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

by Ratna Sari
Professor Masahiro Mambo
Dr. Nyoman Bogi Aditya Karna

ABSTRACT

This study presents the implementation and evaluation of the ASCON lightweight cryptographic algorithm on Internet of Things (IoT) devices using Arduino Uno microcontrollers. The research focuses on analyzing the performance of ASCON using different authentication tag lengths (8, 12, and 16 bytes), with a detailed assessment of encryption time, decryption time, and the avalanche effect measured by Hamming Distance. The system simulates Machine-to-Machine (M2M) communication between two Arduino Uno devices using UART serial communication. Given Arduino Uno ' s hardware limitations (2 KB SRAM and 32 KB flash memory), the ASCON library was manually adapted to ensure compatibility and memory efficiency, enabling secure authenticated encryption within a constrained embedded environment.

The results indicate that the 8-byte tag configuration offers the best balance between speed, memory usage, and security. It achieved the lowest average encryption and decryption times (2208–2236 μ s), with a strong avalanche percentage (46–50%, peaking at 50.96%), while also consuming the least memory (22% flash and 42% SRAM). In comparison, the 12-byte and 16-byte tags provided more stable avalanche values (up to 50.83%) but required additional program storage and processing time. This study concludes that the 8-byte tag is optimal for ASCON implementation on resource-constrained IoT platforms, offering a practical trade-off between cryptographic strength and hardware efficiency. The implementation can serve as a lightweight cryptographic solution for secure data transmission in real-world IoT scenarios.

Key words: *ASCON, lighweight algorithm, cryptographic, IoT.*