BAB 1
USULAN GAGASAN

1.1 Deskripsi Umum Masalah

Perkembangan pesat teknologi *Internet of Things* (IoT) dalam beberapa tahun terakhir telah menciptakan paradigma baru dalam konektivitas perangkat elektronik. Namun, ekspansi masif ini dibarengi dengan munculnya berbagai tantangan keamanan siber yang signifikan. Karakteristik perangkat IoT yang umumnya memiliki konfigurasi keamanan default yang minimal, ditambah dengan implementasi mekanisme pembaruan keamanan yang tidak konsisten, menjadikan perangkat-perangkat tersebut rentan terhadap eksploitasi oleh pelaku kejahatan siber.

Salah satu bentuk nyata dari kerentanan ini terlihat pada kasus serangan malware Mirai yang terjadi pada tahun 2016. Serangan ini berhasil mengkompromikan jutaan perangkat IoT dan menggunakannya untuk melakukan serangan *Distributed Denial of Service* (DDoS) terhadap penyedia layanan DNS Dyn, yang mengakibatkan gangguan layanan internet skala besar. Kasus ini menunjukkan bagaimana kelemahan keamanan pada perangkat IoT dapat berdampak sistemik terhadap infrastruktur internet global.

Dalam konteks komunikasi *Machine-to-Machine* (M2M), aspek keamanan data menjadi tantangan fundamental yang memerlukan perhatian khusus. Setiap transaksi komunikasi antar perangkat IoT harus dilindungi melalui implementasi protokol enkripsi dan dekripsi yang robust untuk mitigasi risiko intersepsi data, manipulasi informasi, dan berbagai bentuk serangan siber lainnya.

Saat ini, kehidupan manusia sangat bergantung pada teknologi, terutama dengan perkembangan IoT yang memungkinkan interaksi dan komunikasi antar perangkat. Namun, IoT memiliki kelemahan karena terbukti rentan terhadap pelanggaran, sehingga diperlukan analisis dan perbandingan teknologi yang sudah ada untuk mengatasi isu keamanan ini [1]. Ancaman terhadap privasi dalam lingkungan IoT menjadi isu penting yang harus diperhatikan dan dilindungi, mengingat data atau informasi dapat disalahgunakan untuk tujuan yang tidak bertanggung jawab.

Tulisan ini secara sistematis mengulas literatur tentang teknologi dan metode yang digunakan untuk melindungi privasi, serta menganalisis solusi yang telah diterapkan. Kami

menemukan bahwa hanya sedikit solusi yang benar-benar efektif dalam melindungi privasi, dan sebagian besar solusi tersebut bergantung pada asumsi bahwa pengguna memiliki kesadaran tinggi terhadap privasi mereka. Oleh karena itu, penelitian lebih lanjut diperlukan untuk mengeksplorasi hubungan antara metode perlindungan privasi dan tingkat kesadaran pengguna [2].

Dengan mempertimbangkan keterbatasan sumber daya pada perangkat IoT penelitian ini difokuskan pada analisis dan perbandingan berbagai sistem enkripsi ringan yang telah dikembangkan. Sistem ini menggunakan pendekatan substitusi dan transposisi yang kuat, serta menerapkan ukuran blok variabel untuk meningkatkan fleksibilitas. Dari hasil evaluasi, sistem yang dianalisis dan dibandingkan menunjukkan kinerja yang sangat bervariasi, baik dari segi kecepatan maupun efisiensi penggunaan memori, sehingga penting untuk menentukan algoritma yang paling sesuai untuk mengamankan data solusi yang potensial untuk mengamankan data di perangkat IoT [3]. Dengan banyaknya perangkat yang terhubung di IoT dan jumlah data yang sangat besar yang tersebar di udara, berbagai jenis serangan telah menjadikan data sangat rentan. Algoritma kriptografi digunakan untuk menjaga kerahasiaan dan integritas data

Namun, ukuran perangkat, kemampuan komputasi, memori, dan sumber daya yang terbatas membuat sulit untuk menggunakan algoritma kriptografi konvensional yang intensif sumber daya untuk menjaga keamanan data. Analisis dan perbandingan berbagai skenario kriptografi ringan ini menjadi langkah penting untuk menemukan pendekatan yang paling tepat bagi perangkat IoT. Melalui pemanfaatan teknologi *blockchain* untuk meningkatkan transparansi dan otentikasi data dapat menjadi pendekatan yang efektif. Dalam kombinasi kriptografi ringan dan teknologi canggih ini, perlindungan yang lebih kuat dan efisien bagi perangkat IoT dapat tercapai, tanpa mengorbankan kinerja atau sumber daya [4].

1.2 Analisis Masalah

1.2.1 Aspek Ekonomi

Dalam pengembangan perangkat IoT, aspek ekonomi menjadi pertimbangan utama yang mempengaruhi kelayakan implementasi teknologi dalam produksi massal. Penggunaan algoritma kriptografi ringan memberikan keuntungan dalam hal efisiensi daya dan memori, sehingga memungkinkan penggunaan mikrokontroler dengan biaya lebih rendah. Hal ini

berdampak pada pengurangan biaya produksi dan operasional, terutama untuk perangkat IoT berskala besar [5].

1.2.2 Aspek Manufakturabilitas

Aspek manufakturabilitas menjadi salah satu pertimbangan penting dalam pengembangan perangkat IoT yang akan diproduksi secara massal. Manufakturabilitas mengacu pada tingkat kemudahan suatu produk atau teknologi dapat diimplementasikan dalam proses produksi, baik dari sisi desain perangkat keras (hardware), perangkat lunak (software), maupun biaya produksi secara keseluruhan [6]

1.2.3 Aspek Teknis

Aspek teknis berkaitan erat dengan kemampuan perangkat IoT dalam menjalankan algoritma kriptografi sesuai keterbatasan sumber dayanya. Perangkat IoT umumnya memiliki daya baterai yang terbatas, kapasitas pemrosesan yang rendah, dan memori yang kecil, sehingga implementasi algoritma kriptografi yang kompleks berpotensi menurunkan performa perangkat secara signifikan [7]

1.2.4 Aspek Keamanan

Aspek keamanan merupakan inti dari implementasi kriptografi pada IoT, mengingat tingginya ancaman siber terhadap perangkat dengan konektivitas terbuka. Perangkat IoT sering kali memiliki celah keamanan seperti pengaturan default yang lemah, jarangnya pembaruan firmware, serta lemahnya mekanisme manajemen kunci [8]. Salah satu masalah penting adalah pengelolaan kunci enkripsi, yang mencakup pembuatan, distribusi dan penyimpanan kunci. Sistem yang tidak mampu menangani algoritma enkripsi yang kompleks akan mengalami penurunan performa.

1.2.5 Aspek Lingkungan

Aspek lingkungan menjadi pertimbangan penting dalam pengembangan perangkat elektronik modern. Perangkat IoT yang hemat energi tidak hanya memperpanjang masa pakai baterai, tetapi juga berkontribusi dalam mengurangi limbah elektronik akibat seringnya pergantian perangkat yang rusak karena konsumsi daya yang berlebihan [9]. Penggunaan algoritma kriptografi ringan yang hemat energi secara tidak langsung berkontribusi pada efisiensi ekosistem perangkat IoT, dengan menekan kebutuhan energi listrik baik pada sisi perangkat maupun infrastruktur jaringan pendukung. Hal ini sejalan denganprinsip pengembangan teknologi ramah lingkungan yang berkelanjutan.

1.3 Analisis Solusi yang Ada

Penguatan sistem keamanan dalam komunikasi Machine-to-Machine (M2M) pada ekosistem Internet of Things (IoT) saat ini banyak diarahkan pada pemanfaatan algoritma kriptografi ringan. Pendekatan-pendekatan tersebut dapat dianalisis menggunakan tiga dimensi utama dalam karakteristik sistem kriptografi, yakni berdasarkan jenis operasi, jumlah kunci yang digunakan, dan cara pemrosesan data. Ketiga aspek ini menjadi landasan dalam menilai kesesuaian suatu metode kriptografi terhadap kebutuhan perangkat yang memiliki keterbatasan daya dan sumber daya komputasi.

1.3.1 Jenis Operasi yang Diterapkan

Mayoritas teknik kriptografi ringan dirancang dengan mengombinasikan dua operasi dasar, yaitu *substitution* (pergantian) dan *transposition* (perpindahan). Operasi pergantian dilakukan dengan mengganti elemen-elemen dari plaintext menjadi bentuk lain untuk menyamarkan informasi, sementara operasi perpindahan bertujuan mengubah susunan elemen agar tidak tampak dalam pola aslinya. Kedua operasi ini harus dapat dibalik agar informasi dapat dikembalikan melalui proses dekripsi. Pendekatan gabungan ini sering disebut sebagai product cipher, dan umum diterapkan dalam algoritma ringan karena mampu memberikan perlindungan yang memadai dengan beban komputasi yang rendah.

1.3.2 Jumlah Kunci yang Digunakan

Sebagian besar solusi keamanan pada perangkat IoT mengadopsi sistem *symmetric-key encryption*, yaitu metode di mana proses enkripsi dan dekripsi dilakukan dengan menggunakan satu kunci rahasia yang sama. Metode ini lebih hemat sumber daya dan lebih sederhana dibandingkan *asymmetric-key encryption* yang membutuhkan pasangan kunci publik dan privat. Penggunaan satu kunci dianggap lebih praktis dalam sistem IoT karena mempercepat proses komunikasi dan mengurangi kebutuhan pertukaran kunci yang kompleks, khususnya pada jaringan dengan keterbatasan *bandwidth* dan daya.

1.3.3 Metode Dalam Pemrosesan Data

Dalam hal pemrosesan plaintext, terdapat dua pendekatan utama, yaitu block cipher dan stream cipher. Block cipher bekerja dengan membagi data ke dalam blok berukuran tetap dan mengenkripsinya secara menyeluruh per blok, yang membuatnya ideal untuk implementasi pada sistem tertanam karena struktur dan keamanannya yang terbukti andal. Sementara itu, stream cipher mengenkripsi data secara berurutan dalam unit kecil dan menghasilkan output secara langsung seiring dengan input yang diterima, sehingga lebih cocok untuk aplikasi yang memerlukan pemrosesan cepat dan latensi rendah. Di samping itu, beberapa pendekatan

modern mengintegrasikan fungsi autentikasi ke dalam skema enkripsi berbasis blok, sehingga mampu menjamin baik kerahasiaan maupun integritas data secara simultan dalam satu proses enkripsi [10]

1.4 Tujuan Tugas Akhir

1.4.1 Tujuan umum

Menghasilkan solusi keamanan data yang efektif dan efisien untuk komunikasi *Machine-to-Machine* (M2M) pada perangkat IoT dengan keterbatasan sumber daya, melalui implementasi dan evaluasi algoritma kriptografi ringan

1.4.2 Tujuan Khusus

1. Aspek Ekonomi

   Menyediakan pilihan algoritma enkripsi yang hemat daya dan memori sehingga mengurangi biaya operasional jangka panjang, walaupun investasi awal penelitian dan pengembangan diperlukan
2. Aspek Manufakturabilitas

   Menghasilkan solusi keamanan yang mudah diintegrasikan ke perangkat IoT dalam skala manufaktur, tanpa memerlukan spesifikasi hardware yang mahal atau rumit.
3. Aspek Teknis

   Mengimplementasikan algoritma kriptografi yang ringan dan sesuai dengan keterbatasan teknis perangkat IoT, sehingga tetap mempertahankan performa optimal dan efisiensi daya.
4. Aspek Keamanan

   Meningkatkan keamanan komunikasi data antar perangkat IoT agar lebih tahan terhadap serangan siber, sekaligus tetap mempertahankan performa yang stabil.
5. Aspek Lingkungan

   Mendukung efisiensi energi pada perangkat IoT sehingga berdampak pada pengurangan limbah elektronik dan konsumsi energi secara keseluruhan, sejalan dengan upaya pelestarian lingkungan

1.5 Batasan Tugas Akhir

Tugas akhir ini memiliki batasan pada ruang lingkup pengujian dan analisis algoritma kriptografi ringan yang diterapkan untuk mendukung keamanan komunikasi *Machine-to-Machine* (M2M) pada perangkat IoT dengan keterbatasan sumber daya. Penelitian ini difokuskan pada implementasi algoritma kriptografi simetris, yaitu PRESENT, LED, ASCON, dan TWINE, tanpa membahas algoritma kriptografi asimetris maupun metode manajemen kunci tingkat lanjut.

Implementasi dilakukan dalam skala kecil menggunakan simulasi dua perangkat mikrokontroler yang berkomunikasi secara langsung, sehingga tidak mencakup penerapan pada jaringan IoT berskala besar maupun topologi multi-node yang kompleks. Evaluasi yang dilakukan terbatas pada parameter efisiensi waktu pemrosesan, konsumsi memori, serta analisis confusion dan diffusion. Pengujian terhadap ketahanan algoritma terhadap serangan nyata tidak termasuk dalam cakupan penelitian ini. Batasan-batasan tersebut ditetapkan untuk menyesuaikan dengan keterbatasan alat, ruang lingkup *Capstone Design*, serta sebagai fokus utama penelitian dalam mengkaji efektivitas algoritma kriptografi ringan pada komunikasi IoT sederhana.