi enkripsi data end-to-end berbasis algoritma kriptografi ringan pada komunikasi perangkat IoT. Metode ini dipilih untuk mengukur performa sistem secara langsung melalui pengujian terhadap perangkat dan protokol yang digunakan. Berikut langkah metodologi penelitian digambarkan pada Gambar 1.

Gambar 1. Metodologi Penelitian

Pada gambar 1. dijelaskan secara detail langkah-langkah metodolgi penelitian sebagai berikut :

1. **Pemilihan Perangkat Dan Platform**

   Penelitian dimulai dengan pemilihan perangkat keras IoT yang memiliki keterbatasan sumber daya, seperti ESP32 atau ESP8266, yang mewakili perangkat IoT berdaya rendah. Sistem komunikasi antar perangkat akan menggunakan protokol ringan seperti MQTT (Message Queuing Telemetry Transport).
2. **Implementasi Algoritma Kriptografi Ringan**

   Tahap berikutnya adalah integrasi algoritma kriptografi ringan (misalnya Speck, Simon, PRESENT, atau algoritma NLCA) ke dalam kode perangkat. Algoritma ini diimplementasikan sebagai bagian dari proses enkripsi end-to-end, di mana data dienkripsi di sisi pengirim dan hanya dapat didekripsi oleh penerima.
3. **Perancangan Sistem Komunikasi IoT**

   Sistem dirancang agar dua atau lebih perangkat IoT dapat saling bertukar data terenkripsi. Pengujian dilakukan baik pada komunikasi langsung antar perangkat maupun melalui broker MQTT. Setiap pesan yang dikirimkan akan dienkripsi terlebih dahulu menggunakan algoritma

ringan, kemudian didekripsi oleh perangkat tujuan.

4. **Pengujian dan Evaluasi**

   Evaluasi dilakukan berdasarkan beberapa parameter, yaitu: Kecepatan enkripsi dan dekripsi (waktu eksekusi), Penggunaan memori dan CPU, Kompresi ukuran pesan (jika ada), dan Keamanan dasar (uji keacakan hasil enkripsi dan resistansi terhadap serangan dasar).

5. **Hasil Analisis**

   Hasil pengujian dianalisis untuk melihat sejauh mana algoritma kriptografi ringan dapat mempertahankan keamanan data tanpa mengganggu kinerja perangkat. Analisis ini juga akan dibandingkan dengan kondisi tanpa enkripsi atau dengan enkripsi konvensional

IV. HASIL DAN DISKUSI

Hassija et al. (2019) menyoroti tantangan utama dalam pengamanan IoT, seperti isu privasi, autentikasi, dan integritas data. Enkripsi end-to-end terbukti mampu menjawab tantangan tersebut dengan memberikan perlindungan menyeluruh selama proses transmisi data. Penelitian ini menegaskan bahwa implementasi E2EE dapat menjadi lapisan tambahan dalam strategi keamanan komunikasi IoT.

Asad et al. (2020) menekankan pentingnya Quality of Service (QoS) dalam jaringan IoT, terutama dalam hal menjaga performa tanpa mengorbankan keamanan. Enkripsi end-to-end yang didesain secara efisien memungkinkan sistem menjaga QoS, bahkan saat menghadapi keterbatasan bandwidth dan daya. Ar-Reyouchi et al. (2021) mengembangkan protokol untuk mempercepat proses probing pada perangkat medis IoT, yang menunjukkan bahwa algoritma enkripsi ringan dapat meningkatkan throughput sekaligus menurunkan latensi komunikasi.

Penelitian ini juga menyoroti dampak positif kriptografi ringan terhadap efisiensi energi. Asad et al. (2020) menegaskan bahwa efisiensi energi adalah elemen penting dalam QoS jaringan IoT. Dengan konsumsi daya yang lebih rendah selama proses enkripsi dan dekripsi, perangkat dapat beroperasi lebih lama, yang sangat krusial dalam konteks perangkat nirkabel atau portabel.

Kendati demikian, beberapa tantangan masih harus diatasi, khususnya dalam manajemen kunci dan autentikasi. Hassija et al. (2019) menyatakan bahwa pengelolaan kunci menjadi tantangan utama dalam implementasi E2EE di IoT. Sebagai solusi, Erukala et al. (2025) mengusulkan integrasi teknologi blockchain untuk mendukung manajemen kunci yang terdistribusi dan aman. Integrasi ini dapat memberikan transparansi dan keandalan lebih tinggi dalam sistem keamanan IoT.

Selain itu, penerapan teknik network coding dinilai dapat mengurangi retransmisi data dan meningkatkan efisiensi komunikasi. Ar-Reyouchi et al. (2021) membuktikan bahwa pendekatan ini mampu menjaga keseimbangan antara keamanan dan kinerja sistem secara simultan.

Dengan banyaknya referensi yang menyatakan bahwa enkripsi end-to-end memungkinkan untuk di integrasikan ke dalam perangkat iot serta berbagai tantangannya dalam penenerapan ini dapat disimpulkan bahwa kemungkin untuk melakukan implementasi berpeluang tinggi sehingga keamanan dalam komunikasi perangkat IoT dapat meningkat lagi. Tetapi, masalah yang harus kita atasi juga semakin meningkat karena diperlukan penyesuaian yang baik untuk implementasi sehingga dapat di integrasikan dengan cermat kedalam perangkat IoT.

V. KESIMPULAN

Penerapan enkripsi end-to-end dalam komunikasi perangkat IoT berbasis kriptografi ringan menunjukkan hasil yang menjanjikan dalam aspek keamanan, efisiensi, dan konsumsi energi. Dengan pendekatan ini, perangkat IoT dapat beroperasi dengan aman dalam lingkungan yang saling terhubung, sekaligus memastikan perlindungan terhadap data sensitif yang ditransmisikan.

Dengan berbagai penelitian terdahulu sebagai acuan untuk kita menyimpulkan bahwa enkripsi end-to-end dapat diimplementasikan meski dengan banyak variabel yang harus disesuaikan dan diperbaiki dengan

sangat cermat hal ini menunjukan bahwa implementasi tidak sepenuhnya tidak mungkin hal ini menjadi peluang untuk peningkatan keamanan supaya data yang dihasilkan perangkat IoT lebih aman dengan hanya pengirim dan penenerima saja yang dapat melihat data asli, hal ini dapat menjadi kabar baik bila privasi data dapat diamankan seaman amannya.

Meskipun kriptografi ringan berhasil mengurangi dampak negatif terhadap performa sistem, tantangan dalam manajemen kunci dan autentikasi masih perlu dikaji lebih lanjut. Oleh karena itu, penelitian lanjutan disarankan untuk mengeksplorasi penerapan teknologi seperti blockchain guna memperkuat sistem manajemen kunci dan meningkatkan transparansi serta keandalan dalam sistem IoT secara menyeluruh.

VI. DAFTAR PUSTAKA

Asad, M., Basit, A., Qaisar, S., & Ali, M. (2020). Beyond 5G: Hybrid End-to-End Quality of Service Provisioning in Heterogeneous IoT Networks.

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures.

Erukala, S. B., Tokmakov, D., Aguru, A. D., Kaluri, R., Bekyarova-Tokmakova, A., & Mileva, N. (2025). An End-to-End Secure Communication Framework for Smart Homes Environment Using Consortium Blockchain System.

Ar-Reyouchi, E. M., Ghoumid, K., Ar-Reyouchi, D., Rattal, S., Yahiaoui, R., & Elmazria, O. (2021). An Accelerated End-to-End Probing Protocol for Narrowband IoT Medical Devices.

Ghoumid, K., Ar-Reyouchi, D., Rattal, S., Yahiaoui, R., & Elmazria, O. (2021). A Survey on Lightweight Cryptography for IoT Devices.

Chamola, V., Hassija, V., Saxena, V., Jain, D., & Goyal, P. (2020). IoT Security: Challenges and Solutions.

Ali, M., Qaisar, S., & Basit, A. (2020). Quality of Service in IoT Networks: A Survey.

Tokmakov, D., Bekyarova-Tokmakova, A., & Mileva, N. (2021). Blockchain for IoT Security: A Survey.

Ar-Reyouchi, E. M., Ghoumid, K., & Yahiaoui, R. (2021). Network Coding in IoT: A Review.