

BAB I PENDAHULUAN

I.1 Latar Belakang

Di Indonesia, terdapat beberapa fenomena yang masih menunjukkan kurangnya tingkat keamanan digital di Indonesia. Data dari Veritrans and Daily Social yang diterbitkan pada 2016 memperlihatkan bahwa Indonesia berada di peringkat tertinggi pada daftar 10 negara yang paling rentan terhadap keamanan digital. Menurut data TER (*treat exposure rate*) yang merupakan parameter untuk menghitung persentase komputer yang terkena serangan, Indonesia memiliki persentase keterserangan malware sebesar 23,54%. Angka ini lebih tinggi dibandingkan dengan China (21,36%) dan juga Thailand 20,78%.

Pentingnya sebuah informasi pada berbagai aspek memicu adanya usaha pencurian atau pemindahan alihan data maupun informasi oleh pihak yang tidak memiliki wewenang. Media penyebaran dan penyimpanan informasi atau data yang digunakan merupakan salah satu alasan riskannya informasi atau data mudah diambil oleh pihak yang tidak berwenang. Salah satu penyebab utama terjadinya hal tersebut tak lain karena kurang optimalnya sistem keamanan dalam menjaga kerahasiaan informasi ataupun data. Ada berbagai cara yang dapat dipraktikkan dalam menjaga keamanan dan kerahasiaan informasi maupun data, salah satu tahapan yang dapat dilakukan untuk menjaga keamanan informasi serta data yaitu dengan teknik kriptografi.

Kriptografi adalah bidang pengetahuan yang menggunakan persamaan matematika dalam tahapan proses enkripsi serta dekripsinya. Metode ini berfungsi untuk mengubah data biasa menggunakan kunci yang sudah ditentukan menjadi data yang tidak diketahui oleh orang yang tidak memiliki wewenang kecuali bagi orang yang sudah memiliki akses kepada data tersebut. Ada banyak macam algoritma kriptografi salah satunya adalah

rivest code 6 (RC6). Algoritma RC6 merupakan algoritma asimetris pengembangan dari algoritma sebelumnya yaitu RC5 sekaligus salah satu kandidat *Advanced Encryption Standard* (AES) yang diajukan oleh RSA Laboratoriest kepada *National Institute of Standards and Technology* (NIST).

Setelah dilakukannya teknik kriptografi untuk menjaga data sehingga sampai ke tangan pihak yang berwenang, terkadang data informasi tersebut masih mengalami kendala. Kendala yang dialami seperti ukuran data yang harus dikirim berukuran besar sehingga melampaui kecepatan transmisi yang dimiliki oleh perangkat keras yang ada, sehingga bisa menyebabkan *delay time* yang relatif cukup besar, untuk mentransfer file text dengan ukuran 27 mb dengan lebar *bandwidth* 265 Kbps maka diperlukan waktu lebih dari 10 menit. Untuk data-data penting pengirim menyadari bahwa penerima data tersebut adalah orang yang dituju, begitu juga sebaliknya, penerima informasi harus yakin bahwa data yang dikirimkan tersebut memang benar berasal dari pengirim yang sesuai. Untuk permasalahan efisiensi pengiriman tersebut diperlukan suatu metode untuk meningkatkan efisiensi pengiriman. Kompresi merupakan salah satu metode yang dapat digunakan.

Algoritma Huffman adalah algoritma yang dapat digunakan untuk melakukan proses pemampatan data untuk memberikan hasil ukuran file yang lebih kecil dari ukuran file aslinya, agar ruang penyimpanan dapat lebih dihemat. Algoritma Huffman merupakan algoritma yang dinamakan sesuai dengan penemu algoritmanya, Huffman adalah algoritma kompresi yang dibuat oleh David Huffman dan juga salah satu algoritma kompresi tertua yang dibuat pada tahun 1952. Algoritma Huffman tersebut digunakan untuk membuat kompresi file dengan jenis *loseless compression*, yaitu pemampatan data dimana tidak satu byte pun dari data akan hilang sehingga data tersebut utuh dan disimpan sesuai dengan aslinya, dengan

teknik kompresi *loseless*, informasi pada data hasil kompresi dapat disusun kembali ke bentuk awal data tanpa mengurangi sedikitpun informasi dari file awal.

Namun, kombinasi teknik kriptografi dan algoritma kompresi Huffman yang bersifat mengacak suatu pesan dapat menimbulkan kecurigaan. Dalam upaya meminimalisir kecurigaan tersebut munculah teknik steganografi yang merupakan pengembangan dari kriptografi. Sadikin (2012) menjelaskan, ‘Teknik steganografi merupakan teknik yang digunakan untuk menyamarkan atau menyembunyikan pesan informasi ke dalam media penampung yang dapat berupa gambar, video, audio atau media digital lainnya’. Teknik ini bertujuan agar informasi atau data rahasia tidak dapat diakses oleh pihak yang tidak berwenang. Saat ini ada beberapa metode steganografi yang digunakan. Salah satunya adalah dengan metode *End of File* (EOF). Sesuai dengan namanya, Metode *End Of File* menyisipkan pesan di akhir sebuah file dimana prinsip kerja metode ini adalah menyisipkan karakter EOF pada akhir file sebelum ditambahkan pesan tersembunyi di belakang file tersebut.

Berdasarkan latar belakang diatas penulis berusaha membuat suatu program pengaman data dengan kombinasi kriptografi, kompresi dan steganografi yang bertujuan sebagai bentuk upaya optimalisasi menghindari penyalahgunaan dan perubahan data oleh pihak yang tidak berwenang, serta pemampatan sebagai upaya untuk meningkatkan transfer data. Tiga teknik ini dikombinasikan guna mendapatkan hasil secara maksimal dalam pencegahan akses data oleh pihak yang tidak berwenang. Oleh karena itu penulis memberi judul pada penelitian ini, **“Optimalisasi Sistem Keamanan Data Untuk Jenis File Dokumen Menggunakan Teknik Steganografi *End Of File*, Algoritma Kriptografi *Rivest Code 6* dan Algoritma Kompresi Huffman”**.

I.2 Rumusan Masalah

Berdasarkan latar belakang yang diuraikan oleh penulis, maka disimpulkan rumusan masalah:

1. Bagaimana cara mengenkripsi, mengkompresi dan menyembunyikan file dengan informasi rahasia ke dalam media digital sehingga informasi rahasia tersebut benar-benar terjaga kerahasiaannya?
2. Apakah proses pengamanan data dengan menggunakan metode enkripsi algoritma RC6, kompresi Huffman dan steganografi EOF dirasa cukup optimal dalam menjaga keutuhan data?

I.3 Tujuan Penelitian

Tujuan penelitian berdasarkan uraian latar belakang dan rumusan masalah diatas yaitu,

1. Menghasilkan model aplikasi enkripsi menggunakan Bahasa pemrograman *Java* dan berbasis *desktop*.
2. Berhasil mengimplementasikan aplikasi yang mengkombinasikan teknik kriptografi, kompresi serta steganografi dengan ukuran file yang optimal untuk penggunaan ruang memori yang lebih kecil.
3. Berhasil mendapatkan hasil optimal dalam pengamanan data, sehingga data yang telah diamankan sulit untuk diakses oleh pihak yang tidak berwenang.

I.4 Manfaat

Berdasarkan latar belakang, rumusan masalah dan tujuan penelitian yang telah dipaparkan di atas, dapat disimpulkan bahwa penelitian ini memiliki manfaat:

1. Dapat menjadikan luaran yang diharapkan dari penelitian ini sebagai bentuk pengamanan data untuk memitigasi risiko terhadap keaslian data, sehingga informasi dan data tersebut tidak dapat diakses oleh orang yang tidak berhak.

2. Dapat dijadikan referensi untuk penelitian yang terkait dengan pembahasan pada tulisan ini.

I.5 Ruang Lingkup

Ruang lingkup pada Implementasi Steganografi, Kriptografi dan Kompresi dalam pengamanan data adalah sebagai berikut:

1. Metode kriptografi yang digunakan adalah metode algoritma *Rivest Code 6 (RC6)*.
2. Metode kompresi yang digunakan adalah metode algoritma Huffman.
3. Metode Steganografi yang digunakan adalah metode *End Of File*.
4. Pengamanan data hanya terfokus pada file dokumen berformat *docx, pdf* dan *xlsx*.
5. Pembuatan sistem ini menggunakan Bahasa pemrograman *Java*.
6. Format *file* yang disisipkan pada metode steganografi berupa *jpg* dan *png*.

I.6 Luaran Yang Diharapkan

Luaran yang diharapkan pada penelitian ini adalah sebuah Aplikasi yang digunakan untuk mengamankan data dari pihak yang tidak berhak mengaksesnya.

I.7 Sistematika Penulisan

Penulis akan memaparkan gambaran sistematika penulisan laporan penelitian ini yang terdiri dari beberapa bagian utama berikut:

BAB 1 Pendahuluan

Bab ini menjelaskan secara singkat terkait latar belakang permasalahan, rumusan masalah, ruang lingkup, tujuan dan manfaat, luaran yang diharapkan dan sistematika penulisan.

BAB 2 Landasan Teori

Bab ini berisi mengenai teori-teori yang bersangkutan dengan penelitian, metode dan alat yang digunakan untuk melaksanakan penelitian.

BAB 3 Metodologi Penelitian

Bab ini membahas metode, kerangka berfikir dan jadwal kegiatan yang dilakukan dalam penelitian.

Daftar Pustaka