BAB I PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi digital telah membuat sistem kontrol industri semakin terhubung dengan jaringan, namun hal ini juga meningkatkan potensi risiko serangan siber. Sistem-sistem tersebut menjadi lebih rentan terhadap ancaman digital, yang bahkan bisa berpengaruh langsung pada aspek fisik dan operasional. Salah satu contoh besar terjadi pada tahun 2000 di Australia, ketika sistem pengendali limbah berbasis SCADA milik Maroochy Shire Council diretas oleh mantan karyawan menggunakan perangkat radio ilegal. Insiden ini menyebabkan gangguan sistem yang berujung pada tumpahan limbah mentah ke taman, sungai, dan area sekitarnya, yang mengarah pada pencemaran dan bau tak sedap di kawasan pemukiman. Peristiwa ini menunjukkan bahwa keamanan sistem kontrol merupakan aspek yang sangat penting, terutama bagi industri yang sangat bergantung pada otomatisasi untuk mencapai efisiensi dan menjaga keselamatan [1].

Salah satu tipe serangan siber yang sering terjadi pada sistem berbasis jaringan adalah *eavesdropping*, yaitu teknik penyadapan di mana pelaku mencuri informasi yang sedang dikirimkan melalui jaringan komunikasi korban [2]. Penyerang umumnya menggunakan perangkat lunak *packet sniffer* untuk menyadap lalu lintas data, dan aplikasi ini dapat dengan mudah ditemukan di internet, sehingga meningkatkan potensi eksploitasi jika tidak ada perlindungan yang memadai. Data sensitif seperti perintah kontrol, informasi teknis, atau kredensial dapat diakses tanpa terdeteksi. Oleh karena itu, penggunaan enkripsi data dianggap sebagai langkah penting untuk melindungi kerahasiaan dan integritas komunikasi dalam sistem kontrol industri [3].

Berbagai penelitian sebelumnya telah mempelajari metode enkripsi dalam sistem kontrol untuk memperkuat keamanan komunikasi. Kogiso dan timnya pada tahun 2015 menerapkan enkripsi homomorfik berbasis RSA dan ElGamal pada pengendali PID motor DC untuk menyembunyikan parameter dan sinyal dalam pengontrol. Metode ini terbukti efektif dalam menjaga kerahasiaan data, namun memiliki kompleksitas komputasi yang tinggi, sehingga kurang cocok untuk perangkat dengan sumber daya terbatas [4].

Pada tahun 2023, Kogiso melanjutkan penelitiannya dengan mengembangkan *Keyed-Homomorphic Public Key Encryption* (KH-PKE) yang dapat mendeteksi serangan siber secara *real-time*, seperti pemalsuan sinyal dan parameter kontrol, serta mengurangi beban komputasi dan dampak kuantisasi pada sistem kontrol [5]. Namun, metode ini masih memiliki kekurangan berupa kompleksitas implementasi yang tinggi dan belum terbukti efektif pada perangkat dengan sumber daya terbatas di lingkungan industri. Selain itu, Li Yuan pada tahun 2017 mengembangkan *Stochastic Algorithm*

Framework (SAF) untuk mengoptimalkan daya transmisi sensor, agar komunikasi tetap aman meskipun berada dalam kondisi rawan penyadapan dan *jamming* [6]. Meskipun demikian, sebagian besar penelitian tersebut masih terbatas pada skala besar atau simulasi dan belum banyak diterapkan langsung pada sistem kendali berbasis mikrokontroler yang memiliki keterbatasan sumber daya.

Salah satu metode enkripsi adalah *Elliptic Curve Cryptography* (ECC). Algoritma ini menyajikan kekuatan kunci yang sama dengan panjang kunci yang berbeda, yang mana sebagai contoh 256-bits ECC hampir sama kuatnya dengan 3072-bits RSA. Hal ini dapat mengefisiensikan komputasi serta ruang penyimpanan [7].

Pada tahun 2023, Naura menguji penggunaan algoritma ECC dalam sistem komunikasi dengan menerapkannya pada komunikasi sistem *smart grid*. Hasil penelitian menunjukkan bahwa metode ECC efektif dalam menawarkan keamanan yang sebanding tetapi dengan panjang kunci yang lebih pendek dengan salah satu jenis algoritma metode asimetris lainnya seperti algoritma RSA [8]. Namun, penerapan enkripsi ECC dalam sistem kontrol yang lebih rumit, seperti kendali PID pada motor DC, masih jarang diteliti. Sistem kontrol PID memerlukan tingkat presisi yang tinggi dan respons yang cepat, sehingga penting untuk mengevaluasi sejauh mana enkripsi ECC dapat diterapkan tanpa mengurangi kinerja kendali.

Penggunaan kontrol PID dalam penelitian ini didasarkan pada fakta bahwa algoritma PID adalah metode umpan balik yang paling banyak digunakan dalam sistem kontrol industri. Sekitar 90% sistem kontrol yang diterapkan di industri menggunakan kontrol PID, karena algoritma ini memberikan keseimbangan antara kemudahan implementasi, proses *tuning* yang sederhana, serta kemampuan dalam menjaga kestabilan dan akurasi sistem [9]. Oleh karena itu, penelitian ini fokus pada penerapan ECC dalam kontrol motor dengan menggunakan kontrol PID, serta menganalisis pengaruhnya terhadap respons transisi.

Penelitian ini dikembangkan untuk mengatasi kesenjangan antara kebutuhan akan keamanan komunikasi dan efisiensi sistem kontrol *real-time*. Analisis akan dilakukan terhadap lima parameter respons transien, yaitu *delay time, rise time, peak time, settling time*, dan *maximum overshoot*, serta analisis terhadap *steady state error*. Respon transien dan *steady state error* perlu dianalisis agar dapat menunjukkan kecepatan sistem dalam merespon perubahan perintah dan kemampuan sistem untuk mencapai dan mempertahankan target diinginkan yang dikirimkan melalui jaringan TCP/IP yang dienkripsi. Respon transien dan *error steady state* yang buruk akan menjadikan sistem lambat dalam merespon perubahan masukan dan tidak mampu mencapai posisi yang akurat setelah kondisi stabil. Dengan demikian, penelitian ini diharapkan dapat memberikan wawasan yang lebih mendalam mengenai pengaruh penerapan enkripsi terhadap kinerja sistem kendali pada pengontrol, sekaligus menjadi

pedoman dalam pengembangan sistem kendali yang aman dan efisien untuk digunakan di lingkungan industri.

1.2 Rumusan Masalah

Rumusan Masalah pada penelitian ini adalah sebagai berikut :

1. Bagaimana cara menerapkan enksripsi ECC pada komunikasi data sinyal kontrol PID pada sistem *online controller*?
2. Bagaimana pengaruh enkripsi ECC terhadap parameter sistem respons transien, yaitu *delay time, rise time, peak time, settling time,* dan *maximum overshoot*, serta *steady state error* dalam pengontrolan posisi motor DC?

1.3 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut :

1. Menerapkan enksripsi ECC pada komunikasi data sinyal kontrol PID beserta *feedback*-nya pada *online controller*
2. Menganalisis pengaruh enkripsi ECC terhadap parameter respons transien, yaitu *delay time, rise time, peak time, settling time*, dan *maximum overshoot*, serta *steady state error* dalam pengontrolan posisi motor DC.

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat berupa :

1. Meningkatkan keamanan komunikasi data dalam sistem kendali *online*.
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 hanya menggunakan metode enkripsi ECC sebagai teknik pengamanan data.
2. Sistem kontrol terbatas pada pengontrol PID dalam bentuk *online controller*.
3. Penelitian difokuskan pada pengendalian posisi sudut motor DC menggunakan algoritma pengendali PID berbasis komunikasi *online*.
4. Sistem kendali dikembangkan menggunakan protokol komunikasi TCP dan UDP tanpa mempertimbangkan protokol lain.

5. Evaluasi performa sistem hanya mencakup parameter respons transien yaitu *delay time, rise time, peak time, settling time*, dan *maximum overshoot,* serta analisis *steady state error.*

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.