Abstract

Technological advancements enable smart devices to connect via the Internet of Things (IoT), opening various application opportunities in everyday life. However, this also raises concerns about data security and privacy, especially because IoT devices have limitations in computing power, memory, and battery life. To address this, lightweight cryptography such as the New Lightweight Cryptographic Algorithm (NLCA) is crucial. NLCA promises faster performance compared to other lightweight cryptographic algorithms. However, it has not yet been tested on low-computing-power devices. In this study, data with lengths of 32, 200, 400, and 800 characters were tested using an ESP32 device simulator. For data of 200 characters, NLCA takes 66.645 seconds, whereas AES only requires 1.682 seconds. The research findings indicate that NLCA has a longer average execution time compared to AES, with the F function being the main factor that extends the excecution time.

Keywords: lightweight cryptography, Internet of Things