

Performance Analysis of AES 128 and 256 Algorithms on ESP32

Muhammad Farras Hafis¹, Maman Abdurohman², Febri Dawani³

^{1,2,3}Fakultas Informatika, Universitas Telkom, Bandung

¹farrashafis@students.telkomuniversity.ac.id, ²abdurohman@telkomuniversity.ac.id,

³febridawani@telkomuniversity.ac.id

Abstract

The Internet of Things (IoT) is an idea that emerged as a result of rapid technological development. Currently, the application of IoT is in several fields of agriculture, health, car factories, and smart homes. But sometimes problems such as data theft are one element that is rarely noticed in IoT due to limited resources. In this study, the author applied the AES algorithm to the ESP32 microcontroller and Soil Moisture sensor using MQTT as a communication protocol and then the data will be stored in the MySQL database. Tests conducted in this study include testing the performance of encryption algorithms by comparing AES128 and AES256 using encryption time parameters.

The study conducted two tests to compare average encryption times using AES128 and AES256. The ESP32 device reads and publishes sensor data once a second. The test will be carried out for 5 minutes and the number of packets sent for each test is around $5 \times 60 = 300$ packets, in the test results the algorithm performance gets an average encryption time value of 2.729 ms on the AES128 algorithm and 2.5045 ms on AES256.

Keywords:Internet of Things, MQTT, ESP32, Soil Moisture,AES.

