

BAB I

PENDAHULUAN

A. Latar Belakang

Isu polusi udara saat ini menjadi salah satu masalah lingkungan dan kesehatan masyarakat paling serius di dunia. Partikulat halus PM_{2.5}, dengan ukuran $\leq 2,5 \mu\text{m}$, mampu menembus hingga ke dalam paru-paru dan sistem peredaran darah, sehingga meningkatkan risiko penyakit pernapasan, kardiovaskular, dan kematian dini. Paparan PM_{2.5} yang melebihi ambang batas aman sebesar $15 \mu\text{g}/\text{m}^3$ per 24 jam telah menjadi ancaman global yang signifikan terhadap kesehatan manusia [1].

Data terbaru di Indonesia menunjukkan bahwa kualitas udara di berbagai wilayah perkotaan masih berada pada kondisi yang perlu mendapat perhatian serius. Konsentrasi PM_{2.5} di sejumlah kota besar sering melampaui ambang batas WHO maupun standar nasional, terutama pada periode tertentu seperti musim kemarau. Kondisi ini menunjukkan bahwa permasalahan pencemaran udara bersifat lintas wilayah dan memerlukan sistem pemantauan yang mampu menyediakan data secara kontinu, akurat, dan dapat diandalkan sebagai dasar pengambilan keputusan berbasis data[2].

Situasi ini juga relevan dengan kondisi di Kepulauan Riau, khususnya Kota Tanjungpinang sebagai ibu kota provinsi dan pusat aktivitas ekonomi serta pelabuhan. Data pemantauan kualitas udara regional menunjukkan bahwa nilai PM_{2.5} pada beberapa periode berada pada kategori "tidak sehat bagi kelompok sensitif". Oleh karena itu, diperlukan sistem pemantauan yang efektif untuk memberikan data *real-time* tentang kondisi udara di wilayah tersebut[3][4].

Untuk mengatasi permasalahan ini, perkembangan teknologi *Internet of Things (IoT)* telah dimanfaatkan dalam sistem pemantauan kualitas udara. Sensor berbiaya rendah yang terhubung ke internet memungkinkan pemantauan konsentrasi PM_{2.5} secara *real-time* dan berkelanjutan. Data yang diperoleh akan disimpan secara otomatis pada sistem server lokal dan *database* untuk mendukung proses analisis dan visualisasi lebih lanjut. Sistem *IoT* biasanya menggunakan protokol komunikasi seperti *Wi-Fi* dengan *MQTT (Message Queuing Telemetry Transport)* karena bersifat ringan dan efisien, serta teknologi *Low Power Wide Area Network (LPWAN)* seperti *LoRa/LoRaWAN* yang memiliki jangkauan luas dan konsumsi daya rendah, sehingga

sesuai untuk implementasi sensor di wilayah perkotaan luas, sebagaimana ilustrasi arsitektur sistem pada Gambar 1 [5][6].

Namun, sistem monitoring berbasis IoT masih rentan terhadap ancaman keamanan karena banyak data ditransmisikan tanpa enkripsi yang memadai. Sejumlah penelitian menunjukkan bahwa masih banyak sistem IoT yang mengirimkan data sensor tanpa perlindungan enkripsi, seperti penggunaan server MQTT tanpa TLS/SSL, sehingga data berpotensi disadap atau dimanipulasi. Hal ini dapat mengganggu integritas dan keandalan data lingkungan yang digunakan sebagai dasar pengambilan kebijakann [7].

Tingkat urgensi keamanan data semakin meningkat seiring dengan bertambahnya kasus kebocoran data digital di Indonesia, salah satunya dugaan kebocoran data kependudukan Dukcapil pada tahun 2023 yang dilaporkan melibatkan sekitar 337 juta data penduduk. Meskipun kasus tersebut terjadi pada aspek penyimpanan data dan berbeda dengan fokus penelitian ini yang membahas keamanan selama proses transmisi, peristiwa tersebut menunjukkan bahwa lemahnya mekanisme perlindungan data dapat menimbulkan risiko yang serius. Pada sistem monitoring lingkungan berbasis *Internet of Things (IoT)*, data sensor seperti PM2.5 yang ditransmisikan melalui jaringan berpotensi mengalami penyadapan maupun manipulasi oleh pihak yang tidak berwenang. Kondisi tersebut dapat menyebabkan informasi kualitas udara menjadi tidak akurat sehingga memengaruhi proses pemantauan dan pengambilan keputusan. Oleh karena itu, diperlukan mekanisme pengamanan transmisi data agar data sensor yang dikirim melalui jaringan IoT tetap terlindungi dari penyadapan dan manipulasi selama proses komunikasi[8].

Meskipun teknologi IoT semakin banyak diterapkan dalam pemantauan kualitas udara, algoritma kriptografi konvensional seperti AES dan RSA sering kali kurang sesuai untuk perangkat IoT karena keterbatasan sumber daya, seperti kapasitas memori, daya listrik, dan kemampuan komputasi. Oleh karena itu, diperlukan algoritma kriptografi ringan (*lightweight cryptography*) yang dirancang khusus untuk perangkat dengan sumber daya terbatas. Salah satu algoritma yang banyak dikaji adalah *PRESENT*, yaitu *lightweight block cipher* yang dirancang untuk memiliki konsumsi memori rendah serta proses enkripsi yang cepat. Algoritma ini juga memiliki tingkat keamanan yang memadai dan efisiensi komputasi yang tinggi untuk mendukung komunikasi data pada sistem IoT. Berbagai penelitian menunjukkan bahwa *PRESENT* unggul dalam efisiensi daya dan kecepatan proses dibandingkan algoritma kriptografi

ringan lainnya, serta terbukti mampu meningkatkan keamanan *end-to-end* tanpa membebani komputasi perangkat IoT. Hal ini menjadikan *PRESENT* relevan untuk melindungi data sensor yang ditransmisikan melalui jaringan IoT berbasis teknologi nirkabel seperti Lora[9][10].

Namun, sebagian besar penelitian di Indonesia terkait sistem monitoring kualitas udara berbasis IoT masih berfokus pada desain sistem dan akurasi sensor, sementara aspek keamanan transmisi data belum menjadi perhatian utama. Beberapa sistem monitoring PM2.5 dan gas polutan lainnya, baik yang terhubung ke *cloud* maupun server lokal, tidak mengintegrasikan mekanisme enkripsi data, sehingga berpotensi menimbulkan risiko kebocoran informasi sensor[11].

Berdasarkan permasalahan tersebut, penelitian ini mengusulkan penerapan algoritma kriptografi ringan *PRESENT* untuk meningkatkan keamanan transmisi data pada sistem monitoring PM2.5 berbasis IoT. Sistem ini mengamankan data pada jalur komunikasi LoRa antara node sensor dan *receiver/gateway* menggunakan algoritma *PRESENT-80* mode CTR. Data dikirim dalam bentuk *ciphertext* sehingga tidak dapat dibaca secara langsung, sedangkan indikasi manipulasi data dapat dikenali melalui validasi hasil dekripsi pada pengujian keamanan. Penelitian ini diharapkan dapat mendukung pengembangan sistem pemantauan kualitas udara yang aman, efisien, dan andal, khususnya di Kota Tanjungpinang.

B. Perumusan Masalah

Rumusan masalah dalam penelitian ini adalah bagaimana merancang dan mengimplementasikan algoritma kriptografi ringan *PRESENT* untuk meningkatkan keamanan transmisi data pada sistem monitoring PM2.5 berbasis *Internet of Things (IoT)*, serta bagaimana mengevaluasi efektivitas keamanan dan kinerja sistem setelah penerapan algoritma tersebut dalam menjaga kerahasiaan data dan mendeteksi manipulasi data melalui validasi hasil dekripsi.

C. Batasan Penelitian

Agar penelitian lebih terfokus dan tidak terlalu luas, maka ditetapkanlah batasan masalah sebagai berikut:

1. Implementasi algoritma *PRESENT* hanya menggunakan *PRESENT-80* dalam mode *Counter (CTR)*. Proses enkripsi dilakukan pada node sensor berbasis ESP32-S3 sebelum data dikirim melalui LoRa, sedangkan proses dekripsi dilakukan pada

node *receiver/gateway* setelah data diterima. Data hasil dekripsi disimpan pada SD Card sebagai penyimpanan lokal/backup dan dikirim ke *server web* lokal untuk disimpan dalam *database* MySQL serta ditampilkan pada *dashboard*. Penelitian ini tidak membahas algoritma kriptografi lain, mode operasi selain CTR, enkripsi pada jalur HTTP/REST API, maupun perangkat IoT selain ESP32.

2. Pengujian keamanan pada penelitian ini dibatasi pada simulasi serangan *sniffing* (*eavesdropping*) dan *Man-in-the-Middle* (*MitM*) pada komunikasi LoRa antara node sensor dan *receiver*. Parameter yang diukur meliputi waktu enkripsi (ms), waktu dekripsi (ms), serta latensi *end-to-end* (ms). Selain itu, dilakukan evaluasi terhadap kemampuan sistem dalam mendeteksi adanya modifikasi data, yang ditunjukkan melalui status *SUSPECT_MODIFIED* pada saat pengujian simulasi *MitM*. Penelitian ini tidak mencakup pengujian terhadap serangan fisik, analisis *side-channel*, gangguan jaringan (*jamming*), serangan pada server web, maupun mekanisme manajemen kunci dinamis.

D. Tujuan Penelitian

Penelitian ini bertujuan untuk mengimplementasikan algoritma kriptografi ringan *PRESENT* pada sistem monitoring PM2.5 berbasis *Internet of Things* (*IoT*) serta menganalisis efektivitasnya dalam menjaga kerahasiaan data dan mendeteksi manipulasi data selama transmisi melalui validasi hasil dekripsi. Selain itu, penelitian ini juga bertujuan untuk mengevaluasi kinerja sistem berdasarkan waktu enkripsi, waktu dekripsi, dan latensi *end-to-end* guna menghasilkan sistem monitoring kualitas udara yang aman, efisien, dan andal.

E. Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat baik secara teoritis maupun praktis dalam upaya meningkatkan keamanan dan keandalan sistem *monitoring* udara berbasis *Internet of Things* (*IoT*). Adapun manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Pengembangan Ilmu Pengetahuan: Memberikan kontribusi pada kajian kriptografi ringan dan keamanan data IoT melalui penerapan algoritma *PRESENT*, serta menjadi referensi bagi penelitian selanjutnya yang berkaitan dengan efisiensi dan keamanan transmisi data pada perangkat berdaya rendah.
2. Peningkatan Keamanan Data *IoT*: Dapat meningkatkan perlindungan data sensor

PM2.5 dari risiko penyadapan, manipulasi, dan serangan *Man-in-the-Middle* sehingga kerahasiaan data lebih terjaga dan indikasi manipulasi dapat dikenali melalui validasi hasil dekripsi.

3. Manfaat Praktis bagi Pengembang Sistem: Memberikan gambaran dalam merancang mekanisme keamanan yang efisien dan ringan, serta menambah pemahaman mengenai pengaruh penggunaan algoritma *PRESENT* terhadap kinerja sistem IoT.
4. Dukungan Data yang Aman untuk Kebijakan Lingkungan: Berpotensi menyediakan data kualitas udara yang lebih aman dan andal sebagai bahan pertimbangan dalam pengambilan keputusan terkait pengelolaan lingkungan.
5. Manfaat Sosial bagi Masyarakat: Memberikan informasi kualitas udara yang lebih akurat dan tepercaya sehingga dapat meningkatkan kesadaran masyarakat terhadap kondisi lingkungan dan dampak kesehatannya.

