# ABSTRACT

The development of the Internet of Things (IoT) has driven an increase in the need for secure Machine-to-Machine (M2M) communication, even though IoT devices generally have limited memory, power, and computing capabilities. Conventional cryptographic algorithms are not always efficient for devices with limited resources, so there is a need for effective and resource-efficient lightweight encryption. This study focuses on comparing the performance of four lightweight cryptographic algorithms—ASCON, PRESENT, LED, and TWINE—in an Arduino-based M2M communication scenario. The evaluation assesses speed, memory usage, the number of machine instructions, as well as the effectiveness of confusion and diffusion.

The method used involves implementing algorithms on two Arduino Uno units, each acting as a transmitter (TX) and receiver (RX) via UART serial communication. Testing was conducted virtually using the Tinkercad platform, with parameters measured including encryption-decryption time, diffusion percentage, Hamming Distance value, algorithm complexity (Big O), and program and data memory usage. Each algorithm was tested five times to obtain consistent data. This process was carried out to ensure that the results were free from the influence of physical environmental variables.

Test results show that ASCON has the best performance with an average encryption time of 318 μs and decryption time of 367 μs, accompanied by a diffusion value close to 50% and high memory usage efficiency. PRESENT and LED excel in lower memory consumption, but have longer processing times compared to ASCON. TWINE offers balanced performance but is not as optimal as ASCON in terms of speed. Based on these results, ASCON is recommended as the most optimal lightweight cryptographic algorithm for M2M communication on IoT devices.

Keyword : IoT, M2M, Lightweight Cryptography, Arduino Uno, Confusion, Diffusion