BAB V
SIMPULAN DAN SARAN

5.1 Simpulan

Berdasarkan hasil penelitian dan pengujian pada pengembangan aplikasi enkripsi file menggunakan AES-128 sebagai solusi keamanan data di cloud yang sudah dilakukan, dapat disimpulkan beberapa hal sebagai berikut:

1. Pengembangan aplikasi *desktop* untuk enkripsi dan dekripsi file menggunakan algoritma AES berhasil dilakukan melalui pendekatan metode *Design and Development* (D&D). Aplikasi dikembangkan menggunakan bahasa pemrograman Java dengan SQLite sebagai basis data lokal, serta Google Drive API untuk integrasi *cloud*. Serta, proses pengembangan dilakukan secara bertahap menggunakan pendekatan *Agile*. Hasilnya, aplikasi dapat dibangun sesuai rancangan dan dapat diuji secara fungsional.
2. Algoritma AES menunjukkan kinerja yang baik dalam menjaga keamanan dan efisiensi file terenkripsi, sebagaimana dibuktikan melalui uji coba pada berbagai jenis dan ukuran file. File hasil enkripsi tidak menunjukkan keterbacaan atau pola tertentu, yang mengindikasikan keberhasilan dalam aspek keamanan. Seperti yang ditunjukkan pada pengujian *Pearson* bahwa tidak terdapat korelasi linear yang signifikan antara *byte* pada file asli dan hasil enkripsinya, karena rata-rata nilai (r) berkisar 0.00461 yang mana mendekati nol pada semua file yang diuji. Dari segi efisiensi, ukuran file sebelum dan sesudah enkripsi tidak mengalami perubahan yang signifikan, sehingga tidak membebani kapasitas penyimpanan lokal maupun cloud dan tetap layak digunakan untuk integrasi dalam aplikasi desktop.

5.2 Saran

Berdasarkan hasil penelitian dan simpulan yang diperoleh, terdapat beberapa saran yang dapat diterapkan untuk mengembangkan aplikasi ini menjadi lebih optimal, diantaranya:

1. Aplikasi saat ini hanya mendukung enkripsi dan dekripsi untuk file dengan format PDF, XLSX, dan DOCX. Penelitian selanjutnya dapat memperluas dukungan terhadap format lain seperti JPG, PNG, ZIP, MP4, dan lainnya, agar lebih fleksibel untuk kebutuhan pengguna yang beragam.
2. Aplikasi masih berjalan pada platform *desktop* berbasis Windows. Disarankan agar pengembangan berikutnya mencakup platform lain seperti Android, iOS, atau versi berbasis web untuk memperluas jangkauan pengguna dan meningkatkan fleksibilitas penggunaan.
3. Meskipun berdasarkan pengujian AES-128 telah terbukti aman dan efisien, sistem dapat dikembangkan lebih lanjut dengan mengkombinasikan dengan algoritma lain, seperti RSA untuk manajemen kunci, atau algoritma tambahan lainnya.