BAB I PENDAHULUAN

1.1 Latar Belakang

Pada saat ini, penggunaan data yang semakin luas digunakan dalam berbagai bidang menjadi isu penting dalam keamanan penyimpanan dan transmisi data. Oleh karena itu, pengamanan data dari pihak yang tidak berhak menjadi hal yang penting. Berdasarkan laporan dari Lembaga Studi dan Advokasi Masyarakat (ELSAM) tentang pencurian data pribadi di Indonesia sepanjang 2013-2017 adalah penyalahgunaan kuasa atas data pribadi sebesar 37%, pencurian dengan *malware* sebesar 30%, pencurian dengan alat besar sebesar 18%, dan pembocoran data sebesar 15% [1].

Komputasi awan atau *cloud computing* merupakan salah satu contoh perkembangan informasi. *Cloud Computing* adalah sebuah model *client-server*, dimana *resource* seperti *server, storage, network* dan *software* dapat dipandang sebagai layanan yang dapat diakses oleh pengguna secara *remote* dan setiap saat [2]. Salah satu layanan komputasi awan yang digunakan adalah *Amazon Simple Storage Service* (S3) atau sering disebut AWS S3. Ruang penyimpanan yang dapat digunakan dan yang paling kecil adalah 1 GB dengan harga $0.025/bulan. Sehingga semakin besar berkas semakin besar pula ruang penyimpanan yang dibutuhkan.

Enkripsi dan kompresi yang dilakukan sebelum berkas diunggah ke *Cloud Storage* merupakan salah satu cara yang dapat digunakan untuk menghemat ruang penyimpanan dan mencegah berkas digunakan oleh pihak yang tidak berkepentingan.

AES (Advanced Encryption Standard) merupakan algoritma kriptografi jenis simetri yang disebut juga sebagai algoritma konvensional, yaitu algoritma yang menggunakan kunci enkripsi dan kunci dekripsi yang sama [3]. AES diperoleh dari pemenang kompetisi yang diadakan NIST tahun 1997. NIST memberikan penilaian pada general security, implementasi software dan hardware, ruang lingkup, implementasi atas serangan, enkripsi dan dekripsi, kemampuan kunci, dan kemampuan lain seperti fleksibilitas dan kepotensialan untuk tingkat instruksi paralel. Akhirnya, 2 Oktober 2000 terpilih lah algoritma

Rijndael yang dibuat oleh Dr. Vincent Rijment dan Dr. Joan Daemen sebagai pemenang [4].

Lempel-ziv-Welch (LZW) adalah algoritma kompresi lossless universal yang diciptakan Abraham Lempel, Jacob Ziv, dan Terry Welch. Algoritma ini melakukan kompresi dengan menggunakan dictionary, di mana fragmen-fragmen teks digantikan dengan indeks yang diperoleh dari sebuah kamus [5]. Algoritma Lempel Ziv Welch (LZW) merupakan algoritma yang sering digunakan dalam proses kompresi data, pada beberapa penelitian terdahulu yang pernah dilakukan, di dalam jurnal yang berjudul Survey on LZW-Dictionary based Data compression Technique, algoritma LZW disimpulkan merupakan algoritma yang memiliki rasio kompresi lebih baik dari algoritma kompresi dasar lainnya [6].

Pada penelitian sebelumnya yang dilakukan oleh Muhammad Faqih, Imam Marzuki, dan Dyah Ariyanti pada tahun 2017, terkait aplikasi kompresi untuk pengiriman data menggunakan metode LZW *(Lempel Ziv Welch)*. Dalam penelitiannya Muhammad Faqih, Imam Marzuki, dan Dyah Ariyanti, menyebutkan bahwa aplikasi kompresi data ini dapat mengkompresi data dengan baik, dengan hasil kompresi yang sesuai dimana data yang lebih besar hasil kompresinya dapat lebih kecil dengan isi data karakter lebih banyak yang sama begitu sebaliknya [7].

Penelitian yang lain dilakukan oleh Ako Muhammad Abdullah tahun 2017 meyebutkan bahwa metode *Advanced Encryption Standard* (AES) memiliki kinerja atau kemampuan untuk memberikan keamanan yang lebih baik dibandingkan dengan algoritma lain seperti DES, 3DES dan lainnya [8].

Maka dari itu dengan mengacu pada penelitian sebelumnya, disusunlah penelitian tugas akhir yang berjudul "**Aplikasi Pengamanan Data dengan Algoritma *Advanced Encryption Standard* (AES) dan Kompresi File Menggunakan Algoritma *Lempel-ziv-Welch* (LZW) pada Cloud Storage**".

1.2 Rumusan Masalah

Berdasarkan latar belakang yang dipaparkan di atas, memiliki beberapa rumusan masalah terkait dengan permasalahan tersebut, yaitu :

1. Bagaimana cara mengimplementasikan algoritma kompresi LZW dan kriptografi AES pada *file* dan mengunggahnya ke *Cloud Storage* sehingga keamanan berkas dapat terjamin?
2. Bagaimana performa dan akurasi algortima kriptografi AES dan kompresi LZW yang digunakan untuk pengamanan data *file* pada *Cloud Storage* ?

1.3 Batasan Masalah

Berdasarkan latar belakang masalah yang sebelumnya telah diuraikan, dengan demikian batasan permasalahan akan dibatasi menjadi lebih sederhana dan lebih khusus agar pembahasan dalam penelitian ini tidak menyimpang dari apa yang telah ditetapkan. Adapun batasan masalah dalam penelitian ini sebagai berikut:

1. Pemrograman yang digunakan berbasis *web* untuk enkripsi dan dekripsi *file*.
2. Layanan penyimpanan / *cloud storage* menggunakan AWS S3.
3. Algoritma enkripsi yang digunakan adalah AES (*Advanced Encryption Standard*).
4. Metode kompresi yang digunakan adalah algoritma LZW (*Lempel-ziv-Welch*).
5. File yang digunakan untuk enkripsi adalah file yang berekstensi .pdf, .txt, .docx/.doc, .xlsx, .jpg, .png, .mp4.
6. Maksimal file size 150MB.
7. Output dari aplikasi ini adalah sebuah *file* yang sudah terenkripsi yang berekstensi .enc dan tersimpan di *cloud storage* dan kemudian dapat di deskripsi menjadi *file* asli yang berekstensi seperti semula sebelum di enkripsi.

1.4 Tujuan Penelitian

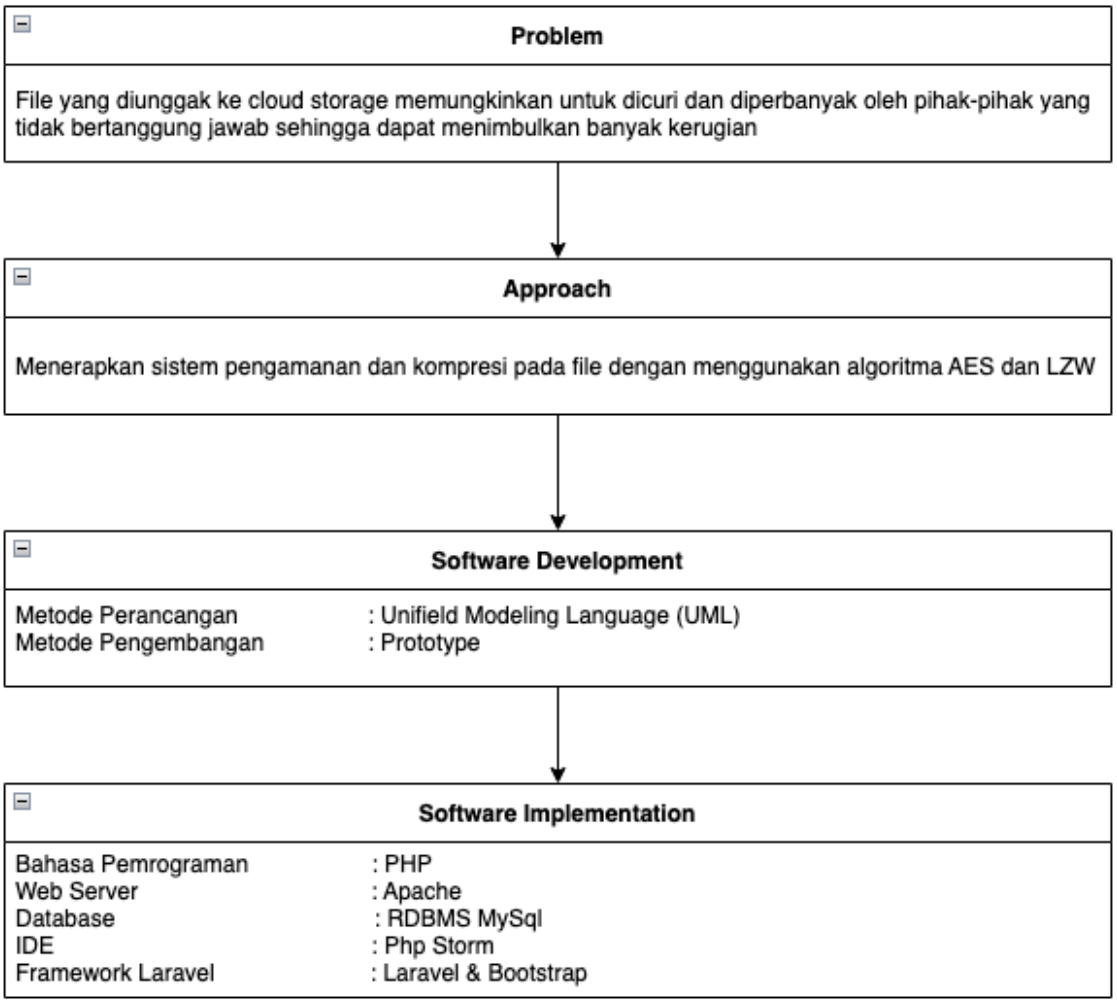
Berdasarkan rumusan masalah yang sebelumnya telah dijabarkan, adapun tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

1. Untuk mengimplementasikan algoritma LZW yang mampu digunakan untuk mengkompresi data dan algoritma kriptografi AES untuk mengamankan berkas yang diletakkan pada *Cloud Storage*.

2. Untuk mengetahui performa dan akurasi algoritma kriptografi AES dan kompresi LZW yang digunakan pada pengamanan file *Cloud Storage.*

1.5 Kerangka Pemikiran

Berikut merupakan kerangka pemikiran pada penelitian tugas akhir yang dapat diuraikan pada Gambar 1.1 dibawah ini.



Gambar 1.1 Kerangka Pemikiran

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini berisi mengenai latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, tujuan dan manfaat penelitian, kerangka pemikiran, metode penelitian, serta sistematika penulisan yang menguraikan urutan penyajian yang digunakan dalam penyusunan skripsi.

BAB II KAJIAN LITERATUR

Bab ini berisi tentang uraian teori-teori yang digunakan dalam analisa permasalahan dan perancangan implementasi.

BAB III METODOLOGI PENELITIAN

Bab ini membahas mengenai hasil analisa dari permasalahan yang ada saat ini dan analisa kebutuhan yang diperlukan untuk mengatasi permasalahan tersebut. Pembuatan desain dari sistem dengan mengacu pada analisis yang telah dibahas.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan mengenai implementasi aplikasi yang telah dianalisis dan dirancang sebelumnya yang kemudian dilakukan pengujian dengan menggunakan metode pengujian *black box*.

BAB V SIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran untuk pengembangan aplikasi lebih lanjut dalam upaya memperbaiki kelemahan pada aplikasi guna untuk mendapatkan hasil kinerja aplikasi yang lebih baik dan pengembangan program selanjutnya.