UNIVERSITAS
MUHAMMADIYAH
SIDOARJO

UMSIDA
DARI SINI PENCERAHAN BERSEMI

Aplikasi Keamanan Berkas dengan Enkripsi AES dan Biometrik Sidik Jari Berbasis Android

Oleh:

Habib Husain Amirullah

Ade Eviyanti

Informatika

Universitas Muhammadiyah Sidoarjo

Januari, 2024

Pendahuluan

Dalam era digital saat ini, keamanan data menjadi prioritas utama mengingat masih sering terjadi kasus pencurian data digital. Biaya rata-rata dari data breach mencapai $3.86 juta pada tahun 2018. Kriptografi, khususnya enkripsi, menjadi solusi untuk menjaga kerahasiaan dan integritas dokumen.

Advanced Encryption Standard (AES) adalah standar terkini yang telah diadopsi oleh pemerintah AS, dan menjadi pilihan utama di seluruh dunia untuk mengamankan informasi rahasia. AES mengubah plaintext menjadi ciphertext yang sulit dipecahkan, hanya dapat dibaca kembali dengan kunci dekripsi yang tepat.

Pendahuluan

Meskipun AES umum digunakan, risiko kunci lemah dan kelalaian pengguna dalam mengelola kunci menjadi masalah. Oleh karena itu, metode autentikasi canggih, aman, dan mudah digunakan diperlukan untuk mengamankan akses ke data yang dienkripsi.

Salah satu solusi yang muncul adalah verifikasi biometrik, khususnya sidik jari, sebagai bentuk autentikasi pengguna. Sidik jari unik untuk setiap individu, bersifat tidak dapat ditebak, dan tidak berubah seumur hidup. Dengan memahami risiko keamanan, penelitian ini mengembangkan aplikasi keamanan berkas dengan enkripsi AES128 dan autentikasi sidik jari berbasis Android, diharapkan dapat memberikan kontribusi positif dalam meningkatkan keselamatan dan keamanan data di era digital saat ini.

Pertanyaan Penelitian (Rumusan Masalah)

1. Bagaimana solusi teknologi terkini dapat digunakan untuk meningkatkan keamanan data dan mencegah akses yang tidak sah pada dokumen digital?

2. Bagaimana merancang dan mengembangkan aplikasi berbasis Android untuk melakukan enkripsi data menggunakan algoritma AES-128?

3. Bagaimana implementasi dan penggunaan sidik jari sebagai metode verifikasi pengguna di aplikasi Android?

Metode

Studi Literatur dan Analisis

Studi literatur dimulai dengan melakukan pencarian artikel jurnal terkait dengan pengembangan Aplikasi Keamanan Berkas dengan Enkripsi AES dan Biometrik Sidik Jari melalui Google Scholar. Tahap berikutnya melibatkan riset dan identifikasi cakupan area penelitian yang dieksplorasi.

Desain Sistem

Proses desain sistem diawali dengan penyusunan *Proof of Concept*, diikuti oleh perancangan *Flowchart*, Diagram *Use Case*, dan terakhir, pembuatan Desain *User Interface*.

Metode

Implementasi

Dalam tahap implementasi, dilakukan eksekusi dari konsep desain yang telah dirancang sebelumnya pada tahap perancangan sistem. Pelaksanaan ini mencakup pengembangan aplikasi Android dengan memanfaatkan framework Jetpack Compose.

Evaluasi

Tahap evaluasi melibatkan uji coba secara otomatis (Automated Testing) dengan menggunakan skrip pengujian. Proses pengujian ini dirancang untuk mengidentifikasi kinerja, keandalan, dan keberlanjutan aplikasi Android yang telah dikembangkan.

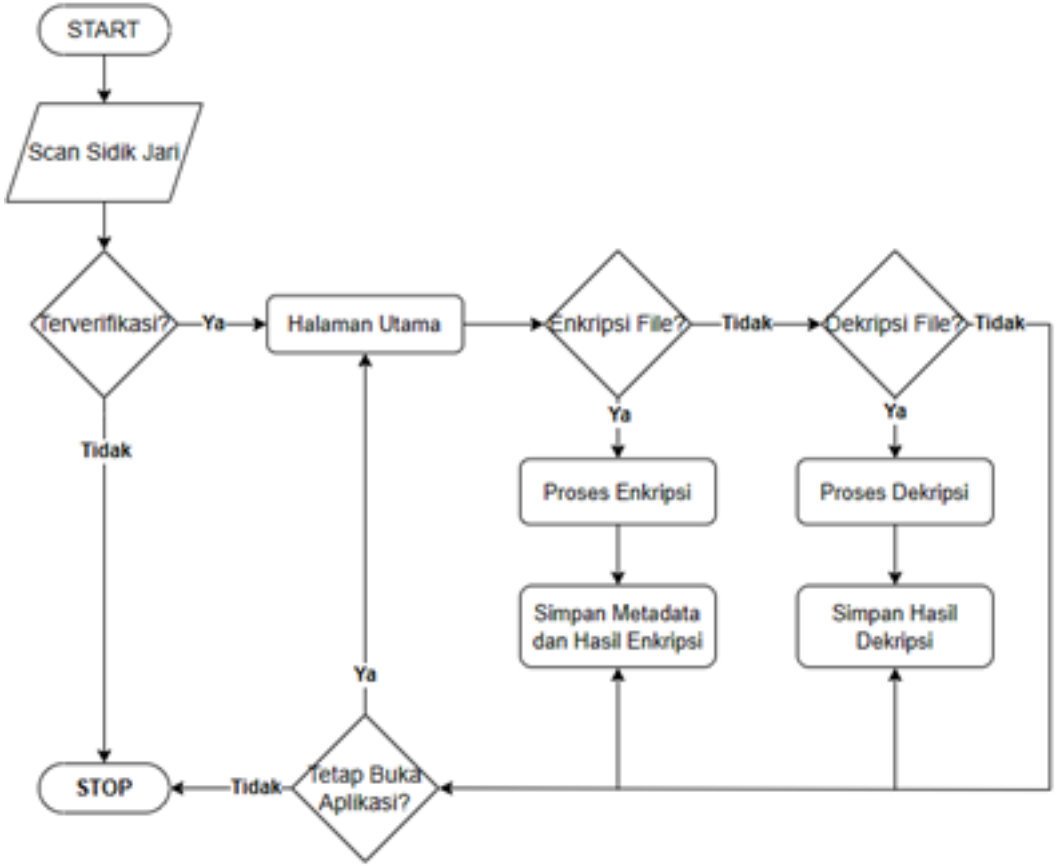
Metode

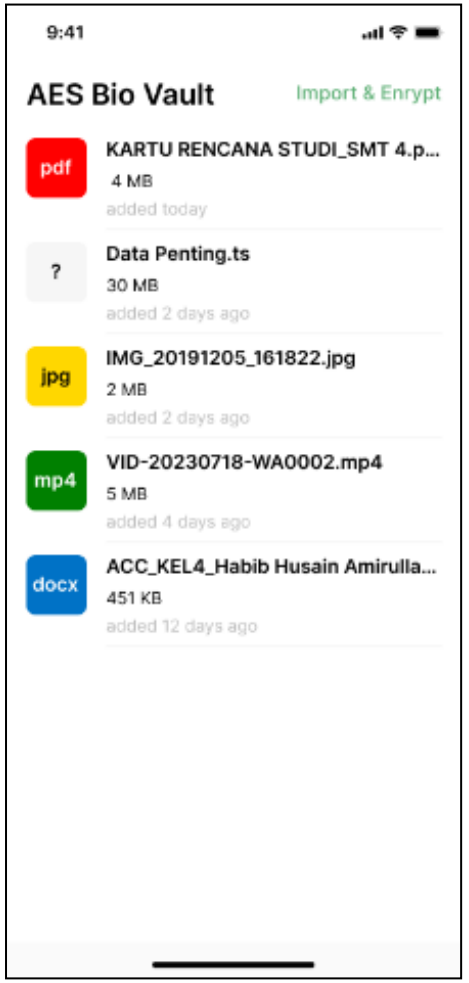
Deployment

Tahap akhir, yakni deployment, dilakukan setelah aplikasi melewati evaluasi sukses. Pada tahap ini, Aplikasi Keamanan Berkas Android dengan Enkripsi AES dan Biometrik Sidik Jari disiapkan untuk dirilis dan digunakan oleh pengguna. Aplikasi yang telah siap dapat diunggah ke PlayStore atau dipublikasikan melalui Github Release, tergantung pada pertimbangan dana rilis di PlayStore.

Hasil

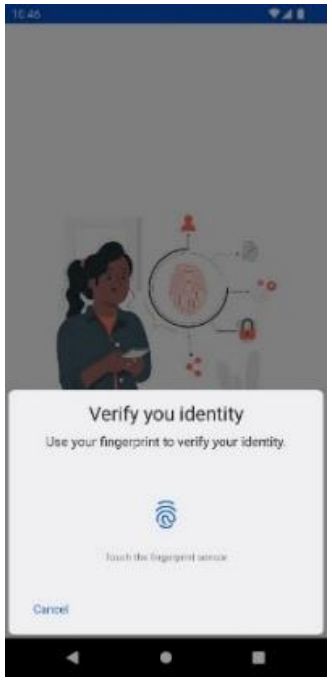
Flowchart dan Desain Interface:





Hasil

Implementasi Aplikasi :

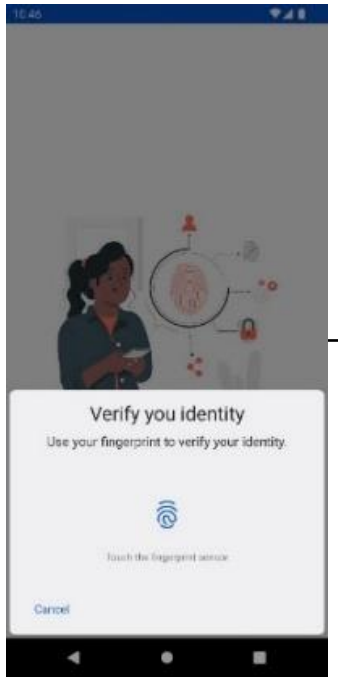


Halaman Login

Halaman Utama

Pembahasan

Halaman Login:



Halaman Login

Gagal Memverifikasi Sidik Jari

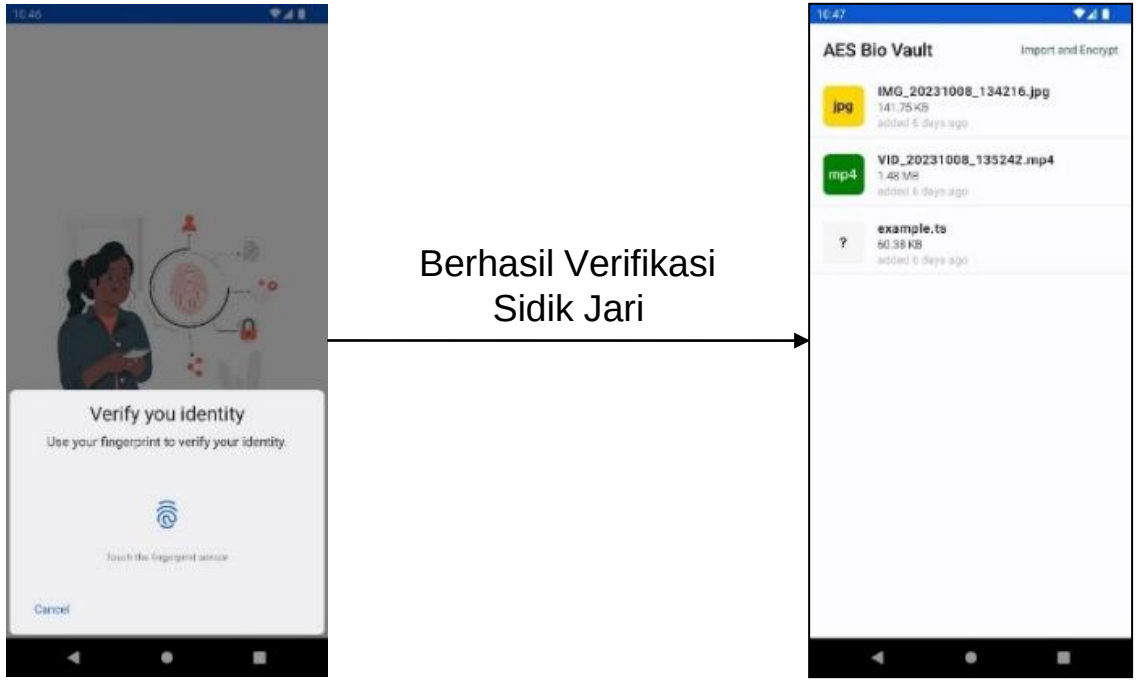
Pesan Gagal Verifikasi Sidik Jari

Di Halaman Login, pengguna diminta untuk melakukan pemindaian sidik jari yang sebelumnya telah didaftarkan. Sidik jari yang dapat diverifikasi adalah yang sudah tercatat dalam sistem Biometrik Android. Proses verifikasi tersebut memastikan bahwa hanya sidik jari yang terdaftar sebelumnya yang dapat diakui oleh sistem sebagai sah.

Apabila sidik jari gagal terverifikasi, sebuah pesan akan segera muncul, memberi tahu pengguna mengenai kegagalan verifikasi. Pesan ini dirancang untuk memberikan informasi yang jelas dan memberikan petunjuk yang mungkin diperlukan oleh pengguna untuk menyelesaikan masalah.

Pembahasan

Halaman Login:



Halaman Login

Halaman Utama

Jika sidik jari berhasil diverifikasi, langkah berikutnya adalah diarahkan ke Halaman Dashboard. Setelah proses verifikasi sukses, pengguna akan diizinkan untuk mengakses dan menjelajahi berbagai fitur serta informasi yang tersedia pada dashboard aplikasi. Hal ini menciptakan pengalaman pengguna yang lancar dan memberikan akses instan ke fungsionalitas utama dari aplikasi Keamanan Berkas dengan Enkripsi AES dan Biometrik Sidik Jari Berbasis Android.

Pembahasan

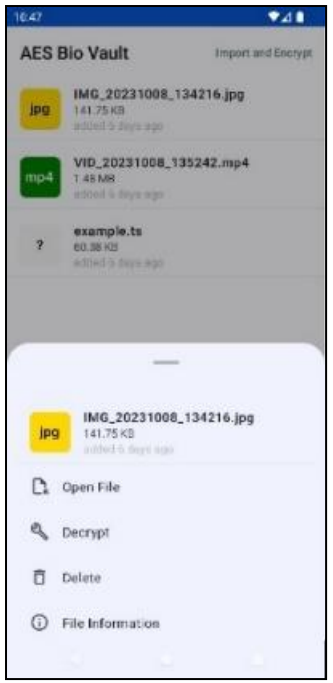
Halaman Utama:

Halaman Utama

Pada halaman utama, terdapat daftar berkas yang telah berhasil dienkripsi. Di bagian pojok kanan atas, terdapat tombol yang memungkinkan pengguna untuk menambahkan atau melakukan enkripsi berkas baru. Fasilitas ini dirancang untuk memberikan kemudahan akses dan kontrol penuh kepada pengguna dalam mengelola berkas-berkas yang akan dienkripsi atau ditambahkan ke dalam sistem. Selain itu, apabila salah satu berkas dalam daftar ditekan, akan muncul bottom sheet yang memuat opsi dan pengaturan terkait berkas sesuai dengan preferensi dan kebutuhan pengguna.

Pembahasan

Halaman Utama:



Tampilan Bottom Sheet

Bottom Sheet Berisi operasi yang dapat dilakukan pada sebuah berkas yang dipilih. Operasi tersebut antara lain:

1. *Open File* : Opsi untuk membuka berkas. Berkas harus terlebih dahulu didekripsi sebelum bisa dibuka.

2. *Decrypt* : Opsi untuk melakukan dekripsi berkas, berkas yang sudah didekripsi akan otomatis terkunci kembali setelah 10 menit.

3. *Delete* : Opsi untuk menghapus berkas dari penyimpanan internal aplikasi.

4. *File Information* : Opsi untuk melihat detail dari berkas yang tersimpan, termasuk informasi mengenai ukuran dan lokasi setelah didekripsi.

Pembahasan

Halaman Utama:

Halaman Utama Setelah Salah Satu File Berhasil Didekripsi

Setelah sebuah berkas berhasil didekripsi, daftar berkas tersebut akan berubah warna menjadi merah, menandakan bahwa berkas tersebut sedang dalam kondisi terdekripsi. Selanjutnya, akan muncul informasi terkait "Decrypted Until" yang menunjukkan hingga kapan berkas tersebut akan tetap dalam kondisi terdekripsi sebelum dienkripsi kembali secara otomatis oleh sistem.

Temuan Penting Penelitian

Secara bawaan, kelas EncryptedFile pada platform Android hanya mensupport algoritma AES-256. Oleh karena itu, jika terdapat kebutuhan untuk menggunakan algoritma AES-128, perlu dilakukan beberapa penyesuaian pada kode sumber kelas EncryptedFile. Sementara opsi modifikasi kode ini tersedia, untuk mempermudah proses pengembangan dan menjaga keseragaman, disarankan agar penelitian berikutnya mempertimbangkan penggunaan algoritma AES-256. Hal ini tidak hanya meminimalkan kerumitan dalam penyesuaian kode sumber, tetapi juga menjaga konsistensi dalam penerapan keamanan pada level file enkripsi di lingkungan Android.

Manfaat Penelitian

Tujuan dan manfaat penelitian ini adalah untuk mengatasi tantangan keamanan data pada era digital dengan mengembangkan sebuah aplikasi berbasis Android yang menggunakan algoritma AES-128 untuk melakukan enkripsi data. Aplikasi ini mengintegrasikan metode verifikasi sidik jari sebagai lapisan keamanan tambahan guna mencegah akses yang tidak sah pada dokumen digital. Penelitian ini bertujuan untuk menyediakan solusi yang efisien dan efektif dalam melindungi data pengguna dan mengamankan dokumen dalam bentuk digital agar hanya dapat diakses oleh pemiliknya dengan keamanan terjamin.

Referensi

[1] E. M. De Los Reyes, A. M. Sison, and R. P. Medina, "File encryption based on reduced-round AES with revised round keys and key schedule," Indones. J. Electr. Eng. Comput. Sci., vol. 16, no. 2, pp. 897–905, 2019, doi: 10.11591/ijeecs.v16.i2.pp897-905.

[2] B. E. Widodo and A. S. Purnomo, "Implementasi Advanced Encryption Standard Pada Enkripsi Dan Dekripsi Dokumen Rahasia Ditintelkam Polda Diy," J. Tek. Inform., vol. 1, no. 2, pp. 69–77, 2020, doi: 10.20884/1.jutif.2020.1.2.21.

[3] D. Wong, Real-World Cryptography. Manning Publications, 2021.

[4] D. Selent, "ADVANCED ENCRYPTION STANDARD," RIVIER Acad. J., vol. 6, no. 2, 2010.

[5] A. Prameshwari and N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," Eksplora Inform., vol. 8, no. 1, p. 52, 2018, doi: 10.30864/eksplora.v8i1.139.

[6] K. Muttaqin and J. Rahmadoni, "Analysis and Design of File Security System Aes (Advanced Encryption Standard) Cryptography Based," J. Appl. Eng. Technol. Sci., vol. 1, no. 2, pp. 113–123, 2020, doi: 10.37385/jaets.v1i2.78.

[7] E. Setyaningsih, "Keamanan file dokumen menggunakan algoritme Advanced Encryption Standard pada aplikasi berbasis Android," Jnanaloka, pp. 11–23, Apr. 2020, doi: 10.36802/jnanaloka.2020.v1- no1-13.

[8] A. I. Suranta and D. V. S. Y. Sakti, "Penerapan Algoritma Aes (Advance Encryption Standart) 128 Untuk Enkripsi Dokumen Di Pt. Gunung Geulis Elok Abadi," Skanika, vol. 5, no. 1, pp. 1–10, 2022, doi: 10.36080/skanika.v5i1.2118.

[9] Y. H. Jo, S. Y. Jeon, J. H. Im, and M. K. Lee, "Security analysis and improvement of fingerprint authentication for smartphones," Mob. Inf. Syst., vol. 2016, no. Krait 400, 2016, doi: 10.1155/2016/8973828.

Referensi

[10] S. Iqbal et al., "A novel mobile wallet model for elderly using fingerprint as authentication factor," IEEE Access, vol. 8, pp. 177405–177423, 2020, doi: 10.1109/ACCESS.2020.3025429.

[11] M. Fahmi Shamsudin and N. Hidayah Ab Rahman, "An Authentication of Carpooling Apps Using OTP and Fingerprint," Appl. Inf. Technol. Comput. Sci., vol. 2, no. 1, pp. 1–10, 2021, [Online]. Available: https://publisher.uthm.edu.my/periodicals/index.php/aitcs/article/view/480

[12] B. Acharya and K. Sahu, "Software Development Life Cycle Models: A Review Paper," Int. J. Adv. Res. Eng. Technol., vol. 11, no. 12, pp. 169–176, 2020, doi: 10.34218/IJARET.11.12.2020.019.

[13] H. Himawan and M. Yanu F, Interface USER EXPERIENCE. 2020.

[14] N. Smyth, Android Studio 3.0 Development Essentials Android 8 Edition. Payload Media, 2017.

[15] R. B. D. Putra, E. S. Budi, and A. R. Kadafi, "Perbandingan Antara SQLite, Room, dan RBDLiTe Dalam Pembuatan Basis Data pada Aplikasi Android," JURIKOM (Jurnal Ris. Komputer), vol. 7, no. 3, p. 376, 2020, doi: 10.30865/jurikom.v7i3.2161.

[16] P. Kong, L. Li, J. Gao, K. Liu, T. F. Bissyandé, and J. Klein, "Automated testing of Android apps: A systematic literature review," IEEE Trans. Reliab., vol. 68, no. 1, pp. 45–66, 2019, doi: 10.1109/TR.2018.2865733


UMSIDA
DARI SINI PENCERAHAN BERSEMI