## 1. Pendahuluan

### 1.1 Latar Belakang

Keamanan data sangat penting dalam dunia teknologi informasi yang terus berkembang. Salah satu cara untuk melindungi data sensitif dari akses yang tidak sah adalah dengan enkripsi data. Advanced Encryption Standard (AES) adalah algoritma enkripsi yang populer dan aman yang digunakan di seluruh dunia [1]. Algoritma AES telah digunakan dalam berbagai aplikasi, seperti komunikasi nirkabel, perbankan online, dan banyak lagi [2], [3]. Namun, kinerja enkripsi AES juga menjadi perhatian penting dalam beberapa aplikasi, terutama di Internet of Things (IoT). Perangkat IoT memiliki sumber daya yang terbatas dalam hal daya dan komputasi. Oleh karena itu, diperlukan versi AES yang lebih ringan, seperti Small AES, yang dapat berjalan pada perangkat IoT dengan sumber daya terbatas.

Pemantauan suhu adalah salah satu aplikasi yang sering ditemukan dalam perangkat IoT. Pemantauan suhu dapat digunakan dalam berbagai industri, seperti pertanian, penyimpanan makanan, dan rumah pintar [4], [5]. Data suhu dapat diserang untuk dimanipulasi datanya menggunakan jenis serangan *Data Manipulation* [6], [7]. Implementasi Small AES pada perangkat IoT untuk pemantauan suhu dapat menjadi solusi yang efektif untuk mengamankan data suhu. Penelitian ini membahas implementasi Small AES pada perangkat IoT, khususnya menggunakan platform Arduino, yang dikenal dengan sumber daya terbatasnya.Performa Small AES pada perangkat ini akan dianalisis dengan mempertimbangkan kecepatan enkripsi dan memori yang digunakan. Penelitian ini juga akan mencakup studi kasus pemantauan suhu sebagai contoh aplikasi praktis.

Hasil penelitian ini diharapkan dapat memberikan wawasan berharga tentang penggunaan Small AES dalam perangkat arduino dengan sumber daya terbatas. Hal ini dapat bermanfaat dalam pengembangan aplikasi keamanan data pada perangkat arduino yang lebih luas. Pemahaman yang lebih mendalam tentang performa Small AES dalam konteks pemantauan suhu juga dapat membantu dalam meningkatkan keamanan data pada aplikasi IoT yang rentan terhadap serangan.

### 1.2 Perumusan Masalah

Penelitian akhir ini berfokus pada evaluasi dan penerapan Small AES dalam konteks Internet of Things (IoT), khususnya pada platform Arduino yang memiliki keterbatasan sumber daya. Permasalahan utama yang akan diteliti adalah bagaimana mengukur dan menganalisis performansi Small AES pada perangkat arduino. Dua pertanyaan kunci yang akan dijawab dalam penelitian ini adalah pertama, bagaimana cara mengukur dan menganalisis performansi Small AES pada Arduino UNO, terutama dalam hal kecepatan enkripsi dan dekripsi, serta penggunaan memori. Kedua, bagaimana performansi Small AES jika dibandingkan dengan algoritma enkripsi ringan lainnya. Penelitian ini akan mengimplementasikan algoritma enkripsi Small AES serta setidaknya satu algoritma kriptografi ringan lainnya. Parameter yang akan digunakan untuk mengevaluasi performa algoritma-algoritma ini adalah kecepatan enkripsi dan dekripsi, konsumsi memori di perangkat Arduino UNO serta analisis perbandingan plaintext dengan ciphertext menggunakan metode *Bit Avalanche Test* [8].

### 1.3 Tujuan

Penelitian ini bertujuan untuk mengimplementasikan Small AES pada perangkat Arduino UNO, untuk menganalisis performansinya dengan fokus pada faktor- faktor seperti kecepatan enkripsi dan dekripsi, penggunaan memori perangkat, serta perbandingan plaintext dan ciphertext yang dihasilkan dengan menggunakan metode *Bit Avalanche Test*. Selain itu, penelitian ini juga bertujuan untuk melakukan perbandingan performansi Small AES dengan algoritma SPECK [9]. Algoritma SPECK dipilih sebagai pembanding karena algoritma ini menggunakan fungsi sederhana di setiap putarannya, berbanding terbalik dengan Small AES yang di setiap putarannya menggunakan berbagai fungsi yang kompleks [9]. Tujuan dari perbandingan ini adalah untuk mengidentifikasi kelebihan dan kelemahan masing-masing algoritma, sehingga dapat memberikan wawasan yang lebih baik dalam pemilihan algoritma enkripsi yang tepat untuk pengaplikasiannya pada perangkat IoT.

### 1.4 Organisasi Tulisan

Paper ini akan disusun dalam 4 bab setelah pendahuluan, yaitu studi terkait, rancangan dan implementasi program, hasil pengujian, dan kesimpulan. Bagian studi terkait menjelaskan berbagai penelitian atau studi yang berkaitan dengan penelitian ini. Rancangan dan implementasi program memberikan gambaran mengenai bagaimana algoritma Small AES bekerja dan bagaimana alur implementasi Small AES ke Arduino UNO yang menerapkan sensor pemantauan suhu. Hasil pengujian menampilkan dan menjelaskan hasil analisis performansi penerapan algoritma Small AES, kemudian membandingkannya dengan algoritma SPECK. Adapun bagian kesimpulan akan memuat kesimpulan dari hasil pengujian dan analisis hasil pengujian serta saran untuk penelitian lebih lanjut.