BAB 1 PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi saat ini berkembang sangatlah pesat, hampir semua orang sudah memanfaatkan teknologi informasi bagaimanapun bentuknya. Penyimpanan berkas di *cloud* merupakan bentuk pemanfaatan teknologi informasi yang sudah tidak asing. Penggunaan media penyimpanan *cloud* di beberapa tahun belakangan ini terus meningkat. Media penyimpanan *cloud* merupakan teknologi penyimpanan yang bersifat digital yang menggunakan server virtual yang bekerja sebagai media penyimpanannya.

Keamanan menjadi fokus utama dalam menggunakan media penyimpanan *cloud*. Salah satu contoh dari ancamanan di media penyimpanan *cloud* adalah data yang disimpan di *cloud* menjadi tidak aman karena *cloud* bersifat *multi-user* dimana banyak user berbagi infrastruktur dan aplikasi yang sama yang bisa. Hal ini bisa memungkinkan oknum tertentu yang tidak bertanggung jawab mengetahui dan merusak isi data yang disimpan di *cloud*. Untuk mengatasi masalah ini bisa dilakukan enkripsi pada file yang akan diunggah oleh pengguna atau bisa disebut *client-side encryption*. Sebenarnya dari pihak penyedia layanan *cloud storage* sudah menyediakan enkripsi dari sisi server atau *server-side encryption* dan untuk saat ini masih relatif aman, namun kita tidak bisa mengabaikan kemungkinan jika pengamanan dari sisi server diretas di masa yang akan datang. Oleh sebab itu enkripsi dari sisi pengguna menjadi tindakan preventif untuk menghindari kebocoran data yang disimpan ke *cloud storage*.

Penelitian tentang keamanan data dengan menggunakan kriptografi telah banyak dilakukan oleh beberapa peneliti. Penelitian yang dilakukan oleh Mohammad Fachry, Ari Kusyanti dan Kaysful Amron (2018) mereka menggunakan algoritma AES dan Shamir secret sharing untuk mengenkripsi data menjadi tiga nilai dan menggunakan shamir secret sharing untuk menyimpan tiga nilai tersebut pada tiga *cloud storage* yang berbeda. Penelitian selanjutnya dilakukan oleh Bokefode Jayant D. dkk (2015). Pada penelitian ini Bokefede dkk membahas tentang kriptografi pada sistem *role-based access control* untuk mengamankan penyimpanan data pada *cloud storage.* Pada penelitian ini *role-based access control* digabung dengan AES dan RSA untuk mengamankan penyimpanan *cloud* yang memungkinkan sebuah organisasi mengunggah data secara aman pada *public cloud.* Lalu penelitian selanjutnya oleh Dr. Rajamohan Parthasarathy dkk (2019), dalam penelitian ini Dr. Rajamohan dkk menggunakan algoritma RSA untuk mengenkripsi data dalam lingkungan *cloud*nya agar hanya pengguna yang memiliki hak yang bisa mengaksesnya.

Berdasarkan penelitian-penelitian di atas, AES banyak digunakan karena merupakan salah satu algoritma simetris kuat yang banyak digunakan dan memiliki perlindungan yang lebih baik dari pada algoritma simetris yang lain. Dan RSA digunakan untuk mengenkripsi kunci AES dikarenakan AES hanya menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Sehingga dengan mengenkripsi Kuncinya dengan RSA maka akan membuat file lebih aman. Oleh karena itu pada penelitian ini penulis akan menggunakan algoritma kriptografi AES dan RSA untuk membuat sistem pengamanan data pada *cloud storage*.

1.2 Rumusan Masalah

Dari latar belakang yang sudah dijelaskan, permasalahan yang akan dibahas adalah sebagai berikut:

1. Bagaimana membangun sistem enkripsi dan dekripsi menggunakan algoritma AES dan RSA untuk pengamanan file yang akan di simpan ke *cloud storage*?
2. Bagaimana kinerja sistem enkripsi dekripsi dengan menggunakan algoritma AES dan RSA yang terhubung ke *cloud storage*?

1.3 Batasan Masalah

Untuk menghindari meluasnya penelitian ini maka permasalahan dibatasi dengan hanya mencakup hal-hal berikut:

1. Penelitian ini hanya melakukan enkripsi file ke *Cloud* Storage dan dekripsi file
2. *Cloud storage* yang digunakan Google Drive dan Dropbox.
3. Bahasa pemrograman yang digunakan adalah PHP.
4. Ekstensi file yang digunakan adalah Dokumen (.txt, .xls, .ppt, .doc, .pdf), Audio (.mp3), Gambar (png, jpg), File Kompresi (.zip) dan Video (.mp4).
5. Ukuran file maksimal adalah 150mb pada Dropbox.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah menerapkan algoritma AES dan RSA dalam sistem pengamanan data file yang akan disimpan ke *cloud storage*, yang dimana dalam penelitian ini adalah Google Drive dan Dropbox.

1.5 Manfaat Penelitian

Manfaat yang didapatkan dari penelitian ini adalah:

1) Bagi penulis:
    a) Mengimplementasi ilmu kriptografi untuk pengamanan data di *cloud storage*.
2) Bagi Pengguna:
    a) Mengamankan data-data penting yang disimpan di *cloud.*
    b) Memudahkan pengguna dalam mengenkripsi data penting ke *cloud storage.*

1.6 Luaran yang Diharapkan

Luaran yang diharapkan pada penelitian ini adalah sebuah sistem keamanan data yang terhubung dengan *cloud storage* (Google Drive dan Dropbox) dengan menggunakan algoritma AES dan RSA sebagai algoritma enkripsi. Diharapkan sistem ini dapat mengenkripsi file ke *cloud storage* (Google Drive dan Dropbox) dan mendekripsi file.

1.7 Sistematika Penulisan

Dalam penulisan proposal tugas akhir ini dibagi menjadi beberapa bab, yaitu:

BAB 1 PENDAHULUAN

Bab ini terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, metodologi penelitian, dan sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA

Bab ini berisi uraian singkat tentang teori yang berhubungan dan diperlukan dalam penelitian ini.

BAB 3 METODOLOGI PENELITIAN

Bab ini menguraikan secara mendetail mengenai metodologi yang digunakan d alam pembuatan sistem pada penelitian ini.

BAB 4 HASIL DAN PEMBAHASAN

Bab ini memuat tentang hasil dari sistem yang sudah dirancang dan dibuat untuk menyelesaikan permasalahan yang ada.

BAB 5 PENUTUP

Bab ini berisi tentang kesimpulan yang dapat diambil dari hasil penelitian dalam menjawab permasalahan yang ada dalam penelitian ini. Serta saran-saran kedepannya untuk mengembangkan hasil yang telah dicapai pada penelitian ini.

DAFTAR PUSTAKA

RIWAYAT HIDUP

LAMPIRAN