

BAB I

PENDAHULUAN

1.1. Latar Belakang

Cloud storage merupakan salah satu teknologi yang saat ini banyak digunakan untuk menyimpan suatu data. Layanan *cloud* memberikan suatu layanan penyimpanan virtual dalam internet di mana para pengguna awam dapat menggunakannya. Setiap data yang saat proses transmisi data dalam *cloud* juga rentan diketahui oleh siapapun.

Selain permasalahan diatas, permasalahan lainnya terletak pada sistem komunikasi. Dalam sistem komunikasi data dari pemancar melalui medium komunikasi disebut kanal komunikasi . Di kanal komunikasi ini pada umumnya menyebabkan terjadinya kesalahan berupa gangguan noise dan sinyal yang melemah bila jarak terlalu jauh (*attenuation*). Gangguan – gangguan tersebut menyebabkan terjadinya kesalahan dalam penerimaan data. Data tersebut akan mengalami pengurangan *bit -bit* selama transmisi sehingga ketika data tersebut sampai pada penerima, data tersebut tidaklah sama seperti data yang dikirim. Pada umumnya jika terjadi suatu kesalahan pada data, maka sistem secara langsung akan melakukan pengiriman kembali data untuk dikirim kembali. Hal ini tentu akan menimbulkan *delay* terhadap data yang dikirimkan

Untuk mengurangi masalah tersebut, maka perlu dibangun suatu sistem *error correction* dengan teknik kriptografi untuk mengenkripsi data. Dalam sistem komunikasi *error correction* digunakan untuk meningkatkan efisiensi dan keakuratan informasi yang dikirimkan.

Banyak teknik kriptografi yang dapat digunakan, salah satunya adalah *Advanced Encryption Standard (AES)*. *AES* merupakan lanjutan dari algoritma enkripsi standar *DES (Data Encryption Standard)* yang masa berlakunya dianggap telah usai karena faktor keamanan. Kecepatan komputer yang sangat pesat dianggap sangat membahayakan *DES*. Kriptografi *AES* sampai saat ini masih digolongkan dalam kriptografi yang masih aman. Banyak dari sistem komunikasi menggunakan *AES* dijadikan dasar sistem karena efisien dan aman. Keamanan dari *AES* ditunjang oleh penggunaan kunci yang sangat besar (128 bit, 192 bit, dan 256 bit).



Sedangkan teknik *error correction* yang digunakan adalah metode *Forward Error Correction* (FEC). FEC merupakan salah satu metode dalam meningkatkan reliabilitas data dalam telekomunikasi data dengan mengoreksi kesalahan *bit-bit* selama transmisi berlangsung. Pada FEC terdapat beberapa teknik pengkodean maupun pendekodean yang dapat digunakan untuk mengoreksi *error* dari data yang diterima. *Turbo Code* merupakan salah satu metode FEC yang akan dibahas pada penelitian ini.

Pada penelitian ini, peneliti akan mengkombinasikan teknik kriptografi AES dengan teknik *Forward Error Correction* (*Turbo Code*). Kemudian kombinasi kriptografi tersebut akan disimulasikan untuk enkripsi dan dekripsi pada berkas *text*, *image* dan *sound* dalam penyimpanan *cloud*. Kemudian di uji menggunakan beberapa parameter seperti BER(*Bit error rate*) terhadap tipe data *text*, *image* dan *sound*, *Avalanche Effect* terhadap tipe data *text*, *image* dan *sound*, waktu eksekusi (waktu enkripsi dan waktu dekripsi) tipe data *text*, *image* dan *sound*.

1.2. Perumusan Masalah

Rumusan masalah dalam penelitian ini adalah seberapa besar performa kombinasi *AES –Turbo Code* dengan tipe data *text*, *image* dan *sound* dilewatkan pada kanal ideal dan AWGN dengan kondisi SNR 0 dB hingga 15 dB sebagai pembangkit awgn, sehingga data yang dikirimkan tersebut tersimpan kedalam penyimpanan *cloud*.

1.3. Tujuan dan Manfaat

Adapun Tujuan dan manfaat yang dapat diambil dari permasalahan diatas antara lain:

1.3.1. Tujuan

Tujuan dalam penelitian ini adalah sebagai berikut :

1. Melakukan simulasi enkripsi dengan kombinasi *Turbo Code* dengan teknik kriptografi AES pada berkas *text*, *image* dan *sound*.
2. Untuk mengetahui performa kombinasi *AES-Turbo Code* pada tipe data *text*, *image* dan *sound*.

1.3.2. Manfaat

Manfaat yang dapat diambil dari penelitian ini yaitu memberikan informasi tentang performa teknik *error correction* pada data dengan mengkombinasikan *Turbo*



Code pada teknik kriptografi AES terhadap gangguan kesalahan seperti derau saat proses pengiriman data ke dalam penyimpanan *cloud*.

1.4. Batasan Masalah

Adapun batasan masalah dalam pengerjaan skripsi ini yakni sebagai berikut:

1. Data yang diproses berupa data *text*, *image* dan *sound*.
2. Tipe kunci yang digunakan *AES 128 bit*.
3. SNR yang digunakan untuk membangkitkan AWGN yakni 0dB hingga 15 dB.
4. Parameter sistem kriptografi ditinjau dari *Avalanche Effect*, waktu enkripsi/dekripsi (waktu eksekusi data) dan BER (*Bit Error Rate*)
5. *Parameter* input dalam *Encode* dan *decoder Turbo Code* yakni , generator polynomial [111;101], *code rate* (1/2). *Decoder* menggunakan Log –MAP dan iterasi pada decoder adalah 1.
6. Implementasi simulasi di buat pada sisi klien berupa aplikasi desktop.
7. *Cloud Storage* yang digunakan adalah *dropbox*.



1.5. Metodologi Penelitian

Pada penelitian ini penulis menerapkan metode penelitian yang bersifat eksperimen. Adapun langkah-langkah yang diterapkan penulis dalam melakukan penelitian adalah sebagai berikut:

1.5.1 Tahap Pertama (Analisa)

Merupakan tahapan dimana penulis melakukan pengamatan dan identifikasi terhadap masalah yang menjadi objek penelitian penulis. Serta melakukan pengumpulan referensi yang dibutuhkan oleh penulis yang dapat diperoleh dari buku, jurnal, artikel, dan lain-lain.

1.5.2 Tahap Kedua (Perancangan Sistem)

1.5.2.1 Perancangan Sistem Kombinasi Kriptografi AES dan Turbo Code

Pada tahap ini, penulis melakukan perancangan pada kriptografi AES dan mengkombinasikan dengan Turbo Code sebagai koreksi *error*.

1.5.2.2 Perancangan Antarmuka

Pada tahap ini, penulis melakukan perancangan antarmuka pada dekstop dan kemudian mengkombinasikan dengan perancangan sistem.

1.5.3 Tahap Ketiga (Implementasi)

Tahap selanjutnya yaitu penulis melakukan penerapan pada kombinasi kriptografi AES dan Turbo Code dalam enkripsi dan dekripsi data pada *client side* untuk keamanan data pada *cloud storage*.

1.5.4 Tahap Keempat (Pengujian)

Pada tahap ini penulis akan melakukan pengujian dan melakukan evaluasi dari hasil penelitian yang telah dilakukan sesuai dengan implementasikan pada sistem. Apabila terdapat kekurangan maka akan dilakukan perbaikan.

1.5.5 Tahap Kelima (Penyusunan Laporan)

Pada tahap ini penulis akan melakukan penulisan terhadap hasil yang didapat dari tahap analisa sampai pada pengujian dari penelitian yang dilakukan.



1.6. Sistematika Penulisan

Secara garis besar, Sistematika penulisan buku dalam skripsi ini adalah sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini menjelaskan tentang latar belakang penelitian, perumusan masalah, tujuan, manfaat, batasan masalah, metode penelitian, serta sistematika penulisan dalam laporan skripsi ini.

BAB II : STUDI PUSTAKA

Pada bab ini menjelaskan penelitian sebelumnya, menjelaskan tentang enkripsi *AES* dan *forward error correction* (FEC) *AES-Turbo Code*.

BAB III : PERANCANGAN SISTEM

Pada bab ini menjelaskan mengenai rancangan sistem beserta rancangan alur *flowchart* yang digunakan dalam pembuatan sistem.

BAB IV : IMPLEMENTASI SISTEM

Pada bab ini menjelaskan tentang hasil implementasi dari sistem yang dibuat berdasarkan rancangan pada BAB III.

BAB V : PENUTUP

Pada bab penutup ini menjelaskan tentang kesimpulan yang penulis dapatkan berdasarkan hasil penelitian. serta pada bab ini juga terdapat saran yang menjadi masukan dalam pengembangan penelitian berikutnya.

