

## **Abstrak**

Perkembangan teknologi memungkinkan smart devices untuk saling terhubung melalui Internet of Things (IoT), membuka berbagai peluang aplikasi dalam kehidupan sehari-hari. Namun, hal ini juga menimbulkan kekhawatiran terhadap keamanan data dan privasi, terutama karena perangkat IoT memiliki keterbatasan daya komputasi, memori, dan daya baterai. Untuk mengatasi ini, kriptografi ringan seperti New Lightweight Cryptographic Algorithm (NLCA) menjadi penting. NLCA menjanjikan kinerja lebih cepat dibandingkan dengan algoritma kriptografi ringan lainnya. Namun, belum diuji pada perangkat berdaya komputasi rendah. Dalam penelitian ini, data dengan panjang 32, 200, 400, dan 800 karakter diuji menggunakan simulator perangkat ESP32. Pada data sepanjang 200 karakter, NLCA memerlukan waktu 66,645 detik, sedangkan AES hanya membutuhkan 1,682 detik. Hasil penelitian menunjukkan bahwa NLCA memiliki rata-rata waktu eksekusi yang lebih lama dibandingkan dengan AES, dengan fungsi F menjadi faktor utama yang memperpanjang waktu eksekusi.

**Kata kunci :** kriptografi ringan, *Internet of Things*