BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era digital saat ini, informasi telah menjadi salah satu aset paling krusial dan berharga, baik untuk individu, perusahaan, maupun lembaga pemerintahan. Transformasi ini tercermin dalam peningkatan volume transaksi dan interaksi daring yang masif. Di Indonesia, sebagai contoh, nilai transaksi perbankan digital diproyeksikan mencapai Rp 63,8 ribu triliun pada tahun 2024[1], terjadinya lonjakan signifikan yang mengindikasikan besarnya volume data sensitif yang dihasilkan, diproses, dan disimpan. Seiring dengan eskalasi nilai dan volume data, risiko terhadap keamanannya pun turut mengalami peningkatan yang mengkhawatirkan.

Lanskap ancaman siber global menunjukkan tren yang semakin serius dan merusak. Proyeksi kerugian ekonomi akibat kejahatan siber secara global diperkirakan akan menyentuh angka $10,5 triliun per tahun pada 2025.[2] Angka ini merepresentasikan transfer kekayaan ekonomi terbesar dalam sejarah, melampaui skala kerusakan yang diakibatkan oleh bencana alam dalam setahun dan lebih menguntungkan daripada perdagangan global semua jenis obat-obatan terlarang. Biaya rata-rata per insiden kebocoran data juga telah mencapai rekor tertinggi sebesar $4,88 juta pada tahun 2024, sebuah kenaikan 10% dari tahun sebelumnya.[4] Dalam konteks ini, Indonesia merupakan salah satu negara yang menghadapi tantangan keamanan siber secara signifikan. Data menunjukkan bahwa Indonesia menempati peringkat kedelapan secara global dalam jumlah insiden kebocoran data pada tahun 2023. Tingginya tingkat ancaman ini dikonfirmasi lebih lanjut oleh laporan Badan Siber dan Sandi Negara (BSSN), yang mencatat adanya 122,79 juta anomali trafik yang dapat ketahui sebagai serangan siber hanya dalam periode Januari hingga Agustus 2024.

Kerentanan infrastruktur digital di Indonesia terekspos secara dramatis melalui serangkaian insiden keamanan berskala besar yang terjadi dalam beberapa waktu terakhir. Serangan ransomware dengan varian Brain Cipher, sebuah versi baru dari LockBit 3.0, terhadap Pusat Data Nasional Sementara (PDNS) pada Juni 2024 menjadi contoh nyata.[1] Serangan ini berhasil melumpuhkan sedikitnya 210 hingga 282 layanan publik krusial, termasuk layanan imigrasi di bandara, pendaftaran siswa,

dan perizinan acara, di mana para penyerang menuntut tebusan senilai $8 juta.[1] Insiden ini diperparah oleh fakta bahwa serangan dimulai dengan penonaktifan fitur keamanan Windows Defender beberapa hari sebelumnya, yang memungkinkan malware berjalan tanpa hambatan.[1] Kritik keras dari berbagai pihak, termasuk legislatif, menyoroti kegagalan berulang dalam menanggulangi serangan siber, mempertanyakan apakah ini sekadar "kecelakaan atau kebodohan nasional" mengingat BSSN telah melaporkan ribuan insiden sebelumnya tanpa tindakan preventif yang komprehensif.

Kejadian ini bukanlah insiden yang terisolasi. Tidak lama setelahnya, pada Agustus 2024, terjadi kebocoran data yang mengkompromikan lebih dari 4,7 juta catatan milik pegawai negeri sipil (PNS) dari Badan Kepegawaian Negara (BKN). Menyusul kemudian, pada September 2024, peretas yang sama dengan nama samaran 'Bjorka' mengklaim telah membocorkan 6,6 juta data wajib pajak, termasuk informasi sensitif milik pejabat tinggi negara, dan menjualnya di forum gelap. Sektor administrasi pemerintahan secara konsisten menjadi target utama, dengan 186 dugaan insiden siber pada tahun 2023, yang mencakup 71 insiden kebocoran data terkonfirmasi. Tabel 1.1 merangkum beberapa insiden signifikan ini.

Tabel 1.1: Ringkasan Insiden Siber Signifikan di Indonesia (2023-2024)

No.	Tanggal Insiden	Target/Korban	Jenis Serangan/Insiden	Dampak
1.	Juni 2024	Pusat Data Nasional Sementara (PDNS)	Ransomware (Brain Cipher)	Gangguan layanan publik nasional (imigrasi, dll.), tuntutan tebusan $8 juta, kelumpuhan sistem.
2.	Agustus 2024	Badan Kepegawaian Negara (BKN)	Kebocoran Data	Terkomprominya 4,7 juta data pribadi pegawai negeri sipil (nama, telepon, email, dll.).
3.	September	Wajib Pajak (DJP)	Kebocoran	Terkomprominya 6,6 juta

	2024		Data (oleh 'Bjorka')	data wajib pajak, termasuk data pejabat tinggi negara.
4.	2023	Administrasi Pemerintahan	Kebocoran Data	Menjadi sektor dengan jumlah insiden kebocoran data tertinggi, sebanyak 71 insiden terkonfirmasi.
5.	Jan-Ags 2024	Umum	Anomali Trafik	BSSN mencatat 122,79 juta anomali trafik internet yang mengindikasikan serangan siber.

Rangkaian insiden terhadap infrastruktur nasional ini menunjukkan sebuah pola yang jelas dan mengkhawatirkan: ketergantungan mutlak pada sistem keamanan terpusat memiliki risiko kegagalan katastrofik. Ketika benteng pertahanan di tingkat jaringan atau pusat data berhasil ditembus, seluruh data sensitif yang tersimpan di dalamnya menjadi rentan. Lebih dari sekadar kelemahan teknis, kegagalan berulang ini yang digambarkan sebagai "kegagalan tata kelola digital" mengikis kepercayaan publik terhadap kemampuan institusi untuk melindungi data warganya. Hal ini menciptakan sebuah defisit kepercayaan yang mendalam, di mana individu merasa tidak berdaya dan ragu untuk mempercayakan informasi pribadi mereka kepada entitas mana pun.

Kondisi ini melahirkan kebutuhan psikologis dan praktis akan alat yang dapat mengembalikan kedaulatan data ke tangan pengguna. Dengan demikian, muncullah kebutuhan mendesak akan lapisan pertahanan tambahan yang terdesentralisasi, yaitu keamanan di tingkat pengguna akhir (*endpoint security*). Dengan memberdayakan individu untuk mengamankan data mereka sendiri secara

langsung di perangkat lokal, sebuah lapisan pertahanan terakhir yang independen dapat dibentuk. Aplikasi enkripsi yang diusulkan dalam penelitian ini—bersifat sumber terbuka, gratis, dan beroperasi secara lokal—secara langsung menjawab defisit kepercayaan ini dengan menyediakan instrumen pemberdayaan bagi pengguna. Pendekatan ini sejalan dengan dorongan strategis nasional untuk memperkuat kedaulatan digital melalui adopsi teknologi *open-source* yang transparan dan dapat diaudit oleh komunitas.[10]

Dalam menghadapi ancaman seperti pencurian data, peretasan, dan *malware*, enkripsi data merupakan salah satu mekanisme pertahanan proaktif yang paling fundamental dan efektif. Enkripsi adalah proses mengubah data dari format yang dapat dibaca (*plaintext*) menjadi format yang tidak dapat dibaca (*ciphertext*) tanpa kunci yang benar, sehingga melindungi kerahasiaan (*confidentiality*) informasi. Untuk mengimplementasikan solusi enkripsi yang efektif dan mudah diakses, pemilihan teknologi menjadi krusial. Bahasa pemrograman Python dipilih karena popularitasnya yang tinggi, sintaksis yang relatif mudah dipelajari, dan ekosistem pustaka pihak ketiga yang sangat kaya, terutama untuk keperluan kriptografi. Pustaka seperti cryptography menyediakan akses ke algoritma kriptografi modern yang telah teruji dan aman. Sebagai algoritma enkripsi, *Advanced Encryption Standard* (AES) dipilih karena statusnya sebagai standar industri global. AES diadopsi oleh pemerintah Amerika Serikat untuk melindungi informasi hingga tingkat "Top Secret" dan telah terbukti tangguh terhadap berbagai jenis serangan kriptanalisis.[1]

Meskipun banyak berbagai perangkat lunak enkripsi, adopsi oleh masyarakat umum sering kali terhambat oleh kompleksitas teknis dan antarmuka yang tidak ramah pengguna. Alat enkripsi klasik seperti PGP secara historis sulit digunakan oleh pengguna non-teknis. Menyadari hal ini, tren industri perangkat lunak keamanan saat ini bergerak menuju "User-Centric Design," di mana kemudahan penggunaan menjadi fitur utama. Produk seperti NordLocker dan Kruptos 2 Professional secara eksplisit menonjolkan antarmuka yang sederhana, seperti mekanisme *drag-and-drop*, untuk menjangkau audiens yang lebih luas.

Celah inilah yang ingin diisi oleh penelitian ini: mengembangkan sebuah aplikasi enkripsi file berbasis desktop yang tidak hanya aman secara teknis dengan menerapkan praktik kriptografi modern (AES-GCM), tetapi juga dirancang dengan antarmuka yang intuitif khusus untuk pengguna non-teknis di Indonesia. Dengan demikian, penelitian ini bertujuan untuk menghasilkan alat yang bersifat sumber terbuka (*open-source*), tidak memerlukan biaya, dan dapat diadopsi oleh kalangan yang lebih luas untuk melindungi aset data digital mereka secara mandiri.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, masalah utama dalam penelitian ini dapat dirumuskan ke dalam beberapa pertanyaan penelitian yang spesifik sebagai berikut:

Contoh:

1. Bagaimana merancang dan membangun sebuah aplikasi desktop menggunakan bahasa pemrograman Python dan pustaka cryptography untuk melakukan enkripsi dan dekripsi file secara aman dan efisien?
2. Bagaimana mengimplementasikan algoritma kriptografi simetris Advanced Encryption Standard (AES) dengan mode operasi modern yang menyediakan enkripsi terotentikasi (seperti GCM) untuk menjamin kerahasiaan dan integritas data secara simultan?
3. bagaimana merancang antarmuka pengguna grafis (GUI) yang intuitif menggunakan pustaka Tkinter agar proses enkripsi, dekripsi, dan manajemen kunci dapat dioperasikan dengan mudah oleh pengguna dengan latar belakang teknis yang minimal?
4. Bagaimana mengevaluasi efektivitas fungsional dan kinerja aplikasi yang dikembangkan melalui serangkaian skenario pengujian black-box dan white-box?

1.3 Batasan Masalah

Untuk menjaga agar penelitian tetap fokus dan mendalam, ruang lingkup penelitian ini dibatasi pada aspek-aspek berikut :

1. Algoritma Kriptografi: Penelitian ini secara eksklusif berfokus pada implementasi algoritma kriptografi simetris Advanced Encryption Standard (AES). Algoritma lain seperti RSA, DES, atau ECC tidak akan diimplementasikan dan hanya akan dibahas secara teoretis sebagai perbandingan.
2. Platform dan Pustaka: Aplikasi akan dikembangkan secara murni menggunakan bahasa pemrograman Python (versi 3.x). Pustaka utama yang digunakan adalah cryptography untuk logika inti enkripsi dan Tkinter untuk pengembangan antarmuka pengguna grafis (GUI).
3. Jenis File yang Didukung: Aplikasi dirancang untuk dapat menangani berbagai jenis file biner umum (misalnya, dokumen teks.txt, gambar.jpg, dokumen PDF.pdf, dokumen Word.docx). Tidak ada optimasi khusus yang dilakukan untuk format file tertentu.
4. Manajemen Kunci: Mekanisme manajemen kunci yang diimplementasikan bersifat dasar, yaitu pengguna memasukkan kata sandi yang kemudian akan diproses oleh Key Derivation Function (KDF) untuk menghasilkan kunci enkripsi. Sistem manajemen kunci yang lebih kompleks, seperti distribusi kunci melalui jaringan, penggunaan key server, atau integrasi dengan Hardware Security Module (HSM), berada di luar cakupan penelitian ini.
5. Lingkup Pengujian: Pengujian kinerja akan difokuskan pada pengukuran waktu proses enkripsi dan dekripsi untuk file dengan ukuran yang representatif (misalnya, kecil <1 MB, sedang 1-50 MB, besar 50-200 MB) yang dijalankan pada lingkungan komputasi lokal. Analisis kinerja dalam skenario jaringan atau pada file dengan ukuran sangat besar (skala terabyte) tidak akan dilakukan.

1.4 Tujuan Penelitian

Sejalan dengan rumusan masalah yang telah ditetapkan, tujuan dari penelitian ini adalah sebagai berikut :

1. Menghasilkan sebuah perangkat lunak aplikasi enkripsi file yang fungsional, berbasis desktop dengan Python, yang mengimplementasikan algoritma AES secara benar dan aman.
2. Menerapkan mode operasi AES modern yang bersifat *Authenticated Encryption with Associated Data* (AEAD), yaitu *Galois/Counter Mode* (GCM), untuk memberikan jaminan keamanan ganda: kerahasiaan dan integritas data.
3. Membangun sebuah antarmuka pengguna (GUI) yang sederhana, bersih, dan intuitif, yang memfasilitasi penggunaan aplikasi oleh audiens yang luas, termasuk mereka yang tidak memiliki keahlian teknis.
4. Melakukan verifikasi dan validasi terhadap aplikasi yang dikembangkan melalui metode pengujian *black-box* dan *white-box* untuk memastikan bahwa aplikasi berfungsi sesuai dengan spesifikasi fungsional dan bebas dari kesalahan kritis.

Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat baik secara teoretis maupun praktis. Sebagai berikut:

1.4.1 Manfaat Teoretis

1. Menyediakan studi kasus yang komprehensif mengenai implementasi praktis konsep kriptografi modern (AES-GCM) menggunakan bahasa Python dan pustaka cryptography.
2. Menyajikan analisis perbandingan dan justifikasi pemilihan metodologi pengembangan perangkat lunak (Model Prototype) untuk proyek sejenis yang menyeimbangkan antara kompleksitas teknis dan kebutuhan antarmuka pengguna.
3. Dapat menjadi bahan referensi akademis bagi mahasiswa dan peneliti lain yang tertarik pada bidang keamanan data dan kriptografi terapan.

1.4.2 Manfaat Praktis

1. Menghasilkan sebuah produk perangkat lunak enkripsi yang bersifat open-source dan dapat digunakan secara bebas oleh individu, jurnalis, aktivis, atau organisasi skala kecil untuk meningkatkan keamanan data digital mereka.
2. Menawarkan alternatif keamanan yang terdesentralisasi dan dapat dipercaya di tengah menurunnya kepercayaan pada sistem terpusat, memberikan pengguna alat untuk mengontrol keamanan data mereka sendiri.
3. Meningkatkan kesadaran dan literasi digital mengenai pentingnya enkripsi sebagai alat pertahanan siber di tingkat personal. Upaya ini sejalan dengan program-program edukasi keamanan siber yang bertujuan memberdayakan masyarakat untuk melindungi diri dari ancaman digital seperti pencurian data dan penipuan daring. Aplikasi ini dapat berfungsi sebagai alat praktis bagi masyarakat untuk menerapkan pengetahuan yang mereka peroleh dari program literasi tersebut.

1.5 Sistematika Penulisan

Skripsi ini disusun untuk menyajikan hasil penelitian yang dilakukan. Pendahuluan dimulai dengan latar belakang penelitian untuk menggambarkan konteks dan alasan pemilihan topik. Selanjutnya, Rumusan masalah digunakan untuk mengidentifikasi permasalahan yang akan diselesaikan. Tujuan penelitian disampaikan untuk menjelaskan tujuan yang ingin dicapai melalui penelitian ini. Manfaat penelitian dijelaskan untuk menggambarkan manfaat penelitian ini dalam pengembangan ilmu pengetahuan dan praktik terkait. Dalam tinjauan pustaka, terdapat studi literatur dan dasar teori. Studi literatur mencakup penelitian-penelitian yang sudah dilakukan sebelumnya. Pada bagian ini, peneliti memberikan tinjauan umum tentang topik penelitian, merangkum penelitian-penelitian terkait, dan menyoroti temuan utama, metodologi, dan hasil dari penelitian-penelitian tersebut. Sementara itu, bagian dasar teori menjelaskan dasar teoretis yang digunakan dalam penelitian. Pada bagian ini, peneliti menjelaskan teori-teori yang relevan dengan topik penelitian, konsep-konsep yang terkait

Metode penelitian meliputi alur penelitian, dan alat dan bahan yang digunakan. Alur penelitian menjelaskan langkah-langkah yang akan diambil dalam penelitian. Alat dan bahan menjelaskan tentang peralatan, instrumen yang akan digunakan dalam penelitian. Hasil dan pembahasan mencakup beberapa komponen penting, seperti analisis sistem berjalan, diagram, kamus data, struktur tabel, dan pengujian sistem. Analisis sistem berjalan dilakukan untuk mengetahui permasalahan yang sebenarnya. Diagram digunakan untuk memvisualisasikan struktur dan alur sistem. Pengujian sistem merupakan tahap evaluasi dan verifikasi terhadap sistem yang telah dikembangkan. Kesimpulan memberikan ringkasan dari hasil penelitian yang telah dilakukan. Sedangkan saran menjelaskan bagian yang memberikan rekomendasi dan panduan untuk penelitian selanjutnya atau pengembangan lebih lanjut. Referensi dalam penulisan mencakup berbagai sumber yang digunakan, seperti buku, jurnal, artikel, dan sumber elektronik.