BAB 5
PENUTUP

Pada bagian ini, berisi tentang kesimpulan dari hasil penelitian dan saran agar dapat menjadi referensi untuk penelitian selanjutnya.

A. Kesimpulan

1. Berdasarkan percobaan yang dilakukan, kombinasi metode AES dan MAC mampu mengamankan komunikasi antar perangkat dalam protokol MQTT dan memastikan *confidentiality, integrity,* dan *Authentication*. Ini dibuktikan dengan hasil percobaan *sniffer* tidak dapat melihat pesan asli dalam proses *sniffing*, nilai MAC dan Key MAC dapat divalidasi dengan benar di sisi penerima.
2. Penggunaan memori pada metode yang digunakan cukup rendah dengan nilai 13% dari total memori yang tersedia.
3. Pengunaan *flash* untuk metode yang digunakan memiliki nilai yang cukup tinggi 67% - 68% dari total *flash* yang tersedia.
4. Waktu yang diperlukan untuk *Generate* MAC memiliki waktu tercepat yaitu 14,27 ms dan waktu terlama 20,91 ms.
5. Waktu yang diperlukan untuk enkripsi pesan memiliki waktu rata-rata enkripsi untuk varian AES 128 berkisar 59,692 ms – 62,292 ms. Sedangkan untuk varian AES 256 berkisar 75,104 ms – 79,17 ms.
6. Waktu yang dibutuhkan untuk dekripsi pesan memiliki waktu rata-rata antara 59,379 ms – 59,38 ms AES 128. Sedangkan untuk variasi AES 256 memiliki waktu rata-rata 76,04 ms.

7. Untuk verifikasi nilai MAC memiliki waktu rata-rata relatif sama yaitu 32,29 ms. Baik SHA2 maupun SHA3 memiliki waktu proses verifikasi MAC yang sama.
8. Frekuensi pengiriman data, variasi keamanan AES128-HMAC-SHA256 memiliki frekuensi pengiriman paling besar yaitu 197 data dan memiliki waktu *generate* dan pengiriman data paling kecil yaitu 0,914 ms. Sedangkan variasi keamanan AES256-HMAC-SHA3_512 memiliki frekuensi pengiriman paling besar yaitu 163 data dan memiliki waktu *generate* dan pengiriman data paling besar yaitu 1,104 ms. Waktu ideal untuk memberikan *delay* antara waktu *generate* dan pengiriman data selanjutnya yaitu 5 detik untuk setiap variasi keamanan yang digunakan.
9. Hasil *overhead analysis* bergantung pada spesifikasi perangkat mikrokontroler yang digunakan, seperti perbedaan ukuran *flash*, memori, *clock speed* dan lainnya. Untuk analisis berdasarkan hasil *overhead*, semua variasi kombinasi AES dan MAC ini cocok untuk diterapkan pada protokol MQTT, terutama pada perangkat Nodemcu ESP32.

B. Saran

1. Pada penelitian ini, server yang digunakan masih bersifat lokal. Oleh sebab itu, untuk penelitian selanjutnya, dapat membuat server yang dapat dilihat melalui website atau aplikasi.
2. Dikarenakan penggunaan MAC yang cocok diterapkan pada protokol MQTT, untuk penelitian selanjutnya dapat menggunakan variasi MAC selain HMAC.
3. Untuk penelitian selanjutnya, dapat melakukan uji coba sistem dengan metode lainnya.