BAB I
PENDAHULUAN

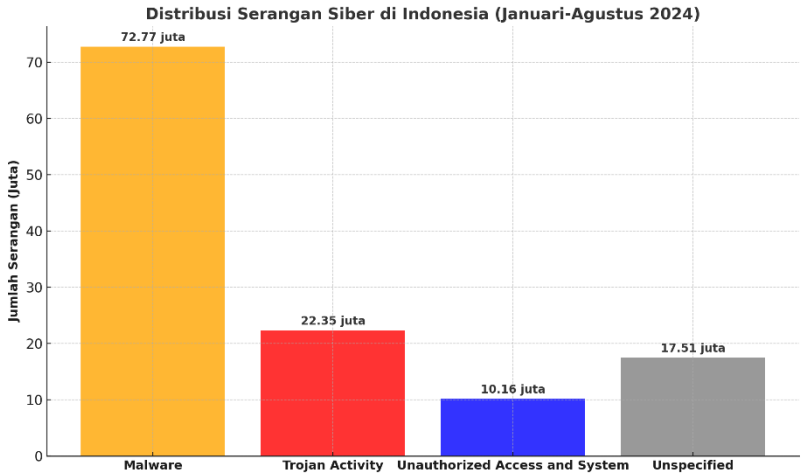
1.1 Latar Belakang Penelitian

Perkembangan teknologi informasi yang sangat pesat dalam dua dekade terakhir telah membawa perubahan signifikan dalam cara individu dan organisasi melakukan penyimpanan, mengakses, serta membagikan informasi digital. Di tengah transformasi digital ini, isu mengenai keamanan data menjadi semakin krusial. Data yang sebelumnya tersimpan secara lokal kini banyak dialihkan ke sistem yang memungkinkan akses dari mana saja, melalui jaringan *internet*, sehingga memberikan fleksibilitas, efisiensi biaya, dan kemudahan penggunaan. Namun, perubahan ini juga memperbesar potensi ancaman terhadap integritas, kerahasiaan, dan ketersediaan data. Untuk mengatasi ancaman tersebut, diperlukan keamanan data, yang merupakan sebuah proses yang memadukan regulasi dan teknologi untuk melindungi informasi dari kerusakan, modifikasi, maupun penyebaran tanpa izin (Kurnia dkk., 2025). Mengingat data kini menjadi salah satu aset paling berharga baik berupa informasi pribadi, finansial, maupun rahasia bisnis (Sitompul & Nasution, 2024).

Berdasarkan data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) jumlah pengguna internet di Indonesia pada tahun 2024 mencapai 221.563.479 jiwa dari total populasi 278.696.200 jiwa penduduk Indonesia tahun 2023. Sejak tahun 2018, penetrasi internet di Indonesia terus menunjukkan peningkatan yang konsisten, dari 64,8% pada tahun 2018 menjadi 78,19% pada tahun 2023. Peningkatan tersebut mengalami kenaikan sebesar 1,4% dibandingkan periode sebelumnya. Tingginya jumlah pengguna ini menunjukkan besarnya ketergantungan masyarakat Indonesia terhadap teknologi digital, yang di sisi lain juga meningkatkan potensi ancaman terhadap keamanan data sensitif mereka.

Namun, di balik tingginya jumlah pengguna internet di Indonesia, muncul risiko terkait keamanan dunia digital. Serangan siber menjadi ancaman nyata yang dapat membahayakan data pribadi maupun informasi penting. Dalam beberapa tahun terakhir, peningkatan ketergantungan terhadap teknologi dan internet turut

beriringan dengan peningkatan ancaman serangan siber yang semakin kompleks. Adapun data distribusi serangan siber di Indonesia dapat dilihat pada Gambar 1.1.



Gambar 1.1 Data distribusi serangan siber di Indonesia (BSSN, 2024)

Berdasarkan Gambar 1.1 Badan Siber dan Sandi Negara (BSSN) mencatat pada periode Januari hingga Agustus 2024, serangan siber di Indonesia mencapai 122,79 juta anomali trafik internet. *Malware* menjadi jenis serangan paling dominan, dengan jumlah serangan mencapai 72,77 juta atau sekitar 59,26% dari total serangan. Di posisi kedua, aktivitas *trojan* tercatat sebanyak 22,35 juta serangan atau 18,20%, diikuti oleh serangan *unauthorized access and system* yang mencapai 10,16 juta atau 8,28%. Sementara itu, kategori *unspecified* menyumbang 17,51 juta serangan, menggambarkan 14,26% dari total serangan.

Mengingat tingginya jumlah serangan yang terjadi, penting untuk menjaga keamanan data sensitif yang dapat terancam oleh ancaman siber. Salah satu pendekatan yang telah terbukti efektif dalam menjaga kerahasiaan dan integritas data adalah melalui penerapan kriptografi. Algoritma *Advanced Encryption Standard* 256-bit (AES-256) merupakan salah satu algoritma simetris yang banyak digunakan karena menawarkan tingkat keamanan yang tinggi. Dengan panjang kunci sebanyak 256-bit, AES-256 memberikan perlindungan yang kuat terhadap serangan *brute force* dan telah menjadi standar dalam berbagai sistem keamanan data modern (Ridho & Romli, 2024). Namun, proses enkripsi menggunakan algoritma ini juga memiliki kelemahan, yaitu kecenderungan menghasilkan ukuran

file terenkripsi yang lebih besar dibandingkan ukuran *file* aslinya, yang berdampak pada efisiensi dalam proses penyimpanan maupun transmisi data.

Untuk itu, diperlukan metode tambahan yang dapat digunakan untuk menangani kendala tersebut adalah dengan menggunakan teknik kompresi data. Kompresi data adalah proses pengurangan ukuran *file* dengan cara menghilangkan redundansi atau pengulangan informasi di dalam data tersebut. Salah satu algoritma klasik yang sering digunakan adalah Huffman *Coding*, yaitu teknik kompresi berbasis pohon biner yang menghasilkan representasi bit paling efisien untuk setiap simbol berdasarkan frekuensi kemunculannya. Namun, efisiensinya menurun apabila saat dihadapkan dengan *string* data yang berulang, karena pendekatannya yang terbatas pada level simbol. Untuk mengatasi kelemahan tersebut, penelitian ini akan memanfaatkan algoritma Deflate yang menawarkan efisiensi lebih tinggi karena merupakan kombinasi dari algoritma LZ77 dan Huffman, sehingga mampu menangani *string* berulang dalam rentang lebih panjang serta mendukung pemrosesan blok dinamis secara lebih fleksibel (Deutsch, 1996). Dengan demikian, Deflate menjadi pilihan tepat untuk menurunkan ukuran *file* secara signifikan sebelum dilakukan enkripsi.

Selain itu, kebutuhan akan aplikasi yang mendukung keamanan *file* secara praktis dan efisien semakin meningkat, seiring dengan meningkatnya ketergantungan terhadap layanan digital berbasis web. Penelitian oleh Kafa dkk. (2024), yang menerapkan algoritma AES-256 dan Huffman, memang menunjukkan hasil positif dalam hal efisiensi kompresi. Namun, penelitian tersebut masih terbatas pada pengujian lokal, belum menjelaskan mekanisme penyimpanan *file* secara daring, serta justru menghasilkan ukuran *file* yang justru membengkak setelah melalui proses enkripsi.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk mengembangkan sebuah aplikasi web berbasis *cloud* yang mampu menggabungkan keamanan (melalui enkripsi AES-256) dan efisiensi penyimpanan (melalui kompresi Deflate), dengan penambahan kemampuan akses *online* dan penyimpanan terpusat menggunakan teknologi *cloud*. Dalam konteks ini, Google Cloud Platform (GCP) dipilih bukan untuk membangun sistem keamanan *cloud* yang kompleks,

tetapi lebih sebagai sarana untuk mendukung *deploy* aplikasi web yang dikembangkan oleh peneliti agar dapat berjalan secara *online*, serta sebagai media penyimpanan *file* yang telah diproses. Layanan seperti Cloud Run digunakan untuk menjalankan aplikasi secara otomatis dan fleksibel tanpa perlu konfigurasi *server* manual, sementara *Cloud Storage* digunakan untuk menyimpan *file* hasil kompresi dan enkripsi, serta Firestore yang berfungsi sebagai basis data *Not Only Structured Query Language* (NoSQL) untuk menyimpan dan mengelola data pengguna serta metadata *file*. Pemilihan GCP juga didasarkan pada tingkat fleksibilitas tinggi yang ditawarkan, di mana peneliti dapat menyesuaikan konfigurasi layanan sesuai dengan kebutuhan spesifik sistem, baik dari sisi skala, integrasi *Application Programming Interface* (API), hingga kontrol akses. GCP menyediakan antarmuka yang ramah pengguna serta dokumentasi yang lengkap, sehingga memudahkan proses pengembangan khususnya pada proyek dengan skala kecil hingga menengah. Dengan pendekatan ini, diharapkan solusi yang dihasilkan dapat memberikan kontribusi nyata terhadap tantangan keamanan dan efisiensi data di era digital, baik bagi pengguna individu maupun organisasi.

1.2 Rumusan Masalah Penelitian

Berdasarkan latar belakang yang telah diuraikan, permasalahan utama yang akan dibahas pada penelitian ini antara lain.

1. Bagaimana cara merancang sebuah aplikasi web berbasis *cloud* yang mengintegrasikan algoritma kriptografi AES-256 dengan teknik kompresi Deflate?
2. Bagaimana kinerja algoritma kompresi Deflate dalam mengecilkan ukuran *file* biner yang akan dienkripsi?
3. Bagaimana kinerja algoritma AES-256 dalam mengamankan *file* yang diunggah?

1.3 Tujuan Penelitian

Berdasarkan Rumusan masalah yang telah diuraikan, maka tujuan dari penelitian ini antara lain.

1. Merancang aplikasi web berbasis *cloud* yang mengamankan *file* dengan mengintegrasikan algoritma AES-256 dan kompresi Deflate untuk penyimpanan yang aman dan terkompresi.
2. Mengevaluasi kinerja algoritma kompresi Deflate dalam memperkecil ukuran *file* biner sebelum proses enkripsi dilakukan.
3. Mengevaluasi kinerja algoritma AES-256 dalam mengamankan *file* yang diunggah.

1.4 Manfaat Penelitian

Berdasarkan tujuan yang telah dijelaskan sebelumnya, diharapkan penelitian ini dapat memberikan kontribusi signifikan terhadap perkembangan teknologi, khususnya dalam hal pengamanan data dan efisiensi pengelolaan *file*. Penelitian ini diharapkan dapat memberikan manfaat, antara lain:

1.4.1 Manfaat Teoritis

1. Penelitian ini memberikan kontribusi pada pengembangan teori mengenai penerapan algoritma kriptografi AES dan teknik kompresi Deflate dalam meningkatkan keamanan dan efisiensi penyimpanan *file*.
2. Menyediakan wawasan baru mengenai integrasi algoritma enkripsi dan kompresi dalam sistem pengamanan *file* berbasis web, serta bagaimana kombinasi ini dapat memperkuat perlindungan data digital.
3. Penelitian ini diharapkan dapat memperkaya literatur di bidang keamanan data dan teknologi kompresi, serta memberi landasan bagi penelitian lanjutan yang berfokus pada inovasi metode pengamanan data.

1.4.2 Manfaat Praktis

1. Bagi pengguna, penelitian ini menawarkan solusi praktis dalam melindungi data penting dengan menggunakan enkripsi AES dan kompresi Deflate, memberikan jaminan keamanan bagi pengguna yang perlu menyimpan atau mentransfer *file* secara aman dari potensi akses yang tidak sah.
2. Bagi Peneliti dan pengembang dapat memanfaatkan aplikasi ini sebagai referensi untuk merancang sistem serupa pada proyek berbasis web yang memerlukan perlindungan data sensitif, serta dapat memperdalam pemahaman

mengenai penerapan enkripsi dan kompresi dalam konteks praktis, yang dapat diterapkan dalam pengembangan sistem keamanan data di dunia nyata.

3. Bagi lembaga atau perusahaan yang menangani data sensitif, dapat mengimplementasikan aplikasi ini sebagai bagian dari upaya dalam menjaga keamanan data pengguna dan mengoptimalkan penggunaan ruang penyimpanan melalui teknik kompresi.

1.5 Ruang Lingkup Penelitian

Batasan penelitian diperlukan pada penelitian ini untuk mengarahkan fokus penelitian agar menghindari risiko meluasnya ruang lingkup penelitian yang terlalu luas. Adapun batasan penelitian ini adalah sebagai berikut:

1. Penelitian ini hanya akan berfokus pada perancangan aplikasi web berbasis *cloud* yang mengintegrasikan algoritma kriptografi AES-256 dan teknik kompresi Deflate untuk pengamanan dan efisiensi ukuran *file*.
2. Analisis kinerja akan difokuskan pada efisiensi ukuran *file*, serta kemampuan keamanan yang dihasilkan oleh kombinasi kedua teknik tersebut dalam aplikasi web berbasis *cloud*.
3. Penelitian ini membatasi pengujian pada empat format *file*, yaitu .pdf, .csv, .docx, dan .pptx.
4. Pemanfaatan layanan GCP dalam penelitian ini hanya digunakan sebagai pendukung sistem, yaitu untuk menjalankan aplikasi melalui layanan Cloud Run, menyimpan informasi pengguna melalui layanan Firestore dan menyimpan *file* yang telah diproses melalui Cloud Storage. Penelitian ini tidak membahas pengaturan keamanan lanjutan pada *cloud*, seperti pencatatan aktivitas pengguna atau pengelolaan hak akses secara terperinci, karena fokus utama diarahkan pada integrasi proses kompresi dan enkripsi dalam aplikasi web.
5. Penelitian ini akan membatasi pengujian pada *file* dengan ukuran hingga 32 MB sesuai dengan batas maksimal ukuran *request* yang ditetapkan oleh layanan Google Cloud Run. Hal ini disebabkan oleh ketentuan teknis dari platform, di mana setiap permintaan HTTP, termasuk proses unggah *file*,

tidak boleh melebihi batas tersebut. Oleh karena itu, *file* yang lebih besar dari ukuran ini tidak akan dianalisis dalam penelitian ini.

6. Penelitian ini membatasi pengujian pada *file* dengan ukuran maksimal 10 MB. Pembatasan ini disebabkan oleh keterbatasan teknis pada implementasi kode program, di mana proses konversi *file* menjadi representasi biner dan menyimpannya dalam format .txt tidak dapat menangani *file* yang berukuran lebih dari 10 MB. Jika ukuran *file* melebihi batas tersebut, proses konversi cenderung menyebabkan kegagalan eksekusi (*crash*) atau kode program tidak berjalan sebagaimana mestinya.
7. Penelitian ini tidak membahas aspek terkait model berlangganan atau *subscription* pengguna. Fokus penelitian sepenuhnya diarahkan pada perancangan dan pengujian aplikasi web berbasis *cloud* yang mengintegrasikan algoritma kompresi dan kriptografi, tanpa mempertimbangkan kebijakan, sistem pembayaran, maupun manajemen layanan berlangganan.

1.6 Struktur Organisasi Skripsi

Penulisan karya ilmiah umumnya terdiri dari lima komponen utama, yaitu pendahuluan, tinjauan pustaka, metodologi penelitian, hasil dan pembahasan, serta simpulan, dan saran. Struktur ini mengacu pada Pedoman Penulisan Karya Ilmiah Universitas Pendidikan Indonesia Tahun 2024. Setiap bagian tersebut memiliki peran yang sangat penting dalam menyusun karya ilmiah, dengan rincian sebagai berikut:

1. PENDAHULUAN

Pada bab pertama, peneliti akan menjelaskan latar belakang masalah yang mendasari penelitian, serta mengidentifikasi isu utama yang akan diangkat. Bab ini juga akan menguraikan rumusan masalah yang akan dijawab melalui penelitian, tujuan dari penelitian ini, dan manfaat yang diharapkan dari hasil yang dicapai. Selain itu, akan dibahas pula kelebihan serta keterbatasan dalam penelitian ini, dengan memberikan gambaran tentang ruang lingkup yang akan dibahas.

2. TINJAUAN PUSTAKA

Pada bab kedua ini, pembahasan difokuskan pada literatur yang relevan mengenai pengamanan data dan pengolahan *file*, yang meliputi penggunaan algoritma kriptografi AES-256 untuk enkripsi dan teknik kompresi Deflate untuk mengurangi ukuran *file*. Penelitian ini juga membahas penerapan aplikasi berbasis web untuk pengamanan *file*, sekaligus memanfaatkan teknik kompresi guna mendukung pengelolaan data yang lebih efisien. Selain itu, dijelaskan pula pemanfaatan GCP sebagai infrastruktur pendukung aplikasi, dengan penggunaan layanan Cloud Run untuk menjalankan aplikasi web, Cloud Storage untuk menyimpan *file* hasil proses, serta Firestore sebagai basis data yang menyimpan metadata file dan informasi pengguna.

3. METODOLOGI PENELITIAN

Pada bab ketiga ini, akan dijelaskan mengenai metodologi penelitian yang mencakup tahapan pengembangan aplikasi web berbasis *cloud* yang mengintegrasikan algoritma kriptografi AES-256 untuk enkripsi dan teknik kompresi Deflate untuk efisiensi ukuran *file*. Penelitian ini juga mencakup rencana analisis untuk menilai tingkat keamanan *file* melalui uji korelasi Pearson antara data asli dan terenkripsi, serta efisiensi ukuran *file* berdasarkan perbandingan ukuran *file* sebelum dan sesudah proses kompresi dan enkripsi. Metode *Design and Development* (D&D) dipilih untuk memberikan pemahaman yang jelas tentang pendekatan yang digunakan selama penelitian.

4. HASIL DAN PEMBAHASAN

Pada bab keempat akan menyajikan hasil pengujian dan implementasi aplikasi web berbasis *cloud* yang mengintegrasikan algoritma enkripsi AES-256 dan kompresi Deflate. Pembahasan mencakup evaluasi terhadap efisiensi ukuran *file*, tingkat keamanan data berdasarkan hasil enkripsi, serta kendala yang ditemui selama proses pengembangan dan bagaimana solusi diterapkan. Tujuan dari bab ini adalah untuk menilai sejauh mana sistem yang dibangun mampu menjalankan fungsi kompresi dan enkripsi secara efektif sesuai dengan tujuan penelitian.

5. SIMPULAN DAN SARAN

Pada bab terakhir ini akan merangkum temuan penelitian, memberikan kesimpulan mengenai keberhasilan aplikasi web berbasis *cloud* dalam mengamankan dan efisiensi ukuran *file*. Simpulan dirumuskan berdasarkan hasil pengujian fungsional dan teknis terhadap sistem yang dikembangkan. Selain itu, bab ini juga memuat saran yang dapat dijadikan acuan untuk pengembangan lebih lanjut terkait teknik kompresi dan enkripsi, serta penerapan aplikasi pada jenis *file* atau konteks yang lebih luas.