e-ISSN 2549-7472
Edumatic: Jurnal Pendidikan Informatika
Vol. 7 No. 2, Desember, 2023, **Hal. 485-494**
DOI: 10.29408/edumatic.v7i2.23948

Aplikasi Pengamanan Data Karyawan menggunakan Algoritma *Advanced Encryption Standard* dan *Cloud Computing* berbasis *Mobile*

Adi Kannatasik [1,*] , Moh. Ali Romli [1]
[1] Progam Studi Informatika, Universitas Teknologi Yogyakarta, Indonesia
[*] Correspondence: adi.kannatasik@gmail.com

Received: 5 November 2023 | Revised: 7 November 2023 | Accepted: 22 November 2023 | Published: 20 Desember 2023

Abstrak
Dokumen merupakan aset berharga yang sering berisi informasi penting, termasuk data pribadi karyawan, dan rentan terhadap ancaman keamanan seperti pencurian dan perubahan oleh pihak yang tidak berwenang. Penelitian ini bertujuan mengembangkan aplikasi keamanan dokumen berbasis Android yang menggabungkan algoritma *Advanced Encryption Standard* (*AES*) dan teknologi *Cloud Computing*. Jenis penelitian ini adalah pengembangan dengan menggunakan model System *Development Life Cycle (SDLC)*, yang melibatkan analisis kebutuhan, desain, pengkodean, dan pengujian. Pada tahapan analisis kebutuhan, fokus diberikan pada data karyawan yang perlu diamankan. Desain sistem mencakup struktur data, struktur sistem, dan antarmuka pengguna (UI). Rancangan sistem mencakup elemen *use case, class diagarm*, dan arsitektur aplikasi. Pengkodean dilakukan menggunakan Flutter untuk antarmuka pengguna, Laravel sebagai backend, dan MySQL sebagai database. Pengujian sistem menggunakan blackbox testing. Hasil pengujian kami menunjukkan bahwa aplikasi pengamanan data berhasil dalam melaksanakan proses enkripsi dan dekripsi data. Dibandingkan dengan pengembangan sebelumnya yang berbasis web dan desktop, aplikasi ini memberikan solusi yang lebih adaptif terhadap mobilitas tinggi dalam lingkungan kerja. Integrasi Cloud Computing memberikan fleksibilitas dalam akses data, dan penggunaan platform Android secara signifikan meningkatkan mobilitas pengguna.

Kata kunci: aplikasi; *advanced encryption standard*; dokumen; *cloud computing*; keamanan

Abstract
Documents are valuable assets that often contain important information, including employee personal data, and are vulnerable to security threats such as theft and alteration by unauthorized parties. This research aims to develop an Android-based document security application that combines the Advanced Encryption Standard (AES) algorithm and cloud computing technology. This type of research is developed using the System Development Life Cycle (SDLC) model, which involves requirements analysis, design, coding, and testing. At the needs analysis stage, focus is given to employee data that needs to be secured. System design includes data structure, system structure, and user interface (UI). System design includes use case elements, class diagrams, and application architecture. Coding was done using Flutter as the user interface, Laravel as the backend, and MySQL as the database. System testing uses black box testing. Our test results show that the data security application is successful in carrying out the data encryption and decryption processes. Compared to previous web and desktop-based developments, this application provides a more adaptive solution to high mobility in the work environment. Cloud computing integration provides flexibility in data access, and the use of the Android platform significantly increases user mobility.

Keywords: *advanced encryption standard; application; cloud computing; document; security*

PENDAHULUAN

Keamanan file dokumen merupakan sebuah hal yang sangat penting bagi setiap orang ataupun instansi perusahaan pada saat ini. File dokumen biasanya berisikan informasi-informasi penting seseorang ataupun perusahaan baik itu laporan rahasia perusahaan, strategi bisnis rahasia perusahaan, ataupun riwayat perusahaan (Herman et al., 2021; Imron & Pratama, 2022). Saat ini pencurian data melalui plagiasi dan modifikasi sering ditemui dalam kehidupan digital. Dokumen yang banyak digunakan adalah dokumen dengan ekstensi docx. Hal ini dikarenakan dokumen dengan ekstensi.docx merupakan salah satu dokumen yang mudah dalam proses pembuatan serta penyimpanannya Untuk menjaga kerahasiaan, integritas, pengenalan identitas pengirim dan pencegahan penyangkalan pengiriman datadokumen, maka diperlukan sebuah alat bantu untuk melindungidokumen tersebut (Husaini et al., 2022).

Terfokus pada keamanan, penerapan teknik kriptografi menjadi aspek utama dalam melindungi informasi sensitif. Kriptografi adalah sebuah seni untuk memanipulasi suatu pesan maupun data rahasia ke dalam bentuk yang tidak diketahui oleh banyak orang dengan tujuan pesan atau data rahasia tersebut terlindungi dari orang yang tidak berhak mengetahuinya. (Fauzan et al., 2023; Ramadani & Sauda, 2020). Dalam konteks ini kami akan menggunakan alogotima enskripsi *Advanced Encryption Standard* (AES). Algortima *AES* merupakan algoritma type simetris yang menggunakan kunci (key) yang sama untuk proses enkripsi dan dekripsi (Firdaus & Santika, 2022). Algoritma ini menggunakan kunci yang sama saat enkripsi dan dekripsi, masukan dan keluarannn ya berupa blok dan kunci yang tetap yaitu sebesar 128,192,256 bit (Andriyanto & Sukmasetya, 2022; Fachrozi & Fahmi, 2021). Selain itu kami juga menambahkan layanan *Cloud Computing* untuk meningkatkan kemanan. *Cloud Computing* merupakan sebuah mekanisme, dimana sekumpulan Teknologi Informasi *resource* yang saling terhubung dan nyaris tanpa batas, baik itu infrastruktur maupun aplikasi dimiliki dan dikelola sepenuhnya oleh pihak ketiga sehingga memungkinkan *customer* untuk menggunakan *resource* tersebut secara on-demand melalui network baik yang sifatnya jaringan private maupun public(Khaliq, 2021; Riana, 2020).

Berdasarkan permasalahan keamana data, diperlukan suatu aplikasi pengamanan arsip dokumen (Suranta et al., 2022). Perlunya manajemen file pada sebuah perusahaan adalah suatu hal yang perlu dipertimbangkan, karena file penting pada sebuah perusahaan dapat tersimpan rapi dan aman serta dapat meningkatkan kualitas perusahaan (Riski et al., 2022). Dalam mewujudkan hal tersebut, kami meneliti untuk membuat aplikasi untuk mengamankan file dokumen dengan menggunakan algoritma enkripsi *Advenced Encryption Standart* dan Layanan *Cloud Computing* berbasis *mobile*.

Banyak penelitian sebelumnya yang berkaitan dengan pengembangan implementasi pengaman data dengan algoritma *AES* dan sejenisnya yang menghasilkan yang dapat mengatasi masalah diatas, diantaranya adalah pengembangan sistem pengamanan data dengan *Advanced Encryption Standard* berbasis web (Andhika & Mulyati, 2022; Andriyanto & Sukmasetya, 2022; Azhari et al., 2022; Nurhareza & Siswanto, 2022; Ramadan & Painem, 2022; Suranta & Sakti, 2022) dan berbasis Desktop (Alfiah et al., 2020; Benny & Sewaka, 2022; Prayudha et al., 2019), belum banyak penelitian yang mengeksplorasi pengamanan data karyawan dengan mengintegrasikan *AES* dan layanan *Cloud Computing* secara holistik berbasis *mobile*. Penelitian sebelumnya dari literatur tersebut terdapat kekurangan dalam fleksibilitas, aksesbilitas dan *mobile-friendly* untuk melindungi data karyawan di era digital yang terus berkembang. Oleh karena itu, penelitian ini berupaya mengisi kesenjangan ini dengan mengembangkan aplikasi pengamanan data karyawan yang menggabungkan keandalan *AES* dan fleksibilitas *Cloud Computing*, yang dapat diakses melalui *platform mobile* Dengan demikian, penelitian ini tidak hanya memberikan kontribusi pada literatur terkait keamanan data, tetapi juga menghadirkan solusi inovatif yang sesuai dengan tuntutan mobilitas dalam lingkungan kerja saat ini.

Penelitian ini bertujuan mengembangkan aplikasi keamanan dokumen berbasis Android yang menggabungkan algoritma *AES* dan teknologi *Cloud Computing*. Melalui integrasi *AES* dan *Cloud Computing* yang berbasis *mobile*, diharapkan penelitian ini dapat memenuhi tuntutan mobilitas dalam lingkungan kerja saat ini.

METODE

Metode pengembangan pada penelitian ini, kami menggunakan jenis penelitian *Research and Development (R&D)*, mengadopsi model *System Development Life Cycle (SDLC)* yang mencakup tahapan analisis kebutuhan perangkat lunak, desain, pengembangan/pengkodean, pengujian, dan tahap pendukung/support (Baharuddin, 2021; Oktaviani & Ayu, 2021). Namun pada penelitian ini kami hanya menggunakan empat tahapan yakni, analisis kebutuhan, desain, pengembangan/pengkodean, dan pengujian.

Tahapan analisis kebutuhan yang kami lakukan berdasarkan model terdiri dari kebutuhan perusahaan untuk data apa aja yang penting dan perlu di amankan. Dalam tahapan analisis, kami melakukan pengumpulan informasi terkait kebutuhan perusahaan terkait data yang perlu diamankan. Langkah-langkahnya mencakup wawancara dengan pihak terkait, observasi terhadap proses bisnis yang melibatkan penggunaan data, dan penelaahan dokumen terkait kebijakan keamanan.

Pada tahapan desain, kami merancang struktur data yang mencakup bagaimana data akan diorganisir, struktur sistem yang merinci cara komponen sistem berinteraksi, serta perancangan masukan dan keluaran perangkat lunak yang mencakup elemen-elemen antarmuka pengguna (UI). Ini mencakup pembuatan *use case* diagram untuk mengidentifikasi interaksi antara pengguna dan sistem, *activity diagram* untuk menggambarkan alur kerja, dan sketsa antarmuka pengguna.

Tahap pengembangan/pengkodean, kami menerjemahkan desain yang sudah dibuat ke dalam bahasa pemrograman. Kami menggunakan PHP sebagai bahasa pemrograman untuk backend, Flutter untuk tampilan mobile, dan MySQL sebagai database. Kami mengimplementasikan logika bisnis, antarmuka pengguna, dan fungsionalitas enkripsi/dekripsi dokumen sesuai dengan desain.

Pada tahap pengujian, kami melakukan evaluasi terhadap aplikasi untuk mencari error atau ketidaksesuaian dengan perancangan. *Black box testing* digunakan untuk mengidentifikasi potensi masalah pada input dan output yang tidak diharapkan. Pengujian mencakup berbagai skenario untuk memastikan bahwa aplikasi berfungsi dengan baik dalam kondisi yang berbeda.

HASIL DAN PEMBAHASAN

Hasil

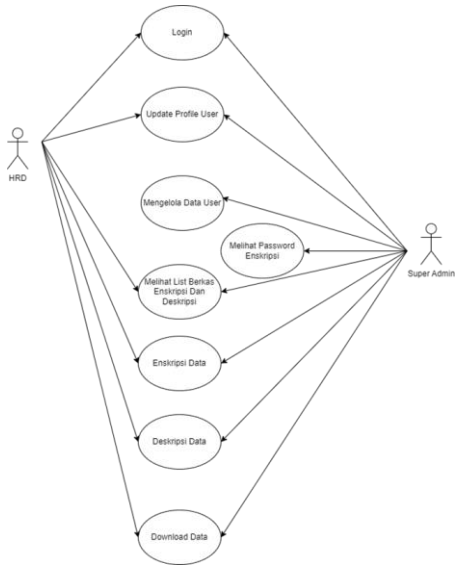
Hasil dari penelitian ini berupa sistem aplikasi pengamanan data berbasis *mobile* yang dikembangkan dengan metode penelitian System *Development Life Cycle (SDLC)*. Hasil temuan kami dari analisis kebutuhan berdasarkan observasi, kami mengidentifikasi jenis data yang perlu diamankan, yaitu data sensitif karyawan seperti PKWT/PKWTT. Kami menemukan bahwa aksesibilitas data perlu diatur dengan cermat, sehingga Super Admin memiliki akses penuh terhadap semua data dan fitur, sementara admin hanya memiliki kewenangan untuk melakukan enkripsi dan dekripsi tanpa dapat mengatur pengguna lainnya. Adapun untuk meningkatkan tingkat keamanan, kami memutuskan untuk menggunakan metode enkripsi *AES 256-bit*, sebuah standar keamanan tinggi.

Selanjutnya, dalam lingkungan pengguna, kami memilih untuk menggunakan Flutter sebagai kerangka pengembangan untuk menghasilkan antarmuka yang ramah pengguna pada perangkat *mobile*. Pilihan ini diambil untuk memastikan aplikasi memiliki tampilan yang responsif dan dapat diakses dengan mudah, sejalan dengan kebutuhan mobilitas pengguna.

Selain itu, kami menemukan bahwa integrasi dengan layanan *Cloud Computing* dapat memberikan keuntungan tambahan. Dengan mengintegrasikan Layanan *Cloud*, aplikasi menjadi lebih fleksibel dan data lebih aman. Dengan demikian, data tidak hanya disimpan secara lokal tetapi juga di *cloud*, meningkatkan kehandalan dan keamanan penyimpanan data. Keseluruhan, temuan dalam tahapan analisis ini membantu membentuk landasan yang kokoh untuk pengembangan aplikasi keamanan dokumen berbasis mobile, dengan fokus pada perlindungan data karyawan dan optimalisasi pengalaman pengguna.

Hasil dari tahapan desain pada penelitian ini melibatkan beberapa aspek penting, termasuk Struktur Data, Struktur Sistem, serta perancangan masukan dan keluaran yang diintegrasikan ke dalam antarmuka pengguna (UI). Struktur Data kami rancang dengan tujuan utama mengatur alur penyimpanan dan pengambilan data agar berjalan dengan efisien. Selain itu, kami juga menghasilkan Struktur Sistem yang menentukan alur penggunaan aplikasi, termasuk fitur-fitur yang dapat diakses oleh pengguna. Untuk memberikan gambaran visual yang lebih komprehensif, kami juga telah mengembangkan hasil Use Case, *Activity Diagram*, dan *Class Diagram* sebagai bagian dari desain system dan tergambar dalam gambar 1 dan gambar 2.

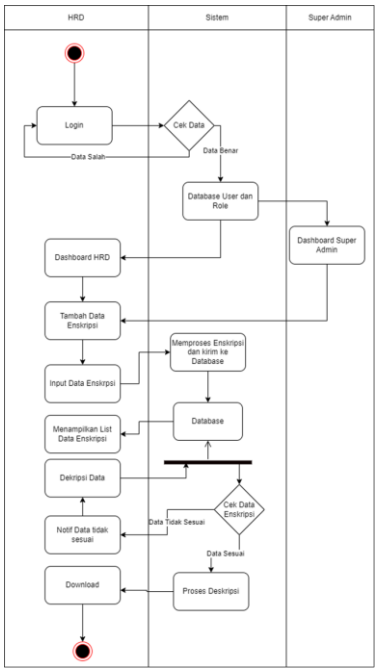
Pada tampilan gambar 1 menunjukan bahwa sistem ini terdiri dari dua level user yaitu superadmin dan HRD yang sebagai admin. Di mana super admin memiliki semua akses hingga mengelola data user dan password, serta melihat password hasil dari enskripsi. Sedangkan admin hanya dapat login, update profile, melihat berkas enkripsi dan dekripsi, melakukan enkripsi dan dekripsi, dan download.



Gambar 1. *Use case*

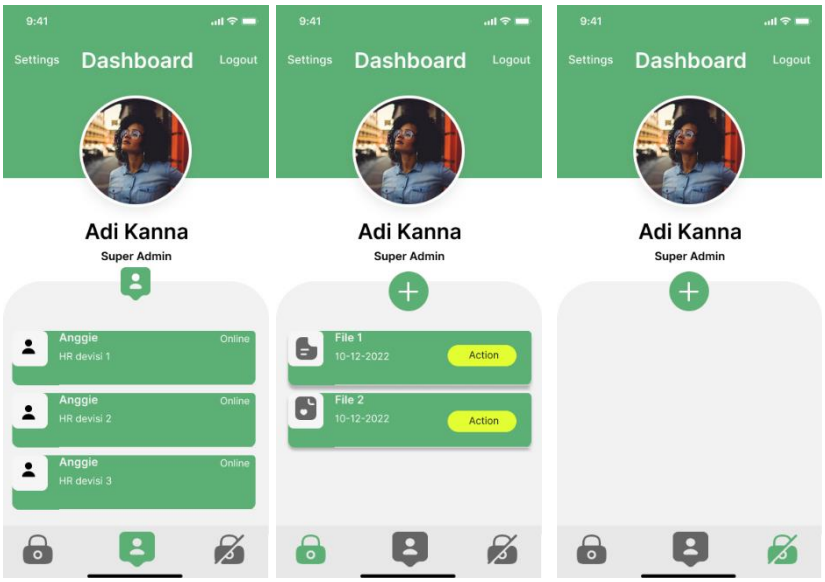
Pada Gambar 2, alur pada *Activity Diagram* dimulai dengan langkah awal "Mulai", diikuti oleh proses "Login". Setelah login, sistem melakukan pengecekan terhadap peran *(role)* pada akun yang terdaftar. Jika peran tersebut adalah admin, pengguna akan diarahkan ke halaman admin, sedangkan jika peran tersebut adalah superadmin, pengguna akan diarahkan ke halaman superadmin. Dari halaman admin, terdapat beberapa langkah, yaitu "Tambah Data Enkripsi" yang melibatkan input data enkripsi, proses enskripsi, dan menampilkan data hasil enskripsi. Setelah itu, terdapat proses "Dekripsi" yang melibatkan proses dekripsi data. Langkah terakhir adalah "Download Data" yang memungkinkan pengguna mengunduh data yang telah diolah. Alur aktivitas tersebut kemudian berakhir pada langkah "Selesai". Dengan urutan logis ini, *Activity Diagram* memberikan gambaran visual tentang bagaimana pengguna berinteraksi dengan berbagai fungsi dalam sistem keamanan dokumen ini.

Terakhir, perancangan masukan dan keluaran telah kami transformasikan ke dalam antarmuka pengguna (UI), yang mencakup elemen-elemen seperti login, dashboard, dan fungsi enkripsi serta dekripsi. Dengan memperhatikan hasil dari *Use Case*, *Activity Diagram*, dan *Class Diagram*, kami memastikan bahwa desain UI tidak hanya memenuhi kebutuhan fungsional yang telah dirancang sebelumnya tetapi juga mencerminkan alur kerja yang dijelaskan dalam tahap analisis. Semua ini menjadi dasar kokoh bagi tahapan implementasi pengkodean, sehingga aplikasi dapat dikembangkan dengan lebih terstruktur dan sesuai dengan kebutuhan yang telah diidentifikasi.



Gambar 2. *Activity diagram*

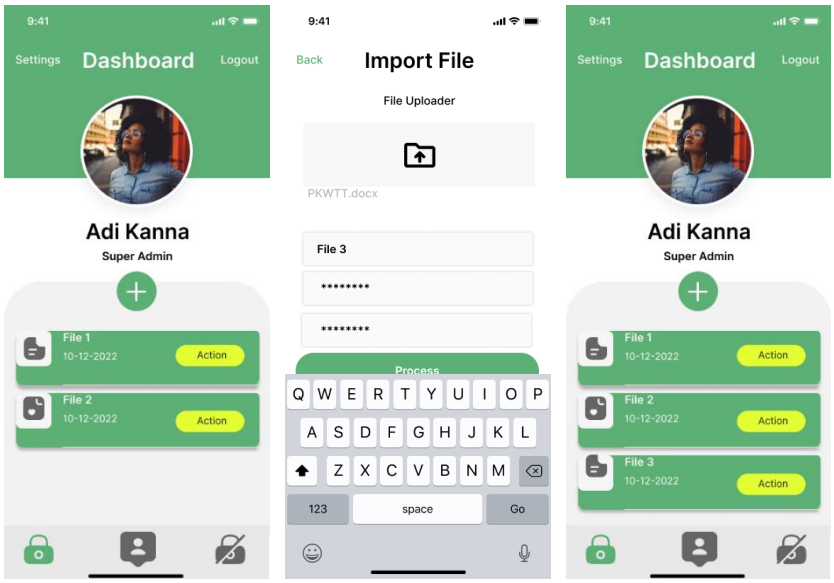
Hasil dari tahap pengembangan/pengkodean penelitian ini, kami berhasil menerapkan desain yang telah dirancang ke dalam bentuk aplikasi yang dapat dijalankan sebagaimana tergambar dalam Gambar 3.



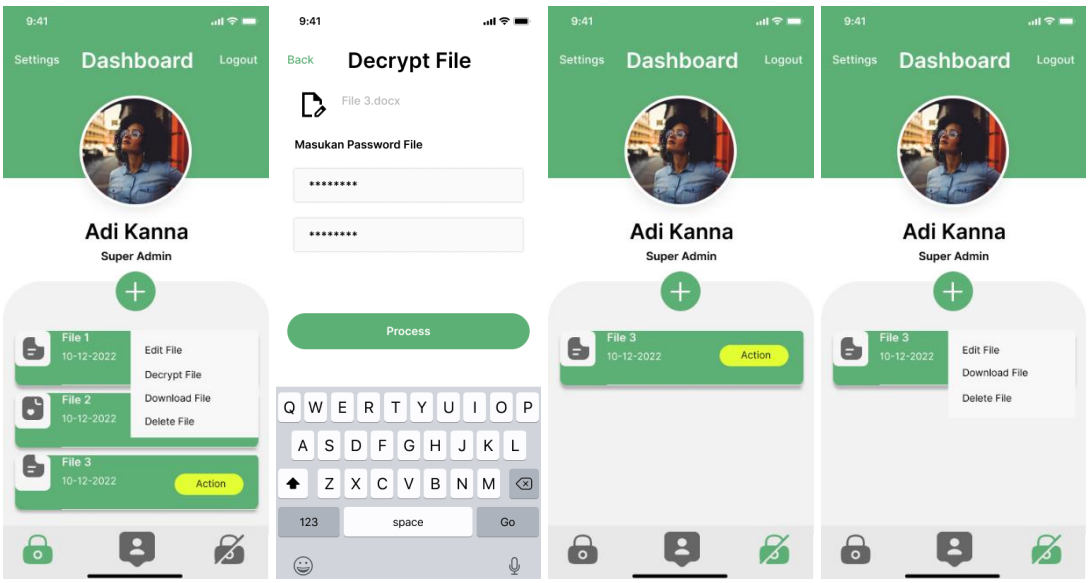
Gambar 3. Halaman *dashboard*

Pada dashboard aplikasi, terdapat tiga menu utama, yaitu User, *Encryption*, dan *Decryption. Menu User* digunakan untuk melihat daftar pengguna yang memiliki akses pada aplikasi ini. Menu *Encryption* berfungsi untuk melihat file yang telah berhasil diamankan melalui proses enkripsi. Sementara itu, menu *Decryption* digunakan untuk melihat file yang belum mengalami proses enkripsi. Dengan penataan menu yang jelas, pengguna dapat dengan mudah mengakses fitur yang diinginkan dan memanfaatkan fungsionalitas aplikasi secara efisien.

Pada tampilan Gambar 4 ini merupakan alur proses enkripsi data di mulai dengan klik tombol tambah, kemudian kita akan di arahkan ke menu *Import File* dan klik logo folder untuk memilih file yang akan kita amankan, setelah memilih berikan nama dan password untuk file tersebut lalu klik tombol proses.



Gambar 4. Proses enkripsi data



Gambar 5. Tombol *action decrypt file*

Pada tampilan gambar 5 ini merupakan alur proses dekripsi data dimulai dengan klik tombol action pada menu *Encryption* lalu pilih *Decrypt File*, maka akan di arahkan ke halaman proses dekripsi, pada halaman tersebut masukan password yang di gunakan untuk enkripsi data

tersebut dan klik proses untuk proses dekripsi file, setelah berhasil maka akan ada pada menu Decryption dan bisa kita download.

Hasil Tahap pengujian menggunakan *black box testing* pada tabel 1 menunjukkan bahwa, semua komponen atau tampilan pada sistem ini sudah berjalan atau berfungsi dengan baik. Seperti mengubah *password*, *login*, tambah file dan sebagainya.

Tabel 1. Hasil pengujian *black box*

Objek Pengujian	Kasus Pengujian	Hasil
Instalasi Aplikasi	Apakah aplikasi dapat di install dengan lancar pada smartphone android?	Berjalan dan berfungsi dengan baik pada android 11 dan 12.
Running Aplikasi	Apakah aplikasi yang telah di install dapat di jalankan?	Aplikasi yang di uji dapat di dibuka semua oleh user
Login	Apakah user dapat melakukan login dengan akun yang di sediakan setelah input email dan password?	User dapat login dengan akun mereka masing masing
Update Password	Apakah user dapat melakukan perubahan password?	User dapat melakukan perubahan password
List User	Apakah user dapat melihat list user yang terdaftar?	User dapat saling melihat user yang terdaftar aplikasi
Encryption	Apakah user dapat melihat, menambahkan data untuk di enkripsi?	User dapat menambahkan data untuk di enkripsi dan melihat file yang sudah di enkripsi
	Apakah user dapat mendecrypt file yang telah di enkripsi?	User dapat melakukan decrypt file yang telah ter enkripsi
Decryption	Apakah user dapat melihat dan meng enskripsi file pada menu decryption?	User dapat melihat file yang sudah di decrypt dan user dapat melakukan enkripsi ulang dengan key berbeda

Pembahasan

Berdasarkan hasil dari tahap analisis, kami menggunkan data PKWT/PKWTT yang merupakan data penting pada perusahaan untuk penelitian ini, aksebilitas data hanya dapat diakses oleh super admin dan admin,untuk super admin dapat mengakases semua data dan fitur yang ada pada aplikasi, sedangkan admin hanya dapat mengkenkripsi dan dekripsi data. Untuk melindungi data dengan menggunakan enskiprsi *AES* 256-bit dan mendapatkan hasil pengamanan yang lebih rumit pengembangan sebelumnya walaupun proses penyimpanan menjadi lebih lama. Dengan integrasi *Cloud Computing* didapatkan hasil lebih fleksible dikarenakan penyimpanan dan proses computing data tersimpan pada *cloud*, sehingga pengguna dapat mengakses data dari mana pun. Untuk lingkungan pengguna kami menggunakan flutter untuk antarmuka pengguna agar lebih *mobile-friendly*, sehingga hasil integrasi dengan *Cloud Computing* memberikan kemudahan untuk mengakses data melalui antarmuka *mobile* yang telah kami desain. Melalui langkah desain, kami berhasil merancang struktur data yang akan di gunakan pada tahap implementasi pengkodean, kami juga berhasil membentuk struktur sistem yang fleksible dari segi teknologi dan pengalaman pengguna. Pada

tahap masukan serta keluaran setelah di transformasikan kedalam antarmuka pengguna (UI) menghasilkan tampilan yang lebih mudah di mengerti atau di gunakan oleh pengguna, selain itu desain antarmuka pengguna menjadi acuan untuk tahapan pengkodean.

Hasil dari tahap pengkodean, desain diubah menjadi bentuk aplikasi menggunakan Flutter sebagai antarmuka pengguna, dan Laravel sebagai backend yang bertanggung jawab atas proses komputasi dan pengolahan data. Data disimpan di dalam database MySQL dan backend dijalankan dan diproses pada server cloud, sehingga memberikan akses yang lebih fleksibel.

Hasil pengujian menunjukkan bahwa aplikasi yang dikembangkan dapat mengenkripsi dan mendekripsi dokumen dengan normal. Pengguna juga dapat menyimpan dokumen ke dalam layanan *Cloud Computing* dengan lancar. Hasil uji coba ini menegaskan bahwa aplikasi dapat memberikan tingkat keamanan yang tinggi terhadap data karyawan, memastikan kinerja yang optimal, dan menyediakan akses yang mudah bagi pengguna hanya dengan menggunakan smartphone *mobile*.

Dibandingkan dengan temuan sebelumnya yang terfokus pada keamanan data berbasis web dan *desktop*, pendekatan kami dalam mengamankan data karyawan melalui aplikasi berbasis Android memberikan solusi yang lebih efektif dan fleksible. Sebagaimana dikemukakan temuan sebelumnya berbasis web (Andhika & Mulyati, 2022; Andriyanto & Sukmasetya, 2022; Azhari et al., 2022; Nurhareza & Siswanto, 2022; Ramadan & Painem, 2022; Suranta & Sakti, 2022) dan berbasis Desktop (Alfiah et al., 2020; Benny & Sewaka, 2022; Prayudha et al., 2019), menunjukkan bahwa pendekatan kami dalam mengamankan data karyawan menggunakan aplikasi berbasis Android memberikan solusi yang lebih efektif dan efisien dalam pengelolaan data sensitif. Hal ini menambahkan nilai dan inovasi dengan memperkenalkan metode baru untuk pengamanan data karyawan yang lebih *mobile-friendly* dan optimal dalam lingkungan kerja saat ini. Penelitian sebelumnya fokus pada keamanan data berbasis web dan desktop, sedangkan fokus kami pada aplikasi Android memperkaya pengetahuan sebelumnya dengan memberikan solusi yang lebih fleksibel, efisien, dan lebih sesuai dengan perkembangan teknologi yang ada saat ini.

SIMPULAN

Berdasarkan hasil temuan kami menunjukan bahwa aplikasi yang telah dikembangkan mampu mengenkripsi, mendekripsi, dan menyimpan dokumen dengan lancar, memberikan tingkat keamanan yang bersifat fleksibel, efisien, dan sesuai dengan kebutuhan mobilitas di lingkungan kerja saat ini, terutama untuk pengguna perangkat *mobile*. Dibandingkan dengan pendekatan sebelumnya yang berfokus pada aplikasi web dan *desktop*, pendekatan berbasis Android ini menawarkan adaptabilitas yang lebih baik terhadap kebutuhan mobilitas tinggi di lingkungan kerja. Integrasi *Cloud Computing* memberikan fleksibilitas akses data yang lebih tinggi, sementara penggunaan *platform* Android memberikan mobilitas yang sesuai dengan harapan pengguna.

REFERENSI

Alfiah, F., Sudarji, R., & Taqiyyuddin Al Fatah, D. (2020). Aplikasi Kriptografi Dengan Menggunakan Algoritma Elgamal Berbasis Java Desktop Pada Pt. Wahana Indo Trada Nissan Jatake. *ADI Bisnis Digital Interdisiplin Jurnal*, *1*(1), 22–34. https://doi.org/10.34306/abdi.v1i1.114

Andhika, R. R. D., & Mulyati, S. (2022). Penerapan Algoritma *Aes*-128 Untuk Aplikasi Pengarsipan Dokumen Berbasis Web Pada Pt Studio Inovasi Teknologi. *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) Jakarta-Indonesia*, 411–420.

Andriyanto, M. R., & Sukmasetya, P. (2022). Penerapan Algoritma *Advanced Encryption Standard* (*AES*) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace. *Journal of*

Computer System and Informatics (JoSYC), *4*(1), 179–187. https://doi.org/10.47065/josyc.v4i1.2451

Azhari, M., Perwitosari, J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi *Advanced Encryption Standard* (*AES*). *Jurnal Pendidikan Sains Dan Komputer*, *2*(1), 2809–476. https://doi.org/10.47709/jpsk.v2i1.1390

Baharuddin, M. R., & Ulfah, U. (2021). Pengembangan Sistem Informasi Manajemen Pelaksanaan Magang FKIP UNCP. *Jurnal Literasi Digital*, *1*(1), 34-41. https://doi.org/10.54065/jld.1.1.2021.6

Benny, S., & Sewaka. (2022). Aplikasi Pengamanan Data Menggunakan Kriptografi Dengan Metode Wake dan Algoritma Des Bebasis Java Desktop. *OKTAL : Jurnal Ilmu Komputer Dan Science*, *1*(7), 808–817.

Fachrozi, Mhd. F., & Fahmi, H. (2021). Penerapan Metode *AES*-128 Untuk Pengamanan Data Absensi FingerPrint Di Balai Penelitian Sungei Putih. *JIKOMSI [Jurnal Ilmu Komputer Dan Sistem Informasi]*, *3*(3), 1–8.

Fauzan, D. A., Fathurrozi, A., & Sugiyatno. (2023). Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma RSA (Rivest Shamir Adleman) dan *AES* (*Advanced Encryption Standard*) Berbasis Web. *Journal of Information and Information Security (JIFORTY)*, *4*(1), 2722–4058.

Firdaus, R., & Santika, R. R. (2022). Penerapan Algoritma *Aes*-128 Untuk Enkripsi Dokumen Di Pt Caveo Biometric Security. *Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*, 111–120.

Herman, Wijaya, R., Farandi, K., Miharja, S., & Wilson. (2021). Implementasi Algoritma *Aes*-128 Dan Sha-256 Dalam Perancangan Aplikasi Pengamanan File Dokumen. *Jurnal TIMES*, *10*(2), 2337–3601.

Husaini, F., Pardede, A. M. H., & Gultom, I. (2022). Penerapan Enkripsi Menggunakan Metode Elgamal guna Meningkatkan Keamanan Data Text dan Gambar. *JUKI : Jurnal Komputer Dan Informatika*, *4*(1), 67–73.

Imron, M., & Pratama, A. (2022). Pengamanan E-Dokumen Berbasis Steganografi Dengan Imron, M., & Pratama, A. (2022). Pengamanan E-Dokumen Berbasis Steganografi Dengan Kombinasi Advanced Encryption Standard (AES) 128 Bit. *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan*, *6*(2), 254-257.

Khaliq, K. F. (2021). Pengamanan Data Akta Dengan Metode Aes Berbasis Cloud Computing. *Jurnal Teknologi Dan Ilmu Komputer Prima (JUTIKOMP)*, *4*(1), 509-512.

Nurhareza, I. K., & Siswanto, S. (2022). Penerapan Algoritme Kriptografi AES 256 Untuk Mengamankan Dokumen Berbasis Web Pada Kelurahan Belendung. *Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*, *1*(1), 302-309.

Oktaviani, L., & Ayu, M. (2021). Pengembangan Sistem Informasi Sekolah Berbasis Web Dua Bahasa SMA Muhammadiyah Gading Rejo. *Jurnal Pengabdian Pada Masyarakat*, *6*(2), 437–444.

Prayudha, J., Saniman, & Ishak. (2019). Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode *Advanced Encryption Standard* (*AES*). *Sains Dan Komputer (SAINTIKOM)*, *18*(2), 119–129. https://doi.org/10.53513/jis.v18i2.150

Ramadan, A., & Painem. (2022). Pengamanan Data Keuangan Menggunakan Algoritma *Advanced Encryption Standard* 128 Pada Pt. Charise Deo Indonesia. *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*, *1*(1), 49-57.

Ramadani, S., & Sauda, S. (2020). Penerapan Algoritma *AES* dan DSA Menggunakan Hybrid Cryptosystem untuk Keamanan Data. *Jurnal Riset Komputer)*, *7*(4), 2407–389.

Riana, E. (2020). Implementasi *Cloud Computing* Technology dan Dampaknya Terhadap Kelangsungan Bisnis Perusahaan Dengan Menggunakan Metode Agile dan Studi

Literatur. *JURIKOM (Jurnal Riset Komputer)*, *7*(3), 439. https://doi.org/10.30865/jurikom.v7i3.2192

Suranta, A. I., & Sakti, D. V. S. Y. (2022). Penerapan Algoritma *AES* (Advance Encryption Standart) 128 untuk Enkripsi Dokumen di PT. Gunung Geulis Elok Abadi. *SKANIKA: Sistem Komputer Dan Teknik Informatika*, *5*(1), 1–10. https://doi.org/10.36080/skanika.v5i1.2118