Penerapan Keamanan Komunikasi pada Jaringan LoRa(*Long Range*) Menggunakan Algoritma *Advanced Encryption Standard*(AES) dan *Message Authentication Code*(MAC)

Putri Apriyanti Windya[1], Vera Suryani[2], Aulia Arif Wardana[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]putriawindya@students.telkomuniversity.ac.id, [2] verasuryani@telkomuniversity.ac.id,
[3]auliawardan@telkomuniversity.ac.id

Abstrak

***Internet of Things* (IoT) merupakan suatu hal yang populer saat ini. Penggunaan IoT semakin meningkat setiap tahun khususnya penggunaan LoRa, begitu juga dengan pengembangan perangkat IoT. Salah satu karakteristik perangkat IoT yaitu *resource* yang terbatas. Perangkat ini sering disebut sebagai *constrained device* IoT. Seiring dengan meningkatnya penggunaan LoRa, aspek keamanan komunikasi pada jaringan LoRa juga harus diperhatikan. Akan tetapi, keterbatasan *resource* yang dimiliki oleh perangkat IoT menjadi tantangan dalam memilih metode *security* yang sesuai. Oleh karena itu, untuk mengatasi masalah tersebut dibutuhkan sebuah metode *security* yang sesuai yaitu pemanfaatan algoritma AES dan MAC. Jenis AES yang digunakan pada penelitian ini yaitu AES128 dan AES256. Sedangkan Algoritma MAC yang digunakan adalah *Hash-based Message Authentication Code* (HMAC). Berdasarkan hasil analisis keamanan yang telah dilakukan, metode ini mampu menjamin aspek *confidentiality, integrity* dan *authentication.* Selain itu, penelitian ini juga melakukan analisis *overhead* pada *constrained devices* IoT kelas 0 dan kelas 2. Hasil analisis *overhead* menunjukkan bahwa metode ini cocok untuk diterapkan pada kelas 0 dan kelas 2.**

Kata kunci : ***Long Range, constrained devices, CIA, AES, HMAC***