

## Analisis Performansi Algoritma AES 128 dan 256 pada ESP32

Muhammad Farras Hafis<sup>1</sup>, Maman Abdurohman<sup>2</sup>, Febri Dawani<sup>3</sup>

<sup>1,2,3</sup>Fakultas Informatika, Universitas Telkom, Bandung

<sup>1</sup>farrashafis@students.telkomuniversity.ac.id, <sup>2</sup>abdurohman@telkomuniversity.ac.id,

<sup>3</sup>febridawani@telkomuniversity.ac.id

---

### Abstrak

Internet of Things (IoT) adalah ide yang muncul sebagai hasil dari perkembangan teknologi yang cepat. Saat ini penerapan IoT terdapat pada beberapa bidang pertanian, kesehatan, pabrik mobil, dan *smart home*. Namun terkadang masalah seperti pencurian data merupakan salah satu elemen yang jarang diperhatikan dalam IoT dikarenakan keterbatasan *resource*. Pada penelitian ini penulis menerapkan algoritma AES pada mikrokontroler ESP32 dan sensor *Soil Moisture* menggunakan MQTT sebagai protokol komunikasi dan kemudian data akan disimpan di database MySQL. Pengujian yang dilakukan pada penelitian ini meliputi pengujian performansi algoritma enkripsi dengan membandingkan AES128 dan AES256 menggunakan parameter waktu enkripsi.

Penelitian ini melakukan dua pengujian untuk membandingkan rata-rata waktu enkripsi dengan menggunakan AES128 dan AES256. Perangkat ESP32 membaca dan meng-*publish* data sensor setiap satu detik sekali. Pengujian akan dilakukan selama 5 menit dan jumlah paket yang dikirim untuk masing-masing pengujian yaitu sekitar  $5 \times 60 = 300$  paket, pada hasil pengujian performansi algoritma mendapatkan rata rata nilai waktu enkripsi 2,729 ms pada algoritma AES128 dan 2,5045 ms pada AES256.

**Kata Kunci:** Internet of Things, MQTT, ESP32, Soil Moisture, AES.

---