BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan proses perancangan, implementasi, dan pengujian yang telah dilakukan, penelitian ini berhasil mencapai semua tujuan yang telah ditetapkan. Kesimpulan utama dapat ditarik dengan menjawab setiap pertanyaan dalam rumusan masalah:

1. Telah berhasil dirancang dan dibangun sebuah aplikasi desktop fungsional menggunakan Python dan pustaka cryptography. Aplikasi ini mampu melakukan enkripsi dan dekripsi file dari berbagai format secara efisien, dengan arsitektur 3-lapis yang memisahkan logika antarmuka, kontrol, dan kriptografi, menghasilkan kode yang terstruktur dan dapat dipelihara.
2. Telah berhasil diimplementasikan algoritma AES dengan mode operasi GCM (AES-GCM). Implementasi ini tidak hanya memberikan jaminan kerahasiaan melalui enkripsi AES-256 yang kuat, tetapi juga jaminan integritas dan otentikasi melalui authentication tag yang melekat pada mode GCM. Pengujian (khususnya BB-TAMPER-01) secara empiris memvalidasi bahwa setiap modifikasi pada file terenkripsi akan terdeteksi, sehingga memenuhi klaim keamanan ganda.
3. Telah berhasil dirancang sebuah antarmuka pengguna grafis (GUI) yang intuitif menggunakan Tkinter. Melalui desain minimalis dan alur kerja tiga langkah yang jelas, aplikasi ini terbukti mudah dioperasikan oleh pengguna dengan latar belakang teknis minimal, seperti yang divalidasi melalui pengujian usabilitas (BB-USABILITY-01). Ini secara efektif mengatasi salah satu hambatan utama adopsi enkripsi.
4. Telah berhasil dievaluasi efektivitas fungsional dan kinerja aplikasi melalui pengujian black-box dan white-box. Hasil pengujian menunjukkan bahwa semua fungsi berjalan sesuai spesifikasi, penanganan error bekerja dengan baik, dan kinerja aplikasi sangat efisien, bahkan untuk file berukuran besar.

Secara keseluruhan, penelitian ini telah menghasilkan sebuah produk perangkat lunak enkripsi file yang fungsional, aman, dan intuitif. Produk ini berhasil mengisi

celah spesifik dalam lanskap perangkat lunak keamanan yang tersedia untuk pengguna di Indonesia, dengan menawarkan solusi sumber terbuka yang memberdayakan individu untuk melindungi data mereka secara mandiri di tengah meningkatnya ancaman siber dan menurunnya kepercayaan pada sistem keamanan terpusat.

5.2 Saran

Berdasarkan temuan dan keterbatasan yang diidentifikasi dalam penelitian, berikut adalah beberapa saran konkret yang dapat ditindaklanjuti untuk pengembangan aplikasi di masa depan:

Berdasarkan temuan dan keterbatasan yang diidentifikasi dalam penelitian, berikut adalah beberapa saran konkret yang dapat ditindaklanjuti untuk pengembangan aplikasi di masa depan:

1. Manajemen Kunci Lanjutan: Untuk meningkatkan kegunaan aplikasi di lingkungan tim atau organisasi, disarankan untuk mengeksplorasi sistem manajemen kunci yang lebih canggih. Ini bisa mencakup implementasi kriptografi kunci publik (misalnya, RSA) untuk pertukaran kunci sesi yang aman, atau integrasi dengan layanan manajemen rahasia terpusat seperti HashiCorp Vault atau Hardware Security Modules (HSM) untuk penyimpanan kunci yang sangat aman.[17]
2. Distribusi dan Dukungan Lintas Platform: Untuk menghilangkan hambatan instalasi bagi pengguna non-teknis, disarankan untuk mengemas aplikasi menjadi file eksekutable (standalone executable) untuk setiap sistem operasi target (Windows, macOS, Linux) menggunakan alat seperti PyInstaller atau cx_Freeze. Ini akan memungkinkan distribusi yang jauh lebih mudah dan tidak memerlukan pengguna untuk menginstal Python secara terpisah.
3. Penambahan Fitur Fungsional: Aplikasi dapat diperkaya dengan fitur-fitur yang akan meningkatkan nilainya bagi pengguna, seperti:
   a. Enkripsi Direktori: Menambahkan kemampuan untuk mengenkripsi seluruh folder dan isinya secara rekursif.
   b. Penghapusan Aman (Secure Wipe): Menambahkan opsi untuk menghapus file asli secara aman setelah enkripsi berhasil, dengan menimpanya

beberapa kali untuk mencegah pemulihan.

c. Integrasi Penyimpanan Awan: Mengintegrasikan aplikasi dengan API dari layanan penyimpanan awan populer (seperti Google Drive atau Dropbox) untuk memungkinkan enkripsi file sebelum diunggah.

4. Menghadapi Ancaman Masa Depan: Lanskap ancaman siber terus berkembang. Mengingat tren keamanan siber untuk tahun 2025 yang menyoroti ancaman dari kecerdasan buatan generatif (Gen-AI) dan supply chain attacks [19], penelitian di masa depan dapat mengeksplorasi cara-cara untuk memperkuat aplikasi. Ini bisa mencakup analisis terhadap potensi serangan rekayasa sosial yang difasilitasi AI atau memastikan semua dependensi perangkat lunak (seperti pustaka cryptography) diverifikasi untuk mencegah serangan supply chain.
5. Audit Keamanan Formal dan Pengembangan Komunitas: Untuk membangun kepercayaan tertinggi, sangat disarankan agar versi aplikasi di masa depan menjalani audit keamanan profesional oleh pihak ketiga yang independen. Selain itu, dengan merilis kode sebagai proyek open-source yang terdokumentasi dengan baik, penelitian ini dapat mendorong terbentuknya komunitas pengembang yang dapat berkontribusi pada pemeliharaan, penambahan fitur, dan peninjauan keamanan secara berkelanjutan.