BAB I
PENDAHULUAN

1.1 Latar Belakang

Transformasi industri menuju era *Industry 4.0* dan *Internet of Things* (IoT) telah mengubah paradigma dari sistem kendali konvensional menjadi *Networked Control Systems* (NCS). Pada sistem NCS, proses pertukaran data antara sensor, pengendali (*controller*), dan aktuator dilakukan melalui jaringan komunikasi digital, sehingga tidak lagi bergantung pada koneksi kabel secara langsung (*point-to-point*) [1]. Pendekatan ini memberikan berbagai keunggulan seperti fleksibilitas sistem, efisiensi infrastruktur, serta kemampuan untuk melakukan monitoring dan pengendalian secara jarak jauh.

Namun demikian, penggunaan jaringan komunikasi juga menimbulkan tantangan baru, terutama dari sisi keamanan sistem. Studi menunjukkan bahwa sistem kendali berbasis jaringan rentan terhadap berbagai serangan siber, seperti *Man-in-the-Middle* (MitM) dan *false data injection*, yang dapat mengganggu integritas data dan menurunkan performa sistem secara signifikan [2]. Oleh karena itu, penerapan mekanisme keamanan berbasis kriptografi menjadi sangat penting untuk menjamin kerahasiaan (*confidentiality*) dan integritas (*integrity*) data pada sistem kendali berbasis jaringan.

Salah satu algoritma kriptografi yang banyak digunakan adalah *Advanced Encryption Standard* (AES), salah satunya dalam mode operasi *Counter* (CTR). Mode AES-CTR memiliki keunggulan dalam hal kecepatan dan efisiensi karena menggunakan pendekatan *stream cipher*, sehingga memungkinkan proses enkripsi dan dekripsi dilakukan secara paralel dengan latensi yang relatif rendah [3].

Meskipun demikian, integrasi mekanisme enkripsi ke dalam sistem kendali tertutup (*closed-loop control system*) tidak terlepas dari konsekuensi berupa penambahan beban komputasi (*computational overhead*). Proses enkripsi dan dekripsi yang dilakukan secara real-time dapat menimbulkan waktu tunda (*delay*) pada jalur komunikasi [4]. Dalam sistem NCS, delay tersebut dapat bersifat variabel (*time-varying delay*) dan menjadi salah satu faktor utama yang menyebabkan penurunan performa sistem, seperti meningkatnya *overshoot*, memperlambat *settling time*, serta berpotensi menyebabkan ketidakstabilan sistem [5].

Berdasarkan tinjauan literatur, sebagian besar penelitian yang ada masih berfokus pada analisis pengaruh enkripsi terhadap sistem kendali tanpa mempertimbangkan strategi kompensasi yang optimal [6]. Di sisi lain, terdapat pula penelitian yang membahas desain pengendali pada NCS dengan mempertimbangkan delay jaringan, namun belum mengintegrasikan aspek keamanan berbasis enkripsi ke dalam sistem [7]. Hal ini menunjukkan bahwa kajian yang menggabungkan antara keamanan sistem, pengaruh delay akibat enkripsi, serta strategi pengendalian yang adaptif masih relatif terbatas.

Dalam praktiknya, pengendali *Proportional-Integral-Derivative* (PID) masih menjadi pilihan utama dalam industri karena strukturnya yang sederhana dan mudah

diimplementasikan. Namun, parameter PID yang dirancang pada kondisi tanpa delay sering kali tidak lagi optimal ketika sistem mengalami tambahan delay akibat proses enkripsi. Oleh karena itu, diperlukan proses penentuan ulang (*retuning*) parameter PID, khususnya secara *online*, agar sistem tetap mampu memberikan performa yang stabil dan responsif meskipun terdapat gangguan delay [8].

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menentukan parameter PID controller secara *online* pada sistem NCS yang menerapkan enkripsi AES-CTR dalam pengendalian posisi sudut motor DC. Selain itu, penelitian ini juga menganalisis pengaruh penerapan enkripsi terhadap karakteristik respon transien sistem, seperti *rise time*, *settling time*, *overshoot*, dan *steady-state error*. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan sistem kendali yang tidak hanya aman dari sisi komunikasi data, tetapi juga tetap optimal dari sisi performa kendali.

1.2 Rumusan Masalah

Rumusan masalah dari penelitian ini adalah sebagai berikut:

1. Bagaimana pengaruh penerapan algoritma enkripsi AES-CTR pada sistem *Networked Control System* (NCS) berbasis Online PID *controller* terhadap karakteristik respons transien sistem, khususnya pada parameter *delay time*, *rise time*, *peak time*, *settling time*, *maximum overshoot*, serta *steady-state error*?
2. Bagaimana menentukan kembali parameter PID yang optimal untuk mengkompensasi penurunan performa akibat beban komputasi enkripsi, sehingga menghasilkan respons transien yang mendekati karakteristik sistem kendali langsung (konvensional)?

1.3 Tujuan

Tujuan dari penelitian ini adalah sebagai berikut:

1. Menganalisis pengaruh penerapan enkripsi AES-CTR pada sistem NCS Online PID kontroller terhadap parameter respons transien sistem, yang meliputi *delay time*, *rise time*, *peak time*, *settling time*, *maximum overshoot*, serta *steady-state error*.
2. Menentukan kembali parameter PID untuk menanggulangi penurunan performa akibat beban enkripsi, guna menghasilkan respon transien yang mendekati karakteristik sistem kendali langsung (konvensional).

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat berupa:

1. Memberikan bukti empiris mengenai seberapa besar dampak beban komputasi dari penerapan enkripsi AES-CTR terhadap siklus eksekusi sistem kendali PID secara *online*, serta pengaruhnya dalam mendegradasi respon transien motor DC.
2. Menghasilkan parameter PID hasil optimasi yang terbukti mampu memulihkan kestabilan sistem kendali akibat gangguan latensi enkripsi.

3. Menjadi acuan teknis bagi industri untuk mengimplementasikan keamanan pada sistem kendali warisan (*legacy systems*) dengan sumber daya terbatas, cukup melalui penentuan ulang kontroler tanpa perlu penggantian perangkat keras.

1.5 Batasan Masalah

Penelitian ini memiliki batasan masalah sebagai berikut:

1. Algoritma kriptografi yang diimplementasikan dibatasi pada AES-CTR (blok 128-bit) sesuai standar RFC 3686, tanpa melakukan modifikasi pada struktur internal algoritma maupun pengujian ketahanan terhadap serangan siber (*cryptanalysis*).
2. Sistem fisis yang dikendalikan adalah posisi sudut Motor DC (bukan kecepatan), menggunakan umpan balik (*feedback*) posisi.
3. Metode optimasi parameter PID yang dilakukan berbasis pada pendekatan Heuristik (*Trial and Error*) atau penentuan eksperimental, yang berfokus pada kompensasi respon terhadap beban komputasi.
4. Pengujian dilakukan pada protokol lapisan transpor TCP (*Transmission Control Protocol*) dan UDP (*User Datagram Protocol*) dalam jaringan lokal (*Local Area Network*).
5. Analisis kinerja dibatasi pada perbandingan parameter respons transien (*delay time, rise time, settling time, overshoot*) dan error steady-state antara kondisi tanpa enkripsi dan terenkripsi.

1.6 Sistematika Penulisan

Penulisan tugas akhir ini disusun secara sistematis untuk memudahkan pemahaman terhadap alur penelitian yang dilakukan. Adapun sistematika penulisan tugas akhir ini terdiri dari lima bab, yaitu sebagai berikut:

BAB I Pendahuluan

Bab ini berisi uraian mengenai latar belakang penelitian, perumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian, serta sistematika penulisan tugas akhir.

BAB II Tinjauan Pustaka

Bab ini memuat landasan teori dan kajian pustaka yang berkaitan dengan topik penelitian sebagai dasar dalam mendukung pelaksanaan dan pembahasan penelitian.

BAB III Metodologi Penelitian

Bab ini menjelaskan metode penelitian yang digunakan, meliputi tahapan penelitian, perancangan sistem, prosedur pengujian, serta teknik pengumpulan dan pengolahan data.

BAB IV Hasil dan Pembahasan

Bab ini menyajikan hasil penelitian yang telah diperoleh beserta pembahasan dan analisis terhadap data yang dihasilkan berdasarkan metode yang digunakan.

BAB V Kesimpulan dan Saran

Bab ini berisi kesimpulan yang diperoleh dari hasil penelitian serta saran yang dapat digunakan sebagai bahan pertimbangan untuk penelitian selanjutnya.