BAB I PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi seperti *Industrial Internet of Things* (IIoT), sistem kendali otomatis, dan jaringan generasi kelima (5G) telah mempercepat transformasi digital dalam industri. Sistem kontrol industri (*Industrial Control Systems*/ICS) yang sebelumnya bersifat tertutup kini terhubung dengan jaringan terbuka, meningkatkan risiko serangan siber seperti *eavesdropping*, data *injection*, dan *sabotage* digital. Serangan ini tidak hanya menyebabkan gangguan operasional dan kerugian finansial, tetapi juga mengancam keselamatan manusia karena hilangnya fungsi keselamatan (*safety functions*) pada mesin [1]. Kasprzyczak et al. menekankan bahwa tanpa proteksi yang memadai, sistem kontrol mesin dapat menjadi titik lemah utama yang dimanfaatkan penyerang untuk mengakses dan memodifikasi parameter kritis pada perangkat lunak maupun perangkat keras [1].

Semakin kompleksnya struktur komunikasi di dalam ICS, pendekatan keamanan siber yang sistematis dan otomatis menjadi sangat penting. Altaleb et al. mengungkapkan bahwa integrasi teknologi 5G dan komponen cerdas (*smart devices*) dalam sistem kontrol industri menambah *attack surface* yang perlu dilindungi [2]. Untuk menjaga kerahasiaan dan integritas data komunikasi, salah satu strategi utama adalah penerapan enkripsi ringan namun kuat, yang mampu melindungi transmisi data real-time tanpa membebani sistem secara signifikan. Oleh karena itu, pendekatan terintegrasi yang mencakup manajemen risiko, kontrol keamanan jaringan, pemantauan lalu lintas, dan mitigasi ancaman juga diperlukan untuk memastikan ketahanan sistem kontrol industri terhadap berbagai vektor serangan siber [3].

Selain itu, pada sistem kendali berbasis jaringan, faktor keterlambatan transmisi data (delay) akibat jenis protokol komunikasi seperti TCP (*Transmission Control Protocol*) maupun UDP (*User Datagram Protocol*) juga dapat mempengaruhi performa kendali. TCP adalah protokol yang sering digunakan untuk komunikasi yang memerlukan keandalan, sedangkan UDP lebih cocok untuk aplikasi yang memerlukan kecepatan pengiriman data. Feriyonika et al. dalam penelitiannya menunjukkan bahwa meskipun TCP memiliki *reliability* yang tinggi, namun menghasilkan waktu *settling time* dan *rise time* yang lebih lambat dibandingkan UDP pada implementasi *Networked Control System* (NCS) berbasis PID *multiloop* [4]. Hal ini menunjukkan bahwa pemilihan protokol juga berperan penting dalam menjaga stabilitas dan kecepatan sistem kendali waktu nyata.

Penelitian lain oleh Bisoyi & Pati menunjukkan implementasi kendali PID berbasis TCP/IP menggunakan LabVIEW, yang menyoroti pentingnya kestabilan komunikasi jaringan dalam sistem kendali jarak jauh. Penelitian ini juga menyebutkan bahwa protokol TCP dapat menghadapi kerentanan terhadap

gangguan komunikasi dan latensi yang berdampak pada performa kontrol waktu nyata [5].

Berbagai studi sebelumnya dalam bidang keamanan komunikasi digital telah menerapkan algoritma kriptografi seperti RSA, AES-GCM, dan HMAC-SHA256. RSA, sebagai algoritma kriptografi asimetris, dikenal memiliki kompleksitas komputasi yang tinggi dan membutuhkan waktu enkripsi yang lama, sehingga kurang sesuai untuk sistem tertanam yang membutuhkan efisiensi waktu dan konsumsi daya rendah. Sementara itu, AES-GCM dan HMAC-SHA256 yang termasuk dalam algoritma kriptografi simetris relatif lebih ringan, namun AES-GCM cenderung mengandalkan dukungan perangkat keras untuk mencapai performa optimal. Dalam konteks perangkat dengan sumber daya terbatas seperti IoT, Susanti et al. menunjukkan bahwa algoritma ChaCha20-Poly1305 unggul dari sisi kecepatan enkripsi, terutama pada ukuran data besar, dan menunjukkan efisiensi yang lebih baik dibandingkan AES-GCM dalam skenario tanpa akselerasi perangkat keras [6].

Di sisi lain, Daniel J. Bernstein sebagai perancang ChaCha20 menjelaskan bahwa algoritma ini dibangun dari struktur ARX (*Addition-Rotation-XOR*) dengan tingkat difusi yang lebih tinggi dibandingkan Salsa20, serta dapat bekerja secara efisien tanpa ketergantungan terhadap akselerasi perangkat keras. Dengan kata lain, ChaCha20 menawarkan performa tinggi yang konsisten pada sistem *real-time* dan tertanam, bahkan mampu mengungguli AES pada beberapa platform prosesor [7].

Selain keunggulannya dalam performa, ChaCha20 juga menawarkan keamanan yang kuat. Berbagai analisis keamanan yang dilakukan terhadapnya menunjukkan bahwa algoritma ini tangguh terhadap berbagai jenis serangan. Misalnya, analisis diferensial, kriptanalisis linear, dan serangan aljabar tidak ditemukan efisien untuk memecahkan ChaCha20. Meskipun serangan *time memory* data *trade off* dan *side-channel* secara teoritis dapat diterapkan, serangan-serangan tersebut dapat diatasi dengan penanggulangan praktis yang efektif [8]. Studi oleh Barbero et al. juga menganalisis kerentanan ChaCha20 terhadap *rotational cryptanalysis* atau kriptanalisis rotasional. Penelitian tersebut menunjukkan bahwa ChaCha20 secara eksplisit dirancang untuk mencegah serangan semacam ini dengan menggunakan konstanta non-simetris di awal permutasi. Walaupun demikian, analisis yang lebih mendalam pada fungsi *quarter-round* ChaCha20 menunjukkan adanya sedikit penyimpangan dari perilaku permutasi acak, di mana probabilitas propagasi pasangan *rotational-XOR* adalah sekitar $2^{-251.7857}$, yang sedikit lebih besar dari probabilitas untuk permutasi acak yaitu 2^{-256}. Namun, secara keseluruhan, ChaCha20 tetap dianggap aman dan tidak menunjukkan kelemahan yang signifikan terhadap serangan-serangan ini [9].

Meskipun performa ChaCha20 telah banyak diuji dalam konteks sistem tertanam dan keamanan jaringan, penelitian yang membahas pengaruh penerapannya secara langsung terhadap dinamika sistem kendali tertutup, seperti pengendali PID nirkabel, masih sangat terbatas. Penelitian oleh Udayakumar lebih

berfokus pada penerapan algoritma XChaCha20 sebagai ekstensi dari ChaCha20 pada sistem penyimpanan *cloud* tingkat *file-system* dan menunjukkan keunggulan dalam aspek efisiensi waktu enkripsi, entropi, dan sensitivitas terhadap gangguan dibanding AES [10]. Namun, studi tersebut tidak meneliti dampaknya terhadap parameter performa sistem kendali seperti *error steady-state*, waktu naik, atau kestabilan kontrol posisi motor.

Penelitian lokal menunjukkan implementasi kendali PID berbasis komunikasi nirkabel dengan menggunakan ESP8266 dan motor DC untuk pengaturan kelembaban tanah, namun belum mengintegrasikan aspek enkripsi pada jalur komunikasinya [11]. Hal ini menunjukkan bahwa pengamanan data dalam sistem kendali nirkabel masih merupakan aspek yang terbuka untuk diteliti lebih lanjut

Penelitian sebelumnya mengusulkan metode enkripsi video ringan dengan menggabungkan algoritma stream cipher ChaCha20 dan hybrid chaotic map untuk meningkatkan keamanan data visual pada perangkat dengan sumber daya terbatas seperti kamera IP dan sensor nirkabel. Pendekatan ini terbukti mencapai efisiensi tinggi dalam waktu enkripsi, entropi, dan daya tahan terhadap serangan statistik, sambil tetap mempertahankan kecepatan pemrosesan yang sesuai untuk aplikasi real-time[12]. Meskipun studi ini menunjukkan keunggulan dari sisi keamanan dan performa kriptografi, fokus utamanya berada pada pengamanan data video, bukan pada sistem kendali tertutup seperti pengendali PID nirkabel. Oleh karena itu, diperlukan kajian lebih lanjut untuk mengevaluasi sejauh mana penerapan algoritma ChaCha20 dalam sistem kendali waktu nyata berdampak terhadap karakteristik respon sistem seperti *rise time*, *settling time*, atau kestabilan sudut posisi motor DC.

Oleh karena itu, terdapat celah penelitian penting yang perlu dijembatani, yaitu bagaimana algoritma ChaCha20 mempengaruhi performa sistem kendali tertutup seperti pengendali PID nirkabel berbasis komunikasi TCP maupun UDP. Kebutuhan akan sistem kendali nirkabel yang andal dan aman terhadap potensi penyadapan data semakin mendesak, terutama dalam penerapan industri dan otomasi yang mengandalkan komunikasi berbasis jaringan.

Penelitian ini diarahkan untuk menganalisis secara komprehensif dampak penerapan algoritma ChaCha20 dalam mengamankan komunikasi data pada sistem kendali motor DC berbasis jaringan nirkabel. Fokus utama penelitian ini adalah pada evaluasi performa sistem kendali PID motor DC yang berkomunikasi melalui dua jenis protokol, yaitu TCP dan UDP, baik dalam kondisi tanpa enkripsi maupun setelah dienkripsi menggunakan algoritma ChaCha20. Evaluasi dilakukan berdasarkan karakteristik respon transien sistem seperti *Delay time*, *Rise time*, *Peak time*, *Settling time*, dan *Maximum Overshoot*, serta parameter *Error Steady State*. Pendekatan ini terinspirasi dari pentingnya menjaga integritas dan kerahasiaan data dalam sistem kontrol berbasis jaringan nirkabel yang rentan terhadap serangan seperti *eavesdropping* dan *man-in-the-middle attack*. Dengan demikian, penelitian

ini tidak hanya menguji sejauh mana ChaCha20 mampu menjaga keamanan data, tetapi juga menilai dampaknya terhadap kestabilan dan kecepatan respons sistem kendali.

1.2 Rumusan Masalah

Berdasarkan identifikasi masalah yang telah diuraikan, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana cara menerapkan enkripsi ChaCha20 pada protokol komunikasi UDP dan TCP data sinyal kontrol PID pada sistem online controller?
2. Bagaimana pengaruh enkripsi ChaCha20 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

Tujuan yang ingin dicapai dari penelitian tugas akhir ini adalah:

1. Menerapkan enkripsi ChaCha20 pada protokol komunikasi UDP dan TCP data sinyal kontrol PID pada *online controller*.
2. Menganalisa pengaruh Enkripsi Chacha20 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

Manfaat yang ingin diperoleh dari penelitian tugas akhir ini adalah:

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

Batasan masalah diberikan agar pembahasan dari hasil yang didapatkan lebih terarah. Batasan masalah dari penelitian ini adalah:

1. Penelitian ini terbatas pada penggunaan algoritma enkripsi ChaCha20 sebagai satu-satunya teknik pengamanan data.
2. Sistem kontrol yang dikembangkan dalam penelitian ini terbatas pada pengontrol PID yang diimplementasikan sebagai *online controller*.
3. Penelitian difokuskan pada pengendalian posisi sudut motor DC menggunakan algoritma *Online* pengendali PID.
4. Sistem kendali dikembangkan menggunakan protokol komunikasi TCP dan UDP tanpa mempertimbangkan protokol lain.

5. Evaluasi performa sistem dalam penelitian ini terbatas pada analisis respons transien, yang mencakup parameter *delay time*, *rise time*, *peak time*, *settling time*, dan *maximum overshoot*, serta analisis *steady state error*.

1.6 Sistematika Penulisan

Sistematika penulisan laporan penelitian disusun sebagai berikut:

BAB I Pendahuluan

Bab I dari penelitian ini menyajikan beberapa poin kunci yang meliputi: latar belakang penelitian, rumusan masalah, tujuan penelitian, batasan masalah, dan sistematika penulisan.

BAB II Tinjauan Pustaka

Bab II dari penelitian ini memuat berbagai teori pendukung yang menjadi landasan konseptual dalam penyelesaian masalah yang dibahas dalam tugas akhir ini.

BAB III Metode Penelitian

Bab ini menyajikan metodologi penelitian yang digunakan. Isinya mencakup diagram alir penelitian, prinsip kerja, bahan yang digunakan, perancangan jaringan, dan teknik pengujian yang dilakukan.

BAB IV Hasil dan Analisa

Bab ini menyajikan hasil dan pembahasan dari penelitian yang telah dilakukan dalam tugas akhir ini.

BAB V Kesimpulan dan Saran

Bab ini memuat kesimpulan dari penelitian yang telah dilakukan serta saran yang dapat menjadi acuan untuk penelitian selanjutnya.

UNIVERSITAS ANDALAS
UNTUK KEDJAJAAN BANGSA