BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Perkembangan teknologi *cloud computing* telah membawa perubahan besar dalam bidang pengelolaan data. IDC memperkirakan sekitar 60% organisasi di seluruh dunia telah menerapkan layanan *hybrid cloud*, baik untuk fasilitas layanan *provider* maupun *on-premises* (Waranggani, 2022). Hal ini dikarenakan *cloud computing* memungkinkan pengguna untuk menyimpan, mengelola, dan mengolah data pada *server* jarak jauh, yang dapat memberikan fleksibilitas, efisiensi, dan penghematan biaya operasional. Keunggulan lain dari teknologi ini adalah kemampuannya untuk menyediakan sumber daya yang dapat diskalakan, sehingga sangat bermanfaat bagi usaha kecil dan menengah (UKM) yang sering kali menghadapi tantangan dalam investasi awal yang besar untuk infrastruktur Teknologi Informasi (Atuah dkk., 2023).

Namun, di balik segala keuntungannya, keamanan dan privasi data dalam cloud masih menjadi perhatian utama. Salah satu risiko terbesar dalam penggunaan layanan *cloud* adalah potensi penyalahgunaan data oleh pihak ketiga, baik karena serangan siber, *insider attacks*, maupun kebocoran data dari penyedia layanan *cloud*. Menurut laporan IBM Security (2024), rata-rata biaya pelanggaran data secara global telah mencapai 4,88 juta USD, meningkat 10% dari tahun sebelumnya dan menjadi rekor tertinggi yang pernah ada. Laporan tersebut juga menunjukkan bahwa sebagian besar insiden melibatkan data sensitif yang disimpan dalam infrastruktur *cloud*, membuat keamanan data menjadi prioritas utama dalam pengembangan solusi *cloud computing* (IBM, 2024).

Salah satu pendekatan utama untuk mengatasi tantangan keamanan data dalam *cloud* adalah melalui penerapan enkripsi. Dalam dunia kriptografi, terdapat beragam algoritma yang digunakan untuk melindungi data melalui enkripsi.

Beberapa algoritma yang dikenal umum termasuk *Data Encryption Standard* (DES), *Rivest Cipher* 4 (RC4), *Blowfish*, *Twofish*, dan *Advanced Encryption Standard* (AES) (Setiani dkk., 2024). Di antara semua algoritma tersebut, AES menjadi salah satu algoritma enkripsi yang paling banyak digunakan.

Advanced Encryption Standard (AES) merupakan algoritma kriptografi simetris yang banyak digunakan untuk mengamankan data dalam berbagai aplikasi, mulai dari komunikasi internet hingga penyimpanan *cloud*. AES bekerja dengan cara mengenkripsi data dalam blok-blok berukuran 128 bit menggunakan kunci 128, 192, atau 256 bit, dan terdiri dari beberapa putaran transformasi yang mencakup substitusi, permutasi, dan operasi aritmatika pada level bit (Rao dkk., 2017).

Terdapat beberapa alasan yang menjadikan AES pilihan utama dalam keamanan data. Pertama, AES telah diterima secara luas dan diakui sebagai standar enkripsi yang aman. Berdasarkan penelitian yang dilakukan oleh Salsabila dkk., (2023), AES menawarkan performa tinggi dengan tingkat keamanan yang tetap kuat dengan menggunakan kunci 128-bit, 192-bit, atau 256-bit, membuatnya sangat sulit untuk diserang dengan metode *brute-force*. Selain itu, AES juga memiliki struktur blok yang efisien dan cepat, sehingga dapat mengenkripsi dan mendekripsi data dalam waktu singkat, seperti yang telah dibuktikan dalam beberapa studi kasus (Wiharto & Mufti, 2025) yang menunjukkan bahwa AES tidak hanya aman, tetapi juga efisien secara waktu. Terakhir, AES juga memainkan peran penting dalam menjamin keamanan data di lingkungan komputasi awan. Penerapan AES dalam lingkungan *cloud* terutama berfokus pada pengamanan data saat disimpan (*at rest*) dan saat ditransmisikan (*in transit*). Struktur kunci simetris serta proses algoritmik yang efisien pada AES memungkinkannya mengelola data dalam jumlah besar dengan aman. Hal ini sangat penting dalam layanan *cloud*, di mana data terus-menerus dipindahkan dan disimpan di berbagai platform (Ajmal dkk., 2022). Penelitian-penelitian tersebut menegaskan bahwa AES tetap menjadi standar pada penggunaannya dalam pengamanan data digital karena keseimbangan antara kecepatan, efisiensi, dan kekuatan enkripsinya.

Penelitian ini bertujuan mengembangkan aplikasi enkripsi file berbasis *desktop* yang memungkinkan pengguna mengenkripsi dan mendekripsi file PDF mereka sebelum disimpan ke *cloud*. Dengan pendekatan ini, pengguna tetap dapat menjaga kerahasiaan data pribadi mereka, sementara sistem tetap berjalan ringan dan efisien. Aplikasi ini akan mendukung proses *upload* dan *download* dari layanan *cloud*, serta memastikan bahwa seluruh file yang disimpan tidak dapat diakses tanpa proses dekripsi melalui kunci rahasia. Sistem yang dikembangkan diharapkan dapat menjadi solusi pengamanan data yang terjangkau, mudah digunakan, dan efektif bagi pengguna individu maupun organisasi kecil yang ingin menyimpan data penting mereka secara aman di *cloud*.

1.2 Rumusan Masalah Penelitian

Berdasarkan latar belakang di atas, dirumuskan beberapa permasalahan penelitian sebagai berikut:

1. Bagaimana mengembangkan aplikasi *desktop* untuk melakukan enkripsi dan dekripsi file menggunakan algoritma AES?
2. Bagaimana kinerja algoritma AES dalam menjaga keamanan dan efisiensi file terenkripsi yang disimpan di *cloud*?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dirumuskan sebelumnya, maka tujuan dari penelitian ini adalah sebagai berikut:

1. Mengembangkan aplikasi *desktop* yang mampu melakukan proses enkripsi dan dekripsi file menggunakan algoritma *Advanced Encryption Standard* (AES).
2. Melakukan uji kinerja algoritma AES dalam hal efisiensi dan kemampuan menjaga keamanan data yang disimpan di *cloud*.

1.4 Ruang Lingkup

Penetapan ruang lingkup dalam penelitian ini bertujuan untuk membatasi cakupan pembahasan agar tetap fokus dan tidak melebar dari permasalahan utama. Adapun batasan ruang lingkup penelitian ini adalah sebagai berikut:

1. Penelitian mendukung proses enkripsi dan dekripsi pada file dengan format *Portable Document Format* (PDF), *Excel Open XML Spreadsheet* (XLSX), dan *Document Open XML* (DOCX).
2. Aplikasi ini didesain untuk perangkat *desktop* dengan sistem operasi Windows.
3. Integrasi penyimpanan cloud terbatas pada layanan Google Drive, menggunakan file kredensial JSON yang dimiliki masing-masing pengguna.
4. Aplikasi tidak menyediakan fitur pengelolaan folder atau struktur direktori dalam Google Drive, dan hanya mendukung fungsi unggah, unduh, dan hapus file.

1.5 Manfaat Penelitian

1.5.1 Manfaat Teoritis

Manfaat teoritis yang diharapkan dari hasil penelitian ini yaitu:

1. Memberikan kontribusi ilmiah dalam bidang keamanan data, khususnya dalam implementasi algoritma *Advanced Encryption Standard* (AES) untuk perlindungan file digital yang disimpan di *cloud*.
2. Menambah wawasan akademik mengenai pengembangan aplikasi desktop untuk sistem enkripsi file, serta penerapan kriptografi simetris dalam konteks penyimpanan *cloud*.

3. Menjadi referensi bagi penelitian selanjutnya yang ingin mengeksplorasi efisiensi dan efektivitas algoritma enkripsi ringan, seperti AES, dalam mendukung perlindungan data di berbagai skenario penyimpanan dan transmisi digital.

1.5.2 Manfaat Praktis

Adapun manfaat praktis yang didapatkan dari hasil penelitian ini diantaranya:

1. Memberikan solusi praktis bagi pengguna individu maupun organisasi kecil untuk mengamankan file penting mereka sebelum disimpan ke layanan *cloud*.
2. Menyediakan aplikasi *desktop* berbasis Java yang mudah digunakan dan dapat dijadikan alat bantu untuk mengenkripsi dan mendekripsi file PDF secara lokal.
3. Membantu meningkatkan kesadaran akan pentingnya perlindungan data melalui enkripsi sebelum proses unggah ke *cloud*, terutama dalam konteks keamanan data pribadi dan informasi sensitif.

1.6 Struktur Organisasi Skripsi

Sistematika penulisan skripsi berperan sebagai pedoman agar penulisan skripsi menjadi lebih terarah. Oleh karena itu, skripsi ini dibagi ke dalam beberapa bab yang masing-masing memiliki fokus pembahasan tersendiri. Adapun struktur organisasi skripsi ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab I berupa Pendahuluan yang berisi latar belakang penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, dan ruang lingkup penelitian.

BAB II TINJAUAN PUSTAKA

Bab II berupa Tinjauan Pustaka yang berisi uraian teori dan penelitian terdahulu yang relevan sebagai dasar untuk mendukung penelitian. Bagian ini juga mencakup kerangka teori dan konsep yang menjadi landasan penelitian.

BAB III METODE PENELITIAN

Bab III berisi uraian Metode Penelitian untuk menjelaskan metode yang digunakan dalam penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab IV berisi uraian Hasil dan Pembahasan untuk menyajikan temuan atau hasil penelitian dalam bentuk teks, tabel, atau grafik, serta memberikan interpretasi dan pembahasan terhadap hasil tersebut. Pada bagian ini, hasil penelitian dikaitkan dengan teori atau penelitian terdahulu.

BAB V SIMPULAN DAN SARAN

Bab V berupa Simpulan dan Saran yang menyajikan ringkasan dari hasil penelitian serta menjawab rumusan masalah. Bagian ini juga memberikan saran untuk penelitian selanjutnya atau implikasi praktis dari temuan penelitian