BAB I

PENDAHULUAN

1.1 Latar Belakang

Media penyimpanan atau *storage* saat ini sudah sangat berkembang, mulai dari jenis sampai kapasitas yang beragam. Koneksi internet pun sudah mulai mudah didapatkan dengan harga terjangkau. Hal ini menjadikan perkembangan *storage* kearah *internet storage* yang lebih dikenal sebagai *online storage*. *Online storage* memberikan fleksibelitas dari segi pengaksessannya, karena selama ada akses internet maka data yang tersimpan pada *storage* pun bisa diakses dari mana saja.

Dengan lebih fleksibelnya pengaksesan storage, hal ini bisa dimanfaatkan untuk membagi data yang tersimpan untuk pihak lain (*sharing*). Dengan terus berkembangnya minat akan penggunaan *online storage* ini, maka banyak bermunculan jasa-jasa penyedia layanan ini dan banyak orang berminat menggunakannya dengan berbagai alasan, *back-up* data penting, *repository syatem*, menghindari kerusakan local akibat virus, *crash* atau malfungsi dari *hardware*.

Dengan semakin berkembangnya *online storage* makin banyak pula keraguan mengenai masalah keamanan dalam penggunaannya. Hal ini ditangani oleh provider *online storage* ini dengan menerapkan enkripsi pada setiap proses penggunaan sampai penyimpanannya. Kriptografi berperan penting dalam hal ini, menurut *The*

Art of Service dalam buku *Cloud Computing Certification Kit Spesilist level: Platform Management & Storage Management*, dengan menerapkan kriptografi akan mencakup tiga aspek utama dari keamanan yang ada: otentikasi, *non-repudiation* (anti penolakan) dan integritas.

Dengan otentifikasi maka pemilik data akan mendapat jaminan bahwa data yang disimpan tidak tersentuh oleh pihak lain yang tidak memliliki hak akses atas data miliknya, jika terjadi perubahan maka pemilik data bisa menyortirnya sebagai data asing yang bukan miliknya karena data sudah berubah. *Non-repudiation* memastikan ketika data yang tersimpan didalam *online storage* diakses data itu benar-benar adalah data miliknya yang asli dan tidak terjadi perubahan. Integritas membuat data yang tersimpan di *online storage* dengan data yang berada di lokal *storage* terjaga kesamaannya tanpa terganggu pihak lain.

Penerapan kriptografi pasti tidak terlepas dari pemilihan penggunaan algoritma yang dipakai. Dalam permasalahan keamanan data yang tersimpan, algoritma AES merupakan pilihan tepat karena AES merupakan salah satu jenis kriptografi *private-key* yang baik. AES menggunakan *private-key*, maka kunci untuk melakukan enkripsi / dekripsi sama, sehingga hanya satu *key* ini satu-satunya kunci untuk memperoleh data. Dan *key* ini hanya dimiliki oleh pemilik atau orang yang memiliki hak akses terhadap data tersebut.

Setelah peran kriptografi yang memberikan pengamanan terhadap data yang disimpan, masalah ukuran *storage* yang tersedia menjadi perhatian berikutnya. Hal ini dikarenakan tidak ada provider penyedia jasa *online storage* yang memberikan jasa secara gratis dengan ful fitur. Setiap ukuran *storage* yang diberikan memiliki perhitungannya sendiri. Dengan adanya hal tersebut maka kompresi berperan dalam menghemat ukuran *storage* dengan membuat data yang akan disimpan menjadi lebih kecil dari ukuran aslinya. Salah satu algoritma kompresi yang sederhana dan mudah diterapkan adalah LZW (Lempel–Ziv–Welch), yang merupakan kompresi dengan metode *dictionary* (kamus) dalam prosesnya dan sangat cocok untuk kompresi data bertipe *hypertext*.

Dengan adanya kriptografi sebagai cara mengamankan data dan kompresi sebagai penghematan ukuran data, maka kolaborasi dari kriptografi dan kompresi akan menjadi sebuah jawaban dari permasalahan *online storage* yang sudah dijelaskan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disebutkan sebelumnya, maka yang menjadi rumusan masalah adalah "Bagaimana menggunakan algoritma kriptografi AES sebagai pengamanan data dan menggunakan algoritma kompresi LZW sebagai usaha untuk menghemat ukuran data pada aplikasi *online storage*", dengan rincian:

1. Bagaimana karakteristik sebuah aplikasi *online storage*.

2. Bagaimana implementasi kriptografi dalam memberikan keamanan *storage*.
3. Bagaimana implementasi kompresi untuk menghemat ukuran *storage*.

1.3 Tujuan Penelitian

Adapun tujuan berdasarkan latar belakang dan rumusan masalah dari pembuatan skripsi ini adalah:

1. Membangun sebuah aplikasi *online storage* yang sesuai dengan karakteristik.
2. Memberikan keamanan data pada aplikasi *online storage* dengan menerapkan kriptografi menggunakan algoritma AES.
3. Memberikan penghematan ukuran *storage* dengan menerakan kompresi menggunakan algoritma LZW.

1.4 Batasan Masalah

Sebagai batasan masalah yang akan dikaji, pembahasan akan difokuskan pada pengimplementasian enkripsi dan kompresi pada aplikasi *online storage*:

1. Aplikasi yang dibuat adalah *online storage* berbasis web.
2. Enkripsi / dekripsi file menggunakan algoritma AES-256 bit.
3. Kompresi file menggunakan algoritma LZW (Lempel–Ziv–Welch).
4. Data yang disimpan dalam aplikasi adalah file hypertext.

1.5 Manfaat Penelitian

Dari pembuatan skripsi ini diharapkan adanya manfaat penelitian sebagai berikut:

1. Bagi penulis, menambah pengetahuan dan wawasan mengenai *online storage* dan kinerja dari kolaborasi antara kriptografi dan kompresi.
2. Bagi pengguna umum, aplikasi *online storage* ini bisa dimanfaatkan untuk keperluan menympan data-data penting yang sering digunakan dengan kebebasan mengakses dari manapun selama ada koneksi internet.
3. Bagi programer, bisa digunakan untuk menyimpan dan *sharing* data utnuk keperluan developing seperti *source code.*

1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penulisan tugas akhir ini adalah sebagai berikut :

1.6.1 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan adalah studi pustaka. Pengumpulan data dengan cara mengumpulkan literatur, browsing internet dan bacaan-bacaan yang terkait dengan *online storage*, keamanan *storage*, kriptografi, algorotma AES, kompresi dan algoritma LZW.

1.6.2 Metode Pembuatan Perangkat Lunak

Teknik analisis data dalam pembuatan perangkat lunak menggunakan paradigma perangkat lunak secara *waterfall* yang meliputi beberapa proses:

1. Analisis

Analisis dalam penelitian ini dimulai dengan menentukan keperluan dan batasan untuk aplikasi *online storage*, pengumpulan materi dari algoritma AES dan algoritma LZW yang akan dipakai.

2. Desain

   Tahap penerjemahan hasil tahapan analisis kedalam bentuk yang bisa dimengerti oleh user sehingga bisa dilanjutkan ketingkat berikutnya.

3. Coding

   Tahap penerjemahan data dan pemecahan masalah yang telah dirancang kedalam baha pemerograman tertentu sesuai dengan hasil tahapan desain.

4. Testing

   Tahapan untuk melakukan pengujian perangkat lunak yang dibangun dengan parameter-parameter yang sudah ditentukan.

1.7 Sistematika Penulisan

Sistematika penulisan proposal ini disusun untuk memberikan gambaran umum tentang perangkat lunak yang akan dibuat. Sistematika penulisan skripsi ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini menguraikan tentang permasalahan yang muncul dari sebuah aplikasi *online storage*, bagaimana cara memebrikan keamanan dan penghematan *storage* dan

tujuan pengimplementasiannya. Dijeaskan juga metode yang dipakai dalam penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini memaparkan materi-materi yang digunakan dalam pembuatan skripsi ini secara rinci, seperti pengertian *online storage*, karakteristik keamanan *online storage*, kriptografi, algoritma kriptografi AES, kompresi dan algoritma kompresi LZW.

BAB III METODOLOGI PENELITIAN

Bab ini memaparkan secara detail tentang tahapan-tahapan pembangunan aplikasi *storage online* dengan implementasi algoritma AES dan algoritma LZW berdasarkan analisis masalah dan perancangan.

BAB IV IMPLEMENTASI

Pada bab ini diuraikan secara detail tentang pengimplementasian hasil analisis dan perancangan kedalam aplikasi *online storage* lengkap dengan antar muka dan pengujian terhadap aplikasi dengan berbagai data.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisi tentang kesimpulan dan saran yang diajukan agar dapat menjadi bahan pertimbangan.