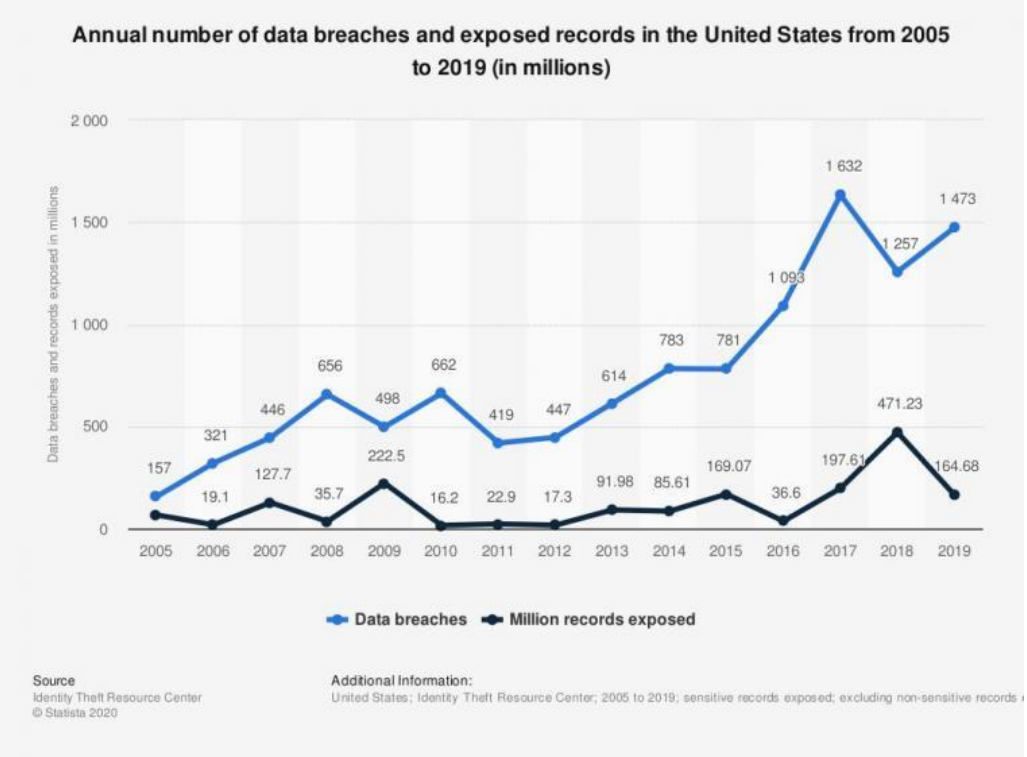
BAB I PENDAHULUAN

1.1. Latar Belakang

Teknologi informasi sekarang ini terus tumbuh semakin pesat, gaya perubahan data serta informasi dapat dilaksanakan dengan cara mudah melalui berbagai macam media yang ada. Keamanan dan penyimpanan menjadi elemen yang sangat penting bagi pemakai teknologi informasi, hal ini tidak lepas bagaimana proses pertukaran data itu dilakukan. Dengan semakin banyaknya orang memanfaatkan layanan komunikasi pertukaran data, tentu masalah pun bermunculan, di antaranya adalah kebutuhan akan media penyimpanan yang semakin besar, keamanan pada data rahasia yang tidak boleh didapatkan serta jatuh ke orang lain, kecepatan proses akan pertukaran data, dan permasalahan lainnya. Dari hal tersebut, maka diciptakan sebuah keamanan bagi seluruh elemen-elemennya, terutama informasi-informasi dan aset-aset penting demi mengamankan kerahasian informasi data tersebut. Keamanan serta penyimpanan menjadi fokus serta point penting yang dibangun serta dikembangkan guna menjamin keutuhan data serta kecepatan dalam informasi.

Pada implementasinya data harus bersifat benar, lengkap, absah, mutakhir, teliti, dan rahasia *(blamtar)* serta dijaga keamanan dan kecepatan untuk mengaksesnya. Penyebab utamanya adalah sebagaimana data semakin tidak memiliki sifat tersebut serta banyaknya pencurian data dilihat dari grafik yang cenderung menunjukan tingkat kenaikan. Selain itu juga proses pemindahan data menjadi permasalahan, di mana data hanya dipindahkan mengunakan media fisik tanpa adanya proses pengamanan terlebih dahulu sebelum proses pengiriman. Salah satu jenis data yang yang harus dijaga keamanan dan prosesnya adalah data antemortem. Sebagaimana yang tertulis dalam pasal 17 UU Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik *(KIP)*, Pasal 44 UU Nomor 43 Tahun 2009 tentang Kearsipan, dan Pasal 26 ayat 1 UU Nomor 19 Tahun 2016 yang turut mengatur tentang perlindungan data pribadi, di mana data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*) yang tidak boleh jatuh ke tangan orang yang tidak bertanggung jawab.

Agar segala sesuatu data yang terkait dengan informasi data pribadi khusunya data antemortem diketahui dan kemudian digunakan oleh orang-orang yang tidak memiliki hak dan kepentingan, maka dibutuhkan sebuah step pengamanan terhadap data tersebut dengan menggunkan teknik kompresi dan kriptografi.



Gambar 1 Serangan Siber Sumber:Identity Theift Resource Center © Statistika 2020

Kriptografi sendiri bertujuan untuk mengubah data yang akan dikirim tidak bisa dibaca dengan mudah oleh pihak yang tidak berwenang serta tidak bertanggung jawab serta untuk menjamin keutuhan data yang terdapat didalamnya. Selain keamanan data, besarnya ukuran file juga membawa kendala, kecepatan transfer data menjadi kendala akan data yang cukup besar guna dalam melakukan pertukaran data informasi. Hal ini tentu akan membawa dampak negatif jika data tersebut harus digunakan dalam waktu yang cepat dan situasi yang mendesak kegunaanya.

Berdasarkan latar belakang diatas penulis berusaha membuat suatu program pengaman data untuk menghindari penyalahgunaan dan pengubahan data, serta pemampatan sebagai upaya untuk pengefisiensian data. Program ini menggunakan algoritma simetrik *Advanced Encrytption Standart (AES)* sebagai algoritma pengamanan data, algortima *AES* memiliki kunci dengan kombinasi yang serupa dengan kunci enkripsi dengan pilihan kunci 128 bit, 192 bit, atau 256 bit (Rinaldi Munir 2019, hlm.275). Algortima kemanan data ini lalu dikombinasikan dengan algoritma pemampatan data kompresi *Huffman* guna memperkecil ukuran serta mempercepat pengiriman data. Dua teknik ini dikombinasikan guna mendapatkan hasil secara maksimal secara efisien maupun keamanan dari data yang kita lindungi yaitu file data antemortem. Oleh sebab itu penulis memberi judul penamaan pada penelitian ini, **"Implementasi Keamanan File dengan *Kompresi Huffman* dan Kriptogrfi menggunkan Algoritma *Advenced Encryption Standart (AES)* pada Pengamanan File Data Antemortem" .**

1.2. Rumusan Masalah

Berlandaskan pemaparan latar belakang pada penjelasan di atas, maka didapatkan rumusan masalah sebagai berikut:

1. Apakah proses enkripsi dengan menggunakan metode algoritma *Kriptografi AES* dapat mengamankan file data antemortem?
2. Apakah proses *Kompresi Huffman* bisa memperkecil ukuran dari berkas hasil kriptografi file data antemortem?
3. Bagaimana kualitas data antemortem sesudah dan sebelum melalui proses penguncian dan pembukaan?

1.3. Batasan Masalah

Berlandaskan pemaparan latar belakang pada penjelasan di atas, bahwa batasan masalah yang diambil dalam hal ini adalah sebagai berikut:

1. Pengamanan file hanya terfokus untuk data antemortem.
2. Algortima *Kriptografi AES* diterapkan pada proses enkripsi dan dekripsi data antemortem.

3. Algorima *Kompresi Huffman* diterapkan pada proses kompresi dan dekrompresi data antemortem.
4. Data antemortem yang dipergunakan hanya sebagaian saja dari keseluruhan data antemortem yang ada.

1.4. Tujuan Penelitian

Tujuan penelitian berdasarkan pemaparan latar belakang dan rumusan masalah:

1. Mengamankan data serta mengefisiensikan *output* hasil dengan teknik kriptografi dan pemampatan data.

1.5. Manfaat

Berlandaskan latar belakang, rumusan masalah, serta tujuan peneletian yang telah digambarkan , dapat disimpulkan bahwa penelitian ini memiliki manfaat:

1. Untuk Institusi terkait

   Menjadikan solusi terkait pengamanan dan pemrosesan dalam data antemortem menggunakan algoritma *Advance Encryption Standart (AES)* dan teknik Kompresi *Huffman.*
2. Untuk Penulis

   Meningkatkan dan mengimplementasikan ilmu pengetahuan yang selama ini didapat selama perkuliahan di bidang keamanan data.

1.6. Ruang Lingkup

Ruang lingkup atas pembahasan pada penelitian ini adalah:

1. Ruang lingkup dari penelitian yang dilakukan dalam penelitian ini mengenai kombinasi antara teknik pengamanan data dan juga proses pemampatan data menggunakan algoritma Kriptografi *AES* dan Kompresi *Huffman* terhadap sebuah data antemortem.

1.7. Luaran yang Diharapkan

Luaran yang diinginkan pada penelitian ini ialah mengetahui seberapa jauh keberhasilan pengamanan terhadap data antemortem menggunakan algoritma Kriptografi *AES* yang dikombinasikan dengan teknik kompresi mennggunakan algoritma Kompresi *Huffman* guna mengefisiensikan hasil pengamanan.

1.8. Sistematika Penulisan

Sistematika penulisan yang dipakai pada penelitian ini diatur dan disusun dalam lima bab dan daftar pustaka serta lampiran yang dibagi menjadi beberap sub bab didalamnya, dengan sistematika penulisan sebagai berikut:

BAB 1 PENDAHULUAN

Bab ini berinformsi tentang bagian dari Latar Belakang, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Manfaat Penelitian, Ruang Lingkup, Luaran yang Diharapkan, dan Sitematika Penulisan dari percobaan ini.

BAB 2 LANDASAN TEORI

Bab yang berisi tentang konsep atau filosofi dasar yang dipergunakan dalam percobaan ini.

BAB 3 METODOLOGI PENELITIAN

Pada bagian bab ini menguraikan sebagian metode penelitian yang terkait dengan penulis gunakan serta urutan tingkatan-tingkatan dalam memenuhi percobaan secara keseluruhan.

BAB 4 HASIL DAN PEMBAHASAN

Pada bab ini mengupas tentang pengunaan algoritma Kriptografi *Advance Encryption Standart (AES)* sebagai algoritma keamanan data dan teknik Kompresi *Huffman* sebagai algoritma pemampatan data.

BAB 5 PENUTUP

Bab ini bagian terakhir yang berisikan atas kesimpulan serta saran dari hasil serta pembahasan yang di gambarkan pada bab 4 (empat) selama proses percobaan sebagai acuan pada penelitian yang selanjutnya.

DAFTAR PUSTAKA

RIWAYAT HIDUP

LAMPIRAN