BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil implementasi dan pengujian sistem yang dilakukan, serta analisis data yang diperoleh, maka dapat disimpulkan hal-hal berikut:

1. Implementasi sistem kendali PID nirkabel untuk pengaturan posisi sudut motor DC berbasis enkripsi AES mode Counter (AES-CTR) telah berhasil direalisasikan. Sistem ini terdiri dari dua unit komputer yang terhubung melalui jaringan nirkabel menggunakan protokol TCP dan UDP. Unit pertama berperan sebagai pengendali PID, sedangkan unit kedua menggerakkan motor DC dengan menerima sinyal PWM dari modul LabJack T7 serta mengirimkan umpan balik posisi dari encoder magnetik. Antarmuka pengguna dikembangkan menggunakan HTML, CSS, dan JavaScript, sementara backend memanfaatkan Node.js dan Python untuk menjalankan algoritma kendali PID serta proses enkripsi dan dekripsi dengan AES-CTR.
2. Hasil pengujian komunikasi TCP menunjukkan bahwa penggunaan enkripsi AES mode Counter (AES-CTR) mempengaruhi kinerja sistem, khususnya pada parameter waktu respons. Delay time dan settling time tercatat lebih tinggi dibandingkan kondisi tanpa enkripsi. Sebagai ilustrasi, pada setpoint 360°, delay time meningkat dari 0,994 detik menjadi 1,101 detik, sedangkan settling time naik dari 1,930 detik menjadi 1,976 detik. Penurunan kinerja ini dipicu oleh *overhead* komputasi yang timbul dari proses enkripsi-dekripsi AES-CTR, serta karakteristik protokol TCP yang mengandalkan mekanisme *three-way handshake*, konfirmasi penerimaan data, dan pengiriman ulang paket untuk menjamin keandalan komunikasi. Kombinasi faktor tersebut mengakibatkan waktu tanggap sistem menjadi lebih lambat dibandingkan saat tanpa enkripsi..
3. Pengujian dengan protokol UDP menunjukkan bahwa sistem memiliki performa yang lebih stabil dan mendekati karakteristik pengujian offline. Sebagai contoh, pada setpoint 90°, settling time meningkat dari 0,675 detik (offline) menjadi 0,799 detik (tanpa enkripsi). Penambahan enkripsi AES-CTR pada UDP hanya menimbulkan peningkatan delay time yang relatif kecil, seperti pada setpoint 180° di mana delay bertambah dari 0,279 detik menjadi 0,311 detik, tanpa memberikan pengaruh berarti terhadap settling time maupun *maximum overshoot*..
4. Karakter UDP yang bersifat connectionless menjadikan latensi jaringan lebih rendah karena tidak memerlukan proses 3-way handshake sebagaimana pada TCP. Berdasarkan data pengujian, protokol UDP secara rata-rata mampu

menurunkan delay time hingga 48% dan settling time sebesar 26% dibandingkan TCP.

5. Penerapan enkripsi AES-CTR terbukti mampu mengubah plaintext menjadi ciphertext dengan tingkat efisiensi yang masih dapat diterima oleh sistem. Dari hasil pengujian, penambahan latensi akibat enkripsi ini hanya berkisar antara 6% hingga 17%, dengan rata-rata sekitar 11% terhadap total delay time sistem. Oleh karena itu, kombinasi protokol UDP dengan enkripsi AES-CTR dapat menjadi alternatif yang menjanjikan bagi sistem kendali real-time yang menuntut kecepatan tinggi sekaligus menjamin keamanan transmisi data
6. Berdasarkan hasil perbandingan antara enkripsi XOR dan AES-CTR, diperoleh bahwa sistem dengan enkripsi XOR secara umum memberikan respons yang lebih cepat dengan nilai delay yang lebih rendah dibandingkan sistem yang menggunakan enkripsi AES-CTR. Namun, pada beberapa titik setpoint tertentu, enkripsi XOR justru menghasilkan delay yang lebih tinggi. Fenomena ini disinyalir disebabkan oleh perbedaan parameter PID yang digunakan dalam masing-masing skenario pengujian, yang secara tidak langsung mempengaruhi durasi proses enkripsi. Meskipun demikian, AES-CTR tetap unggul dari segi aspek keamanan, karena menawarkan tingkat proteksi data yang lebih tinggi dibandingkan enkripsi XOR.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, penulis mengajukan beberapa saran untuk pengembangan studi di masa mendatang.

1. Disarankan untuk mengeksplorasi penggunaan algoritma enkripsi lain dengan tingkat keamanan lebih tinggi guna menilai dampaknya terhadap kinerja sistem kendali.
2. Penelitian selanjutnya perlu difokuskan pada upaya perlindungan sistem kendali industri dari beragam jenis serangan siber, bukan hanya serangan penyadapan.
3. Penelitian berikutnya disarankan menambahkan beban kerja pada kontroler guna menguji ketahanan dan keandalan sistem kendali online terenkripsi dalam kondisi beban tinggi atau skenario operasional yang lebih kompleks..