BAB 1 PENDAHULUAN

1.1 Latar Belakang

Dalam era digital saat ini, sistem kontrol yang terhubung ke jaringan semakin rentan terhadap serangan siber yang dapat mengakibatkan kerusakan fisik dan gangguan operasional. Dalam dunia industri, terdapat beberapa kasus serangan terhadap sistem kontrol jaringan. Pada tahun 2000, terjadi serangan pada sistem pengendali limbah berbasis SCADA yang dikelola oleh Maroochy Shire Council, Australia. Sistem pengendali yang diserang mengalami malafungsi yang menyebabkan limbah mentah tumpah ke taman, sungai, dan area sekitar tempat pengolahan limbah. Akibat dari serangan ini adalah terjadinya pencemaran air dan timbul bau tidak sedap di sekitar pemukiman warga[1].

Serangan siber serupa juga terjadi pada tahun 2015 di Ukraina. Serangan yang menargetkan 3 perusahaan distribusi daya listrik tersebut berdampak pada pemadaman listrik ke 225.000 pelanggan selama beberapa jam. Serangan ini merupakan jenis serangan *False Data Injection Attack* (FDIA) yang merusak keluaran estimasi status sistem tenaga listrik dengan menyuntikkan data palsu ke dalam pengukuran sistem[2]. Dengan melihat kedua kasus tersebut, keamanan dalam sistem kontrol menjadi sangat penting, terutama dalam aplikasi industri yang mengandalkan kontrol otomatis untuk menjaga efisiensi dan keselamatan.

Terdapat berbagai macam serangan siber yang dapat terjadi di industri, salah satunya serangan *eavesdropping*. *Eavesdropping* merupakan serangan *hacking* dengan membajak jaringan komunikasi korban dan mencuri informasi yang masuk ke komputer korban[3]. Serangan *eavesdropping* merupakan serangan yang terjadi paa tahap *reconnaissance*, yang merupakan tahap awal sebelum terjadinya serangan siber yang dapat memberikan dampak besar seperti 2 contoh kasus sebelumnya[4]. Serangan *eavesdropping* dapat dilakukan dengan memanfaatkan aplikasi *packet sniffing* yang dapat diunduh secara gratis di internet. Data yang dikirim pada jaringan dapat dilindungi dari serangan *eavesdropping* dengan cara mengenkripsi data yang dikirim.

Enkripsi dapat mengubah data asli (*plaintext*) menjadi data terenkripsi (*ciphertext*). Data yang telah dienkripsi tidak dapat dibaca oleh pelaku serangan dikarenakan informasi yang ada telah diubah ke bentuk *cipher text*. Dalam menerapkan enkripsi pada komunikasi data, terdapat beberapa algoritma enkripsi yang dapat digunakan. Salah satu metode enkripsi yang paling sering digunakan di industri adalah enkripsi Rivest-Shamir-Adleman (RSA)[5].

Algoritma enkripsi RSA merupakan sistem sandi asimetris, dimana kunci untuk melakukan enkripsi akan berbeda dengan kunci yang digunakan untuk melakukan dekripsi. Perbedaan kunci ini akan meningkatkan keamanan sistem

dikarenakan akan lebih sulit untuk menebak kunci privat walau sudah mengetahui kunci publik yang diberikan. Dengan menerapkan enkripsi asimetris seperti RSA pada sistem kendali jaringan, maka data yang dikirimkan antar komputer dan alat industri akan terjaga keamanannya dari serangan siber.

Penelitian terkait serangan *eavesdropping* pada komunikasi nirkabel telah dilakukan oleh Li Yuan pada tahun 2017. Penelitian yang dilakukan meneliti terkait penggunaan *Stochastic Algorithm Framework* (SAF) dalam pengoptimalan daya transmisi sensor untuk memaksimalkan tingkat komunikasi yang aman. Simulasi yang dilakukan membuktikan bahwa SAF dapat mencapai tingkat komunikasi yang aman yang lebih tinggi, meskipun ada ancaman dari eavesdropping dan jamming.

Pada tahun 2018, penelitian terkait penerapan enkripsi data di sistem kendali telah dilakukan oleh Kogiso[4]. Penelitian yang dilakukan menerapkan algoritma enkripsi RSA dan ElGamal untuk menjaga keamanan data dari serangan *eavesdropping* pada kendali PID motor DC. Hasil dari penelitian yang dilakukan adalah sistem yang telah dienkripsi dapat bekerja dengan baik walau terjadi degradasi kinerja dari motor DC.

Kogiso melanjutkan penelitian terkait sistem enkripsi pada pengendali PID pada tahun 2023. Pada penelitian ini, Kogiso menggunakan *Keyed-Homomorphic Public Key Encryption* (KH-PKE) dalam mengenkripsi data pada kendali posisi PID. Hasil yang didapatkan adalah penggunaan KH-PKE dalam enkripsi sangat berguna dalam menjaga sistem dari serangan pemalsuan data dan memberikan kinerja kontrol yang lebih baik dari metode konvensional. Perbedaan dari penelitian ini dengan penelitian yang telah dilakukan oleh Kogiso adalah media komunikasi yang digunakan, dimana Kogiso menggunakan media kabel untuk mengirimkan data ke *controller* untuk menggerakkan motor DC. Hal ini akan berbeda dengan penelitian yang dilakukan, dimana pada penelitian ini akan menggunakan metode nirkabel dengan komunikasi TCP dan UDP.

Berdasarkan penelitian sebelumnya, diketahui bahwa keamanan dalam sistem kendali sangatlah diperlukan agar tidak terjadi serangan siber yang dapat mengganggu kinerja dari alat di industri. Salah satu perangkat yang sering digunakan di industri adalah motor DC[6]. Apabila terjadi serangan siber yang menargetkan motor DC yang dikendalikan oleh pengendali PID, maka motor tersebut dapat berhenti pada titik yang tidak diinginkan ataupun tidak berhenti pada sudut yang sudah ditetapkan.

Serangan *eavesdropping* yang telah dibahas dapat membuat pelaku serangan siber mengetahui jenis sinyal dan format dari data yang dikirimkan antara pengendali dan alat yang dikendalikan. Dalam hal ini pelaku dapat mengirimkan sinyal yang sesuai dengan format yang didapat dan mengirimkan data palsu ke alat yang dikendalikan tersebut[4]. Kondisi ini akan merugikan perusahaan yang terkena serangan tersebut, dimana motor DC yang berfungsi mengendalikan presisi sudut pergerakan, menjadi tidak bergerak sesuai dengan

sudut yang diinginkan. Apabila hal ini terjadi pada motor DC yang terpasang di tangan robotik yang berguna untuk memindahkan barang, maka kesalahan sudut yang terjadi akan membuat barang yang dipindahkan justru berpindah ke posisi yang salah.

Penelitian ini akan berfokus dalam menerapkan enkripsi RSA agar serangan *eavesdropping* tidak dapat membuat penyerang siber mengetahui format dari data tersebut dan tidak dapat mengirimkan data ke rangkaian *driver* dari alat yang akan dikendalikan. Algoritma RSA dipilih dikarenakan RSA merupakan algoritma enkripsi publik. Selain memiliki kunci privat dan publik yang meningkatkan keamanan data, RSA merupakan algoritma enkripsi yang telah banyak diterapkan di dunia industri dan keamanan, yang membuat enkripsi ini lebih mudah untuk diterapkan pada sistem yang ada sekarang. Penggunaan algoritma enkripsi RSA yang cukup terkenal adalah dalam protokol komunikasi *Secure Sockets Layer* (SSL) dan *Transport Layer Security* (TLS)[5].

Selain dalam mengamankan data, kinerja dari sistem yang telah dienkripsi datanya perlu dibandingkan dengan sistem yang belum dienkripsi agar pengaruh dari enkripsi RSA terhadap kinerja sistem dapat diketahui. Berbeda dengan penelitian sebelumnya, dikarenakan media komunikasi dari sistem berupa komunikasi nirkabel, maka akan dilakukan analisis dari 2 metode komunikasi yang sering digunakan dalam komunikasi ini, yaitu *Transmisson Control Protocol* (TCP) dan *User Datagram Protocol* (UDP). TCP merupakan komunikasi yang sering digunakan dalam *Websocket*, sedangkan UDP merupakan metode yang dapat memberikan data secara *real-time* yang sangat cocok untuk kondisi riil dari kendali motor DC karena mengandalkan kecepatan pengiriman data.

Analisis yang akan dilakukan adalah analisis respons transien, yang mencakup 5 parameter, yaitu *Delay Time*, *Rise Time, Peak Time, Settling Time,* dan *Maximum Overshoot*. Parameter yang juga akan diukur adalah *Error Steady State* dari respon sistem. Analisis transien akan dilakukan pada sistem kendali yang belum diterapkan enkripsi dan telah dilakukan enkripsi, dengan menggunakan protokol komunikasi TCP dan UDP. Metode TCP akan menggunakan *websockets* dalam melakukan komunikasi dan UDP akan menggunakan UDP *Sockets* dalam pengiriman data kendali.

Hasil yang akan dilihat dari penelitian ini adalah keberhasilan dari enkripsi data pada komunikasi nirkabel yang dibuat, dan hasil analisis respon transien dari motor DC yang telah dienkripsi dan menggunakan metode komunikasi TCP dan UDP. Dengan didapatkan hasil dari perbandingan komunikasi dan performa dari motor DC yang dikendalikan, dapat menjadi pertimbangan dalam menerapkan sistem kendali nirkabel yang terenkripsi pada industri.

1.2 Rumusan Masalah

Rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Bagaimana implementasi algoritma RSA dalam menjaga keamanan komunikasi data pada sistem kendali PID berbasis jaringan nirkabel?
2. Bagaimana pengaruh penerapan enkripsi RSA terhadap respon transien motor DC dengan protokol komunikasi TCP?
3. Bagaimana pengaruh penerapan enkripsi RSA terhadap respon transien motor DC dengan protokol komunikasi UDP?

1.3 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut:

1. Menganalisis implementasi algoritma RSA dalam mengamankan komunikasi data pada sistem kendali motor DC berbasis jaringan nirkabel.
2. Menganalisis pengaruh enkripsi RSA terhadap karakteristik respon transien sistem kendali PID motor DC dengan protokol TCP dan UDP.

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat berupa:

1. Meningkatkan keamanan komunikasi data dalam sistem kendali nirkabel.
2. Membantu pengembangan sistem kendali yang lebih tahan terhadap serangan siber.
3. Menganalisis dampak enkripsi terhadap performa sistem kendali.
4. Memberikan panduan dalam memilih protokol komunikasi untuk kendali PID motor DC.

1.5 Batasan Masalah

Penelitian ini memiliki batasan masalah sebagai berikut:

1. Penelitian ini berfokus pada pengendali PID nirkabel yang jaringan sensor nirkabel dengan algoritma kriptografi RSA.
2. Pengendalian yang dilakukan berupa pengendalian sudut putaran motor DC.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini membahas mengenai latar belakang penelitian, rumusan masalah, tujuan yang ingin dicapai, batasan masalah, manfaat penelitian, dan sistem penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini membahas mengenai landasan teori pendukung yang digunakan dalam penyelesaian masalah pada tugas akhir 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 ANALISA

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

BAB V KESIMPULAN DAN SARAN

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