Analisis Performansi Algoritma Small AES Menggunakan Arduino UNO, Studi Kasus : Pemantauan Suhu

Muhammad Naufal Rabbani[1], Farah Afianti[2]

[1,2,]Fakultas Informatika, Universitas Telkom, Bandung
[1]muhnaufalr@students.telkomuniversity.ac.id, [2]farahafi@telkomuniversity.ac.id

Abstrak

Keamanan data dalam konteks Internet of Things (IoT) menjadi sangat penting seiring dengan kemajuan teknologi informasi, terutama dalam aplikasi monitoring suhu. Meskipun algoritma Advanced Encrytion Standard (AES) kriptografi sering dipilih, alternatif algoritma yang lebih ringan seperti algoritma Small AES perlu dipertimbangkan. Penelitian ini bertujuan untuk menerapkan dan mengevaluasi performa Small AES pada platform arduino dengan studi kasus pemantauan suhu. Evaluasi dilakukan dengan membandingkan Small AES dengan algoritma SPECK dengan parameter kecepatan enkripsi dan dekripsi, penggunaan memori, dan Bit Avalanche Test. Hasil penelitian menunjukkan Small AES tidak lebih baik dari SPECK dari segi kecepatan enkripsi dan dekripsi. Akan tetapi Small AES unggul dalam penggunaan memori yang lebih sedikit jika dibandingkan dengan SPECK. Dari hasil Bit Avalanche Test, Small AES lebih baik untuk data berukuran besar sedangkan SPECK lebih baik untuk data berukuran kecil.

Kata kunci : AES, Bit Avalanche Test, IoT, Pemantauan Suhu, Small AES, SPECK