BAB I PENDAHULUAN

1.1 Latar Belakang

Dalam beberapa tahun terakhir, Indonesia telah menyaksikan peningkatan dalam pengembangan teknologi *Internet of Things* (IoT). *Internet of Things* (IoT) adalah jenis teknologi yang memungkinkan perangkat yang memiliki sensor dapat berkomunikasi dan bertukar data dengan perangkat lain melalui internet [1]. Permintaan pasar untuk layanan digital meningkat hingga 38.33% dari 2017 hingga 2022, menjadikannya sektor yang paling berkembang diikuti keamanan *cyber* dan layanan telepon [2].

Teknologi automatisasi yang sudah terintegrasi dengan *Internet of Things* (IoT) sangat penting untuk memulai revolusi industri 4.0. *Internet of Things* membutuhkan kemampuan untuk mengumpulkan dan mengirimkan informasi secara instan. Perangkat sensor dapat berkomunikasi dengan perangkat lain dalam jaringan melalui internet melalui jaringan sensor nirkabel (JSN) atau *Wireless Sensor Network* (WSN) [3].

Perangkat dapat mengumpulkan dan mengirimkan data melalui teknologi internet JSN. Dalam JSN, *node* adalah sensor, dan *sink* atau *basestation* adalah perangkat yang mengumpulkan data dari *node* [4]. Jenis data yang dapat dikumpulkan dan ditransmisikan oleh *node* ditentukan oleh jenis sensor yang digunakan di lapangan. Data yang diperoleh akan dikirim dan ditampilkan pada *sink*, yang memungkinkan pengguna mendapatkan data dibanyak tempat dengan berbagai parameter sekaligus. Karena *node* mengirimkan data secara nirkabel selama *node* berada dalam jaringan internet, jarak antara *node* dan *sink* tidak dibatasi oleh batasan fisik kabel.

Semakin banyak aplikasi IoT, lebih banyak serangan siber juga terjadi. Laporan Symantec dari tahun 2017 menunjukkan bahwa *router*, perangkat yang paling banyak digunakan di JSN, menyebabkan serangan *cyber* paling banyak sebesar 75,5%, dengan perangkat kamera menyumbang 15,5% dari rata-rata 5223 laporan serangan per bulan [5]. Untuk menyelesaikan masalah di atas, desain JSN yang dapat mengirimkan data dengan kecepatan tinggi diperlukan. Namun, kriptografi adalah salah satu cara yang dapat digunakan untuk memastikan *traffic* data yang aman saat mengirimkan data.

Pada tahun 2022, Syah Fadel P.D. menyelidiki desain awal JSN. Jaringan yang dibuat oleh penelitian ini dapat mengirimkan data sensor getar dari *node* ke *sink*. Ini akan memungkinkan melihat grafik di internet secara *real-time*. Sebuah studi meneliti kualitas layanan (QoS) protokol komunikasi TCP dan UDP [1], tetapi tidak mencakup variabel keamanan. Ini menunjukkan bahwa serangan *cyber* memiliki kemampuan untuk memengaruhi data yang dikirimkan ke jaringan.

Penelitian serupa lainnya juga telah pernah dilakukan oleh Pramudio

Fajriand (2023). Pada penelitian tersebut menganalisis jaringan sensor nirkabel untuk mendeteksi gerak benda menggunakan metode *client-server* dengan *socket programming* dengan algoritma kriptografi Rivest-Shamir-Adleman [6]. Penelitian ini berfokus pada perancangan dari sisi algoritma kriptografi AES yang digunakan. Pada penelitian yang akan dilakukan menggunakan algoritma AES sebagai kriptografinya. AES dirancang agar dapat diimplementasikan dengan efisien dalam perangkat keras. Banyak perangkat keras modern, seperti prosesor Intel dan AMD, memiliki instruksi AES-NI (AES New Instructions) yang mempercepat proses enkripsi dan dekripsi. Banyak pustaka kriptografi populer (seperti OpenSSL, Crypto++, dan Bouncy Castle) mendukung AES, membuatnya mudah untuk diintegrasikan ke dalam aplikasi dan sistem yang ada. AES juga diadopsi secara luas oleh industri, organisasi internasional, dan banyak lembaga keamanan global, memberikan kepercayaan tinggi pada algoritma ini.

Penelitian yang dibahas menunjukkan bahwa kedua penelitian membutuhkan jaringan yang tidak hanya dapat mengirimkan data dengan cepat tetapi juga mengkomunikasikan data secara aman. Selain itu, penelitian ini menyelidiki bagaimana teknik kriptografi yang digunakan mempengaruhi kinerja QoS jaringan. Penulis akan membangun jaringan sensor nirkabel yang memungkinkan data berkomunikasi secara serial pada 1 buah *client* dan pararel pada penggunaan 2 atau lebih *client* dengan *socket* pada perangkat *node* sensor. Dengan demikian, data dapat ditampilkan pada situs web secara *real-time*. Metode kriptografi AES digunakan untuk melindungi transmisi data jaringan dan kinerjanya dibandingkan dengan menggunakan protokol TCP dan UDP sebagai protokol komunikasinya .

1.2 Rumusan Masalah

Rumusan masalah dari penelitian ini adalah sebagai berikut:

1. Bagaimana perbandingan protokol komunikasi TCP dan UDP dengan algoritma kriptografi AES?
2. Bagaimana QoS dari jaringan yang telah dibuat?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengetahui pengaruh algoritma kriptografi AES pada protokol komunikasi TCP dan UDP.
2. Mengetahui QoS jaringan sensor nirkabel yang telah dibuat.

1.4 Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut:

1. Mengetahui pengaruh algoritma kriptografi AES pada jaringan.
2. Mengetahui perbandingan protokol komunikasi TCP dan UDP.
3. Dapat digunakan untuk referensi perancangan jaringan sensor nirkabel lainnya.

4. Dapat memisahkan perangkat pengumpul data dengan perangkat pengolah dan penampil data tanpa menggunakan sambungan langsung kabel.
5. Mendapatkan grafik waktu dari data yang diperoleh.
6. Dapat melakukan pengamanan data dengan kriptografi AES dengan menghasilkan QoS yang masih dalam standar ITU (*International Telecommunication Union*)
7. Dapat melakukan pengiriman data secara *Multi-client*

1.5 Batasan Masalah

Penelitian ini memiliki batasan masalah sebagai berikut:

1. Penelitian ini berfokus pada jaringan sensor nirkabel dengan algoritma kriptografi AES.
2. Protokol komunikasi yang digunakan adalah TCP dan UDP.
3. Penelitian ini memperhatikan parameter *Quality of Service* (QoS).
4. Parameter QoS yang diperhatikan adalah *throughput* dan *delay*.
5. Data yang dikirimkan merupakan data dari sensor yang sudah ada.
6. Data yang ditampilkan dari sensor berupa data grafik.
7. Data yang diamati oleh sensor adalah gerak jatuh bebas.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini membahas mencakup pembahasan mengenai latar belakang dari penelitian, rumusan masalah, tujuan yang akan dicapai, batasan-batasan masalah, manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini membahas mengenai landasan teori yang mendukung penyelesaian masalah pada penelitian ini.

BAB III METODOLOGI

Bab ini berisikan penjelasan mengenai metode yang mencakup diagram alir penelitian, prinsip kerja, bahan yang digunakan, perancangan jaringan dan teknik pengujian yang dilakukan.

BAB IV HASIL DAN ANALISIS

Bab ini berisikan informasi hasil dan pembahasan dari penelitian tugas akhir ini.

BAB V SIMPULAN DAN SARAN

Bab ini berisikan kesimpulan dari penelitian yang telah dilakukan dan saran untuk penelitian selanjutnya.