BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi digital dan sistem kendali otomatis telah membawa perubahan signifikan dalam berbagai aspek kehidupan manusia, khususnya di bidang industri, otomasi, dan robotika. Salah satu teknologi yang banyak digunakan adalah sistem kendali berbasis motor DC. Motor DC memiliki karakteristik pengendalian yang baik dan responsif sehingga sering digunakan dalam aplikasi yang memerlukan kendali kecepatan dan posisi yang presisi[1] . Untuk meningkatkan performa sistem, umumnya diterapkan metode pengendalian seperti PID (*Proportional-Integral-Derivative*) yang terkenal karena kesederhanaan dan efektivitasnya dalam mengendalikan sistem linier[2] .

Seiring dengan semakin kompleksnya sistem kendali, kebutuhan akan komunikasi *online* menjadi semakin penting, terutama dalam lingkungan yang tidak memungkinkan penggunaan kabel seperti sistem kendali jarak jauh, sistem robotik, atau aplikasi IoT (*Internet of Things*). Teknologi komunikasi *online* memberikan fleksibilitas tinggi dalam desain dan pengoperasian sistem, namun juga membuka celah terhadap ancaman keamanan data[3].

Dalam sistem kontrol *online*, sinyal kendali yang dikirimkan melalui udara sangat rentan terhadap berbagai serangan seperti penyadapan (*eavesdropping*), manipulasi data (*data injection*), maupun *spoofing* [4]. Ancaman-ancaman tersebut dapat menimbulkan kerusakan serius, seperti perubahan nilai kendali yang dapat mengganggu stabilitas sistem atau bahkan menyebabkan kerusakan fisik pada aktuator seperti motor. Oleh karena itu, keamanan komunikasi data dalam sistem kendali menjadi aspek yang sangat krusial untuk diperhatikan. Salah satu solusi yang umum digunakan untuk mengamankan data dalam sistem komunikasi adalah dengan mengimplementasikan algoritma enkripsi. Enkripsi memungkinkan data dikodekan menjadi bentuk yang tidak dapat dipahami oleh pihak yang tidak berwenang[5].

Beberapa penelitian sebelumnya telah mengkaji integrasi algoritma enkripsi dalam sistem kendali *online.* H. Xia et al dalam IEEE *Communications Magazine* menjelaskan bahwa salah satu tantangan utama dalam sistem kendali *online* adalah keterbatasan *bandwidth* dan *delay* yang disebabkan oleh pengamanan data, yang dapat mempengaruhi performa kendali secara signifikan[6]. Penelitian oleh M. Arya dan L. Siregar menunjukkan bahwa penerapan enkripsi RSA dalam sistem kendali *online* PID berhasil menjaga keamanan data, namun menyebabkan penambahan latensi transmisi hingga 18%, yang memengaruhi respons sistem[7].

Sementara itu, studi oleh F. Rahman et al mengenai penggunaan algoritma AES pada komunikasi *online* menunjukkan hasil yang lebih efisien dalam aspek waktu proses dibandingkan RSA, namun masih menimbulkan *overhead*

pemrosesan di sisi mikrokontroler[8]. Berbeda dengan RSA dan AES, algoritma Twofish dirancang dengan struktur ringan dan cepat serta lebih fleksibel untuk dijalankan dalam sistem real-time. Maka dari itu, penelitian ini mengambil pendekatan dengan menggunakan algoritma Twofish dalam sistem kendali *online* PID untuk mengamankan data kendali dan mengevaluasi pengaruhnya terhadap kinerja sistem, khususnya pada kendali posisi sudut motor DC.

Di antara berbagai algoritma enkripsi yang tersedia, Twofish merupakan salah satu algoritma simetris yang menonjol karena kombinasi antara keamanan tinggi, kecepatan, dan efisiensi sumber daya. Twofish adalah algoritma finalis dari kompetisi AES (*Advanced Encryption Standard*) yang dirancang oleh Bruce Schneier dan timnya, dan telah diuji secara luas oleh komunitas kriptografi[9].Twofish menggunakan struktur Feistel, mendukung panjang kunci hingga 256-bit, dan dirancang untuk bekerja secara efisien baik di perangkat lunak maupun perangkat keras. Tidak seperti beberapa algoritma lain, Twofish bersifat *open-source* dan tidak dikenakan hak paten, sehingga sangat cocok untuk penelitian akademik dan pengembangan sistem tertanam.

Penggunaan algoritma Twofish dalam sistem komunikasi *online* telah diuji oleh berbagai peneliti, salah satunya oleh Kumar et al yang menerapkan enkripsi ini pada sistem transmisi data energi pintar berbasis IoT. Hasil penelitian menunjukkan bahwa algoritma Twofish mampu memberikan tingkat keamanan yang tinggi tanpa mengorbankan efisiensi sistem, bahkan pada perangkat dengan keterbatasan sumber daya[10] .Selain itu, studi oleh Praptodiyono et al membandingkan performa Twofish dengan AES pada proses *signaling Mobile* IPv6, dan hasilnya menunjukkan bahwa Twofish menghasilkan *delay* yang lebih rendah dan *throughput yang* lebih tinggi, menjadikannya pilihan yang kompetitif untuk komunikasi *real-time*[11] . Meskipun demikian, implementasi Twofish dalam sistem kendali yang kompleks, seperti kendali PID pada motor DC, masih relatif jarang diteliti. Sistem kontrol PID menuntut presisi tinggi dan waktu respons cepat, sehingga penting untuk mengevaluasi sejauh mana algoritma Twofish dapat diterapkan tanpa mengganggu kestabilan dan kinerja sistem kendali. Dengan latar belakang tersebut, penelitian ini berfokus pada penerapan algoritma Twofish dalam sistem kendali motor DC berbasis mikrokontroler, serta menganalisis pengaruhnya terhadap parameter respons transien sistem.

Dalam konteks sistem kendali *online* PID, penerapan enkripsi seperti Twofish perlu dipertimbangkan secara cermat. Meskipun dapat meningkatkan keamanan, proses enkripsi dan dekripsi juga dapat menambah latensi dan beban komputasi, yang berpotensi mempengaruhi respons waktu nyata (*real-time*) dari sistem kendali[12] . Hal ini menjadi penting untuk dianalisis, karena sistem kontrol umumnya membutuhkan respons cepat dan stabilitas tinggi.

Penelitian ini bertujuan untuk menganalisis pengaruh penerapan enkripsi Twofish terhadap kinerja sistem kendali *online* PID , khususnya dalam mengendalikan posisi sudut motor DC. Dengan membandingkan performa sistem dengan dan tanpa enkripsi, diharapkan dapat diperoleh pemahaman yang mendalam

mengenai sejauh mana algoritma Twofish mempengaruhi parameter penting seperti akurasi posisi, waktu respons, dan stabilitas sistem, serta apakah algoritma ini layak diterapkan dalam sistem kontrol *real-time.*

Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan sistem kendali yang tidak hanya presisi, tetapi juga aman terhadap potensi ancaman siber, terutama dalam era digital yang semakin terhubung secara luas melalui teknologi *online.*

1.2 Rumusan Masalah

Rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Bagaimana cara menerapkan enkripsi Twofish pada komunikasi data sinyal kontrol PID pada sistem *online controller*?
2. Bagaimana pengaruh enkripsi Twofish terhadap parameter respons transien sistem, 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 Twofish pada komunikasi data sinyal kontrol PID pada *online controller*
2. Menganalisa pengaruh Enkripsi Twofish 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 dalam sistem kendali *online*.
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 hanya menggunakan metode enkripsi Twofish 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 pengendali PID berbasis komunikasi *online.*
4. Sistem kendali dikembangkan menggunakan protokol komunikasi TCP dan UDP tanpa mempertimbangkan protokol lain.
5. Evaluasi performa sistem hanya mencakup parameter respons transien yaitu *delay time, rise time, peak time, settling time, dan maximum overshoot, serta analisis steady state error.*

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.