BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada era globalisasi saat ini kemajuan teknologi berkembang sangat pesat memungkinkan manusia dapat berkomunikasi dan saling bertukar informasi atau data secara jarak jauh. Seiring dengan itu tuntutan akan keamanan terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat. Berkembangnya layanan *video surveillance* di berbagai tempat sangat penting untuk para penggunanya dalam hal keamanan dan juga *privacy*. Dengan adanya video *real-time* yang berfungsi untuk merekam suatu kegiatan, gambar ataupun kejadian penting dapat digunakan di tempat seperti perbankan, instansi pemerintah, perusahaan, perkantoran dan sebagainya. Akan tetapi proses pertukaran informasi tersebut bisa disalahgunakan ataupun diakses oleh orang- orang yang tidak bertanggung jawab. Oleh sebab itu diperlukan suatu cara agar tingkat dari kerahasiaan dan keamanan data tersebut tetap terjaga dengan aman. Maka dari itu digunakan suatu metode yaitu kriptografi yang menggunakan algoritma enkripsi AES [1], agar data tersebut tidak dapat disadap oleh pihak ketiga.

Saat ini metode kriptografi sudah banyak digunakan untuk mengamankan data yang penting dan diimplementasikan dalam beberapa bidang. Kriptografi merupakan sebuah metode pengamanan data dengan cara mengubah data asli menjadi bersandi yang tidak dapat dipahami oleh pembacanya apabila tidak mempunyai kuncinya. Pada Tugas Akhir ini diterapkan algoritma AES untuk melakukan enkripsi dan dekripsi pada video *streaming* secara *real-time* agar nantinya diharapkan dapat mengoptimalkan proses pengiriman maupun tingkat keamanan dan kerahasiaan suatu data.

Kriteria pemilihan AES didasarkan pada 3 kriteria utama yaitu: keamanan, komputasi, dan karakteristik algoritma beserta implementasinya. Keamanan merupakan faktor terpenting dalam evaluasi yang meliputi ketahanan terhadap semua analisis sandi yang telah diketahui dan diharapkan dapat menghadapi analisis sandi yang belum diketahui. Dalam hal struktur enkripsi dan dekripsi, AES menggunakan struktur SPN (Substitution Permutation Network) yang memiliki derajat paralelisme yang lebih besar dibanding pendahulunya yaitu DES[2].

1.2 Rumusan Masalah

Berdasarkan penjelasan diatas maka disusunlah rumusan masalah yangdibahas sebagai berikut:

1. Bagaimana cara menerapkan enkripsi dan dekripsi algoritma AES terhadap aspek *security* di dalam *video surveillance?*
2. Pengujian dilakukan dengan melihat hasil dari nilai yang diperoleh terhadap *delay, Avalanche Effect* dan *Normalized Correlation.*

1.3 Tujuan

Berdasarkan rumusan masalah, maka tujuan yang akan dibahas adalah:

1. Menerapkan algoritma AES dengan kunci yang ditentukan pada saat proses enkripsi dan dekripsi video tersebut.
2. Membuat serta merancang *server* dan *client system* untuk enkripsi data *streaming video-surveillance* dan mendekripsikannya langsung secara *real-time* dengan menggunakan algoritma AES dan kunci yang ditentukan.
3. Menganalisis hasil dari performansi sistem yang dilakukan sesuai parameter yang ditentukan.

1.4 Batasan Masalah

Adapun batasan masalah yaitu :

1. Perangkat untuk rekaman dari *video surveillance* berasal dari *webcam* dan *IP camera*.
2. Menggunakan kunci simetris.
3. Software yang dibuat berbasis java.
4. Tidak membahas soal pembobolan jaringan.
5. Admin tidak memerlukan proses autentikasi.
6. Sistem yang dibuat tidak menyimpan file berekstensi.
7. Client tidak terlibat distribusi kunci.
8. Parameter yang akan diujikan dalam performansi sistem meliputi: *delay, jitter, datarate, frame rate,quality, avalanche effect, normalized correlation* dan *response time.*

1.5 Metodologi Penelitian

Langkah-langkah yang diterapkan dalam menyusun tugas akhir ini sebagai berikut :

1. Studi literature tentang teori-teori dan konsep yang berhubungan dengan kriptografi, algoritma AES, *video streaming, video surveillance* serta dari referensi artikel, jurnal maupun buku yang berhubungan dengan pembahasan Tugas Akhir.
2. Studi Eksperimental

Pada langkah ini menghasilkan implementasi perancangan sistem ke software simulasi sehingga hasilnya nanti akan dianalisis sesuai parameter yang ditentukan serta proses implementasi langsung video *real-time*.

3. Pembuatan laporan dari hasil penelitian Tugas Akhir.

1.6 Perancangan

Setelah melakukan analisa terhadap masalah yang dibahas, dilakukan perancangan untuk perangkat lunak.yang meliputi perancangan sistem kamera.

1.7 Sistematika Penulisan

Kesuluruhan tugas akhir ini terdiri atas lima bab pembahasan,

BAB I PENDAHULUAN

Pada bab ini meliputi tentang pembahasan secara singkat yang meliputi latar belakang, perumusan masalah, tujuan, batasan masalah, metodologi penelitian dan sistematika penulisan

BAB II TINJAUAN PUSTAKA

Pada bab ini membahas teori pendukung penyusunan tugas akhir. Teori pendukung meliputi konsep dan teori dasar kriptografi, algoritma AES, dan *video streaming*.

BAB III PERANCANGAN SISTEM

Dalam bab ini diuraikan mengenai alur diagram dari enkripsi dan dekripsi video dengan menggunakan konsep algoritma AES serta menjelaskan pengujian parameter yang dilakukan dalam penelitian.

BAB IV PENGUJIAN DAN ANALISIS SISTEM

Bab ini menjelaskan analisis dan hasil keluaran berdasarkan nilai dari parameter-parameter yang diuji.

BAB V KESIMPULAN DAN SARAN

Bab ini membahas kesimpulan yang diperoleh sesuai dengan hasil simulasi dan nilai parameter-parameter yang diuji serta saran bagi penilitian selanjutnya