BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Semakin berkembangnya teknologi internet dan keperluan manusia tentang teknologi, maka semakin banyak penelitian yang akan hadir, salah satunya pada IoT. Teknologi IoT mampu menghubungkan berbagai objek untuk saling bertukar informasi dan bekerja sama mencapai suatu keputusan. Penerapan IoT dalam berbagai bentuk telah mulai diaplikasikan pada banyak aspek kehidupan manusia, sehingga akan semakin banyak perangkat dan pengguna yang terhubung dan mengirimkan lebih banyak data. Lebih banyak perangkat yang terhubung, menyiratkan lebih banyak kerentanan dan lebih banyak titik akses untuk dieksploitasi oleh peretas. Dengan meningkatnya jumlah perangkat IoT yang terhubung ini, teknik untuk menyediakan keamanan informasi merupakan tantangan utama yang harus diatasi selama perancangan perangkat tersebut.

Salah satu contoh teknologi IoT, seperti *NarrowBand-Internet of Things* (NB-IoT) yang merupakan teknologi berbasis standar *Low Power Wide Area* (LPWA) dikembangkan untuk memungkinkan berbagai perangkat dan layanan IoT baru [1]. Dalam *Long Term Evolution* (LTE) Rilis 13 [2], NB-IoT diperkenalkan, memberikan peningkatan lebih lanjut seperti pengurangan biaya dan kompleksitas perangkat, masa pakai baterai yang lebih lama, dan *coverage* yang ditingkatkan. Teknologi ini juga menyediakan keamanan *end-to-end*, yang memerlukan fitur keamanan dan otentikasi tepercaya [3]. Sehingga, algoritma kriptografi yang digunakan untuk mengamankan data harus disesuaikan dengan kebutuhan perangkat dengan sumber daya terbatas. Algoritma yang dapat digunakan untuk kerahasiaan dan perlindungan integritas pengguna sistem LTE tersebut diantaranya algoritma SNOW 3G dan AES. Hal ini didefinisikan dalam *Technical Specification System Architecture Evolution* (SAE) dari 3GPP di bawah spesifikasi Arsitektur Keamanan [3].

Menurut penelitian sebelumnya [4], menyimpulkan bahwa SNOW 3G menjamin efisiensi dan kecepatan selama proses enkripsi/dekripsi karena

memiliki kompleksitas waktu linier. Selain itu, SNOW 3G mengkonsumsi jumlah memori yang konstan dan diketahui sangat berguna untuk sistem dengan memori kerja kecil. Dari dua faktor tersebut, maka dari itu SNOW 3G dipilih menjadi algoritma kerahasiaan dan integritas untuk UMTS (UEA2/UIA2) dan LTE (EIA1). Sedangkan, algoritma AES merupakan algoritma yang dirancang untuk tujuan keamanan dan perlindungan data [5]. Dikembangkan dan diperkenalkan oleh NIST pada tahun 2001, AES memiliki berbagai parameter terbaik seperti kemanan, kinerja, efisiensi, kemampuan implementasi baik *hardware* maupun *software*, dan fleksibilitas.

Penelitian pada Tugas Akhir ini, mengusulkan bagaimana melakukan pengujian dan analisa simulasi performansi untuk algoritma AES dan SNOW 3G seperti keacakan dan ketidakakuratan data enkripsi berdasarkan masing-masing nilai *avalanche effect* dan *entropy*. Sehingga, nantinya bisa didapatkan kesimpulan algoritma mana yang paling efektif dan paling aman untuk bisa diimplementasikan pada sistem jaringan teknologi IoT.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka dapat dirumuskan beberapa masalah yang berkaitan dengan penelitian ini, yaitu:

1. Penggunaan algoritma AES dan SNOW 3G sebagai algoritma perbandingan.
2. Simulasi performansi untuk algoritma AES dan SNOW 3G.
3. Penelitian terkait keacakan dan ketidakpastian data yang dihasilkan oleh algoritma AES dan SNOW 3G.

1.3 Tujuan dan Manfaat

Tujuan dari penelitian pada Tugas Akhir ini adalah melakukan analisa keacakan dan ketidakpastian data yang dihasilkan oleh algoritma AES dan SNOW 3G.

Sedangkan, manfaat dari penelitian ini adalah meningkatkan keamanan pada jaringan dengan berbasis IoT, terutama untuk jaringan pada sistem LTE.

1.4 Batasan Masalah

Adapun batasan masalah yang dilakukan pada penelitian ini, yaitu:

1. Penggunaan CrypTool sebagai perangkat lunak simulasi kedua algoritma uji.
2. Pengujian enkripsi dan dekripsi tidak dilakukan secara paralel.

1.5 Metode Penelitian

Metode yang digunakan dalam menyelesaikan proses penelitian ini terdiri daribeberapa tahapan, yaitu:

1. Studi literatur

   Tahap studi literatur merupakan tahap mencari, mengumpulkan, dan mempelajari teori-teori referensi pendukung terkait penelitian, seperti teknik keamanan jaringan, enkripsi dan dekripsi data, algoritma AES dan SNOW 3G, serta materi lain.
2. Perancangan sistem

   Tahap selanjutnya melakukan perancangan sistem keamanan dengan menggunakan algoritma SNOW 3G dan AES.
3. Simulasi sistem

   Pada tahap ini dilakukan simulasi performansi algoritma enkripsi dan dekripsi pada perangkat lunak, sehingga menghasilkan suatu hasil untuk memecahkan masalah pada penelitian ini.
4. Pengujian dan analisis hasil

   Selanjutnya melakukan pengujian terhadap performansi dan kemudian melakukan analisis hasil kinerja algoritma berdasarkan parameter ukur yang telah ditentukan.
5. Penarikan kesimpulan

   Tahap penarikan kesimpulan ini berdasarkan data-data yang didapatkan dari hasil berdasarkan tahap perancangan, simulasi, pegujian, dan analisa performansi pada kedua algoritma.