ANALYSIS OF SECURE LIGHTWEIGHT DATA FOR THE INTERNET OF THINGS (IOT)

by Ratna Sari

Professor Masahiro Mambo

Dr. Nyoman Bogi Aditya Karna

ABSTRAK

Studi ini menyajikan implementasi dan evaluasi algoritma kriptografi ringan ASCON pada perangkat Internet of Things (IoT) menggunakan mikrokontroler Arduino Uno. Penelitian ini berfokus pada analisis kinerja ASCON dengan menggunakan panjang tag autentikasi yang berbeda (8, 12, dan 16 byte), dengan penilaian rinci terhadap waktu enkripsi, waktu dekripsi, dan efek avalanche yang diukur menggunakan Hamming Distance. Sistem ini mensimulasikan komunikasi Machine-to-Machine (M2M) antara dua perangkat Arduino Uno menggunakan komunikasi serial UART.Mengingat keterbatasan perangkat keras Arduino Uno (2 KB SRAM dan 32 KB memori flash), pustaka ASCON diadaptasi secara manual agar kompatibel dan efisien dalam penggunaan memori, sehingga memungkinkan enkripsi terautentikasi yang aman di lingkungan tertanam dengan sumber daya terbatas.

Hasil penelitian menunjukkan bahwa konfigurasi tag 8-byte menawarkan keseimbangan terbaik antara kecepatan, penggunaan memori, dan keamanan. Konfigurasi ini menghasilkan waktu enkripsi dan dekripsi rata-rata terendah (2208–2236 mikrodetik), dengan persentase avalanche yang kuat (46–50%, dengan puncak 50,96%), serta konsumsi memori paling rendah (22% memori flash dan 42% SRAM). Sebagai perbandingan, tag 12-byte dan 16-byte memberikan nilai avalanche yang lebih stabil (hingga 50,83%), namun memerlukan lebih banyak ruang penyimpanan program dan waktu pemrosesan. Studi ini menyimpulkan bahwa tag 8-byte adalah pilihan optimal untuk implementasi ASCON pada platform IoT yang memiliki keterbatasan sumber daya, karena memberikan keseimbangan praktis antara kekuatan kriptografi dan efisiensi perangkat keras. Implementasi ini dapat menjadi solusi kriptografi ringan untuk transmisi data yang aman dalam skenario IoT di dunia nyata.

Kata kunci: *ASCON, algoritma ringan, kriptografi, IoT.*