BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil implementasi, pengujian sistem secara menyeluruh, serta analisis mendalam terhadap parameter respons transien sistem yang telah dipaparkan pada bab sebelumnya, maka dapat diambil kesimpulan utama yang membuktikan ketercapaian tujuan penelitian ini sebagai berikut:

1. Penerapan enkripsi algoritma AES terhadap parameter respons transien sistem NCS Online PID controller terbukti memberikan pengaruh terhadap karakteristik respons sistem akibat adanya tambahan beban komputasi proses enkripsi dan dekripsi selama komunikasi jaringan. Secara umum, implementasi AES pada protokol komunikasi UDP menyebabkan perubahan pada parameter berbasis waktu, yaitu *delay time*, *rise time*, *peak time*, dan *settling time*, yang menunjukkan adanya peningkatan waktu respons dibandingkan sistem *direct* (tanpa jaringan). Meskipun demikian, penerapan AES tetap mampu mempertahankan kualitas respons sistem dengan nilai *maximum overshoot* yang relatif kecil serta *steady-state error* yang tetap rendah pada seluruh kondisi pengujian. Hal ini menunjukkan bahwa penambahan mekanisme keamanan melalui enkripsi AES tidak mengurangi akurasi posisi akhir sistem, melainkan hanya memberikan konsekuensi berupa tambahan waktu respons akibat proses komputasi kriptografi..

2. Penentuan kembali parameter PID (online retuning) terbukti dapat mendekati dan mengatasi penurunan performa sistem yang disebabkan oleh beban komputasi enkripsi AES-CTR dengan tetap mendekati nilai akhir karakteristik nilai langsung (konvensional). Melalui proses penentuan ulang diperoleh parameter PID , yaitu Kp = 19,218; Ki = 6,1278; dan Kd = 2,8311, dibandingkan parameter awal. Parameter hasil penentuan ulang mampu mengerahkan karakteristik respons transien pada seluruh pengujian setpoint. Pada setpoint 360°, terjadi penurunan *delay time* menjadi 0,540 detik, *rise time* menjadi 1,347 detik, *peak time* menjadi 1,949 detik, dan *settling time* menjadi 1,842 detik, disertai penurunan *maximum overshoot* menjadi 0,782% serta *steady-state error* menjadi 0,320°. Perbaikan serupa juga diperoleh pada pengujian setpoint 180° dan 90°, di mana parameter hasil penentuan ulang secara umum dapat mendekati nilai waktu respons, *peak time* dan *settling time*, dengan pengujian direct, serta mempertahankan akurasi posisi akhir sistem. Meskipun pada beberapa kondisi nilai *maximum overshoot* sedikit meningkat

dibandingkan parameter awal, nilainya tetap jauh lebih rendah dibandingkan kondisi *direct*, sehingga secara keseluruhan proses *online retuning* berhasil menghasilkan kompromi yang lebih baik antara kecepatan respons, kestabilan sistem, dan akurasi. Dengan demikian, sistem NCS berbasis komunikasi UDP terenkripsi menggunakan algoritma AES-CTR yang dipadukan dengan proses *online retuning* mampu menghasilkan karakteristik respons transien yang mendekati sistem kendali langsung (konvensional) sekaligus tetap memenuhi aspek keamanan komunikasi data.

5.2 Saran

Berdasarkan rangkaian proses pembuatan, pengujian, serta analisis pada penelitian ini, penulis memberikan beberapa saran dan rekomendasi untuk pengembangan penelitian di masa mendatang:

1. Penelitian selanjutnya disarankan untuk melakukan pengujian pada kondisi jaringan yang lebih bervariasi, seperti penambahan delay, packet loss, jitter, maupun gangguan komunikasi lainnya. Pengujian tersebut diperlukan untuk mengetahui tingkat ketahanan sistem NCS yang menggunakan enkripsi AES-CTR terhadap kondisi jaringan yang mendekati implementasi nyata.

2. Penelitian selanjutnya disarankan menggunakan perangkat keras dengan kemampuan komputasi yang lebih tinggi atau memanfaatkan mikrokontroler yang memiliki fitur Programmable Real-Time Unit (PRU) maupun akselerasi perangkat keras (*hardware acceleration*) untuk algoritma AES. Pendekatan ini diharapkan mampu mengurangi waktu komputasi proses enkripsi dan dekripsi sehingga latensi komunikasi dapat ditekan dan karakteristik respons transien sistem semakin mendekati sistem kendali langsung (*direct control*).

3. Pengembangan aspek keamanan sistem dapat dilakukan dengan mengevaluasi implementasi AES-CTR terhadap berbagai skenario serangan siber pada sistem Networked Control System (NCS), seperti Man-in-the-Middle (MitM), Replay Attack, Denial-of-Service (DoS), maupun serangan modifikasi paket (*packet tampering*). Dengan demikian, penelitian selanjutnya tidak hanya mengevaluasi performa respons transien, tetapi juga mengukur tingkat ketahanan sistem terhadap ancaman keamanan komunikasi.

4. Penelitian selanjutnya dapat mengembangkan metode penentuan parameter PID yang lebih adaptif, misalnya dengan menerapkan algoritma optimasi atau metode *adaptive control* sehingga parameter pengendali dapat menyesuaikan perubahan kondisi jaringan maupun perubahan beban komputasi secara otomatis tanpa memerlukan proses penentuan ulang secara manual.

5. Penelitian berikutnya juga dapat membandingkan performa algoritma AES-CTR dengan mode operasi AES lainnya maupun algoritma kriptografi yang berbeda, sehingga dapat diperoleh metode pengamanan komunikasi yang memberikan kompromi terbaik antara tingkat keamanan, beban komputasi, dan performa sistem kendali.