

BAB I PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi digital telah menyebabkan sistem kontrol industri semakin terhubung dengan jaringan, namun hal ini juga meningkatkan risiko terhadap serangan siber. Sistem-sistem tersebut menjadi lebih rentan terhadap gangguan yang bersifat digital, dan bahkan dapat berdampak langsung pada fisik dan operasional. Salah satu contoh signifikan terjadi pada tahun 2000 di Australia, ketika sistem pengendali limbah berbasis SCADA milik Maroochy Shire Council diretas oleh mantan karyawan melalui perangkat radio ilegal. Aksi ini mengakibatkan gangguan sistem yang menyebabkan tumpahan limbah mentah ke taman, sungai, dan lingkungan sekitar sehingga memicu pencemaran dan bau tidak sedap di area pemukiman. Peristiwa ini menjadi bukti bahwa keamanan sistem kontrol merupakan elemen krusial, terutama bagi industri yang sangat bergantung pada kontrol otomatis demi efisiensi dan keselamatan [1].

Salah satu jenis serangan siber yang sering ditemukan pada sistem berbasis jaringan adalah *eavesdropping*, yaitu teknik penyadapan di mana pelaku mencuri informasi yang sedang ditransmisikan melalui jaringan komunikasi korban [2]. Penyerang biasanya menggunakan perangkat lunak *packet sniffer* untuk menangkap lalu lintas data, dan aplikasi ini tersedia secara bebas di internet, sehingga memperbesar peluang eksploitasi jika tidak ada mekanisme perlindungan yang tepat. Data sensitif seperti perintah kendali, informasi teknis, atau kredensial dapat diakses tanpa terdeteksi. Oleh karena itu, penggunaan enkripsi data menjadi salah satu langkah yang dianjurkan untuk menjaga kerahasiaan dan integritas komunikasi dalam sistem kontrol industri [3].

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

Pada tahun 2023, Kogiso melanjutkan penelitiannya dengan mengembangkan *Keyed-Homomorphic Public Key Encryption* (KH-PKE) yang mampu 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 kelemahan 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) guna mengoptimalkan daya transmisi

sensor agar komunikasi tetap aman meskipun berada dalam kondisi rawan penyadapan dan jamming [6]. Akan tetapi, sebagian besar penelitian tersebut masih terbatas pada skala besar atau simulasi dan belum banyak menyentuh implementasi langsung pada sistem kendali berbasis mikrokontroler yang memiliki keterbatasan sumber daya.

Salah satu metode enkripsi yang sederhana namun cukup efektif adalah operasi logika *Exclusive-OR* (XOR). Algoritma ini bekerja dengan cepat dan efisien dalam mengacak data, menjadikannya cocok untuk aplikasi yang memerlukan latensi rendah dan keterbatasan sumber daya komputasi [7]. Meskipun tidak sekuat enkripsi asimetris seperti RSA, metode XOR banyak digunakan pada sistem berbasis mikrokontroler karena kecepatan dan efisiensi energinya.

Penggunaan algoritma XOR dalam sistem komunikasi melalui jaringan telah diuji oleh Salma et al. pada tahun 2022, yang menerapkan enkripsi ini pada komunikasi sensor suhu. Hasil penelitian menunjukkan bahwa metode XOR mampu menjaga efisiensi konsumsi daya, menjadikannya pilihan tepat untuk sistem yang memerlukan pengolahan data secara real-time dan hemat energi [8]. Namun, implementasi enkripsi XOR dalam sistem kendali yang lebih kompleks, seperti kendali PID pada motor DC, belum banyak diteliti. Sistem kontrol PID menuntut presisi tinggi dan waktu respons yang cepat, sehingga penting untuk mengevaluasi sejauh mana enkripsi XOR dapat diterapkan tanpa mengorbankan performa kendali.

Penggunaan kontrol PID dalam penelitian ini didasarkan pada kenyataan bahwa algoritma PID merupakan bentuk umpan balik yang paling dominan digunakan dalam sistem kontrol industri. Lebih dari 90% loop kontrol yang digunakan di dunia industri menerapkan kendali PID, karena algoritma ini menawarkan keseimbangan antara kesederhanaan implementasi, kemudahan tuning, serta kemampuan menjaga kestabilan dan akurasi sistem [9]. Oleh karena itu, penelitian ini berfokus pada penerapan XOR dalam sistem kontrol motor menggunakan kendali PID, serta menganalisis dampaknya terhadap respons transien sistem.

Penelitian ini dikembangkan untuk menjembatani kesenjangan antara kebutuhan 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 *steady state error*. Dengan demikian, diharapkan penelitian ini dapat memberikan pemahaman yang lebih dalam mengenai dampak penerapan enkripsi ringan terhadap kinerja sistem kendali pada *online controller*, sekaligus menjadi acuan dalam pengembangan sistem kendali yang aman dan efisien untuk dipakai di lingkungan industri.

1.2 Rumusan Masalah

Rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Bagaimana cara menerapkan enkripsi XOR pada komunikasi data sinyal kontrol PID pada sistem *online controller*?
2. Bagaimana pengaruh enkripsi XOR pada unjuk kerja pengontrolan posisi motor DC?
3. Bagaimana pengaruh enkripsi XOR terhadap parameter respons transien system, 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 enkripsi XOR pada komunikasi data sinyal kontrol PID pada *online controller*.
2. Menganalisa pengaruh Enkripsi XOR 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 pada sistem kendali jaringan.
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 fokus pada metode enkripsi XOR 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 *online PID controller*.
4. Sistem kendali dikembangkan menggunakan protokol komunikasi TCP dan UDP tanpa mempertimbangkan protokol lain.
5. Evaluasi performa sistem mencakup parameter respons transien yaitu *delay time*, *rise time*, *peak time*, *settling time*, dan *maximum overshoot*, serta analisis *steady state error*.
6. Waktu tunak yang digunakan pada penelitian ini yaitu $\pm 2\%$.

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.

