1st National Conference on Electrical, Informatics and Industrial Technology (NEIIT-2024)
July 20, 2024

IMPLEMENTASI KEAMANAN DOKUMEN RAHASIA DESA MANGGIS MENGGUNAKAN METODE AES

Mico Alehandro[1], Harso Kurniadi[2], Yudo Bismo Utomo[3].
[1,2,3]Teknik Komputer, Fakultas Teknik, Universitas Islam Kadiri - Kediri
E-mail: [*1]micoalexsandro@gmail.com , [2]harsokurniadi@uniska-kediri.ac.id. , [3]yudobismo@uniska-kediri.ac.id

ARTICLE INFO

Article history:

Submited:
July 16, 2024

Accepted:
July 18, 2024

Published:
July 31, 2024

Keywords:

AES Method, Cryptography, Document Security

Kata Kunci:

Metode AES, Kriptografi, Keamanan Dokumen

ABSTRACT

The focus of data security in the digital age is primarily on data security loopholes that can be exploited by unscrupulous and irresponsible parties. Cryptography is a science that studies techniques for securing information, and one of these techniques is maintaining the confidentiality of documents in Manggis village. However, Manggis village does not yet have an application used to secure important confidential documents, like finances, population data, and local policies. The document needs to be secured in order to prevent abuse and invasion of privacy. To secure important documents in Manggis village, one popular cryptographic algorithm is the AES method, or Advanced Encryption Standard method. The fact that the Advanced Encryption Standard is an extremely strong encryption standard that makes it difficult for careless parties to find security flaws is one of its benefits. Documents holding sensitive and vital information can be encrypted using the AES technique to prevent careless parties from reading them. Because it is extremely safe and difficult to breach security, the researcher decided to employ the AES technique to secure papers in Manggis Village.

ABSTRAK

Keamanan data saat ini menjadi fokus utama di era digitalisasi, karena pengaruh kemajuan teknologi yang sangat pesat celah keamanan dapat dimanfaatkan oleh pihak yang tidak bermoral maupun tidak bertanggung jawab. Kriptografi adalah ilmu yang mempelajari tentang teknik mengamankan informasi, salah satunya yaitu menjaga kerahasiaan dokumen di desa Manggis. Namun, desa Manggis belum memiliki aplikasi yang digunakan untuk mengamankan dokumen-dokumen penting yang bersifat rahasia, seperti data penduduk, keuangan, dan kebijakan lokal. Dokumen tersebut harus diamankan tujuannya untuk mencegah penyalahgunaan dan pelanggaran privasi. Untuk mengamankan dokumen penting yang ada di desa Manggis menggunakan metode AES. Metode AES atau *Advanced Encryption Standard* merupakan salah satu algoritma kriptografi yang sering kali digunakan untuk pengamanan data pada Perusahaan, instansi, maupun data pribadi. Salah satu kelebihan dari metode *Advanced Encryption Standard* adalah standar enkripsi yang sangat aman dan sulit untuk ditembus celah keamanannya oleh pihak yang tidak bertanggung jawab. Dengan menggunakan metode AES, dokumen yang berisi informasi penting dan sensitif dapat dienkripsi sehingga tidak dapat dibaca oleh pihak yang tidak bertanggungjawab. Oleh karena itu, peneliti memilih metode AES ini sebagai metode pengamanan dokumen yang ada di Desa Manggis karena sangat aman dan sulit sekali untuk ditembus celah keamanannya.

This work is licensed under a Creative Commons Attribution 4.0 International License.

Corresponding Author:
Mico Alehandro,
Program Studi Teknik Komputer, Fakultas Teknik, Universitas Islam Kadiri
Jalan Sersan Suharmadji No. 38, Kota Kediri, Jawa Timur, Indonesia.
Email: micoalexsandro@gmail.com

1. PENDAHULUAN

Keamanan data menjadi aspek yang paling krusial di era digital saat ini karena terus berkembangnya teknologi dengan cepat. Setiap kemajuan teknologi baru tidak hanya membawa peningkatan fitur, tetapi juga meningkatkan kebutuhan akan keamanan. Namun, dengan berkembangnya teknologi, muncul juga celah baru yang dapat dieksploitasi oleh individu yang tidak bertanggung jawab untuk kepentingan mereka sendiri, yang berpotensi merugikan banyak pihak. Oleh karena itu, keamanan data telah menjadi prioritas utama dalam berbagai bidang[1][2]. Terutama di bidang pemerintahan desa yang memiliki berbagai dokumen penting maupun dokumen rahasia desa yang memerlukan perlindungan yang kuat agar dapat mencegah terjadinya kebocoran data.

Desa Manggis sebagai representasi dari banyak daerah di Indonesia memiliki kebutuhan yang sama akan perlindungan dokumen penting ataupun dokumen rahasia dengan aman dan kuat. Dokumen rahasia desa dapat mencakup berbagai informasi penting, seperti data penduduk, keuangan, dan kebijakan lokal, yang harus dijaga kerahasiaannya untuk mencegah penyalahgunaan dan pelanggaran privasi. Desa Manggis menggunakan aplikasi "*Smart*" untuk melakukan pengelolaan data dan pelayanan publik, khususnya administrasi persuratan. Namun, desa Manggis belum memiliki aplikasi yang digunakan untuk mengamankan dokumen-dokumen penting yang bersifat rahasia.

Dalam konteks ini, implementasi keamanan dokumen rahasia menggunakan *Advanced Encryption Standard* (AES) menjadi pilihan yang menarik. *Advanced Encryption Standard* (AES) merupakan algoritma *cryptographic* yang dapat digunkan untuk mengamakan data. Algoritma AES adalah blok *chipertext simetrik* yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut *ciphertext*; sebaliknya dekripsi adalah merubah *ciphertext* data menjadi bentuk semula yang kita kenal sebagai *plaintext*. Algoritma AES ini menggunkan kunci kriptografi 128, 192, dan 256 bits untuk mengenkrip dan dekrip data pada blok 128 *bits*[3]. Pengamanan *file* dengan menggunakan teknik kriptografi telah banyak dilakukan dalam berbagai penelitian. Tampaknya implementasi yang hanya menggunakan algoritma kriptografi telah ditinggalkan dan beralih menggunakan kombinasi asimetri dan simetri[4].

AES adalah algoritma kriptografi untuk mengamakan data dimana algoritmanya adalah blok *chipertext simetrik* yang dapat mengenkripsi dan mendekripsi informasi[5]. Implementasi algoritma AES juga dilakukan untuk mengenkripsi dan mendekripsi proses enkripsi dokumen.

2. METODE PENELITIAN

Metode yang digunakan dalam membangun aplikasi keamanan dokumen rahasia desa Manggis menggunakan metode SDLC (Software Development Life Cycles). SDLC adalah tahapan-tahapan pekerjaan yang dilakukan oleh analis sistem dan programmer[6]. Berikut adalah gambar metode SDLC :

Gambar 1. Metode SDLC

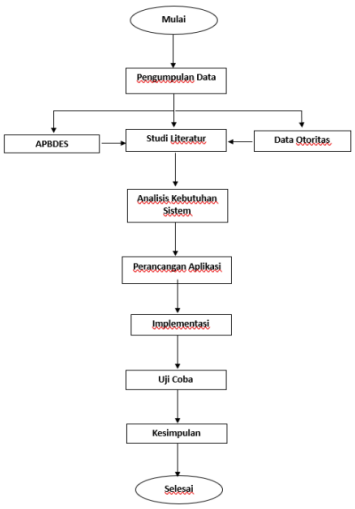
2.1. Alur Penelitian

Alur penelitian dapat berbeda-beda tergantung pada jenis penelitian dan metodologi penelitian yang digunakan. Dikarenakan menggunakan metode SDLC (*Software Development Life Cycles*), maka proses pengembangan perangkat lunak harus dilakukan tanpa adanya kesalahan.

Dalam penelitian yang perlu diperhatikan antara lain yaitu, dengan mulai penentuan judul, mengidentifikasi masalah, metode pengembangan aplikasi, dan tujuan penelitian. Setelah itu peniliti melakukan pengumpulan data secara observasi maupun wawancara untuk mendapatkan data dan informasi-informasi yang valid dan akurat.

Dengan didapatkannya data, proses selanjutnya adalah dengan melakukan Analisa, pada tahap ini semua data yang diperoleh akan diolah untuk kebutuhan aplikasi yang akan dibuat sesuai dengan kebutuhan. Dilanjutkan dengan implementasi, pada tahap implementasi langkah yang harus dilakukan adalah dengan memodelkan sistem informasi

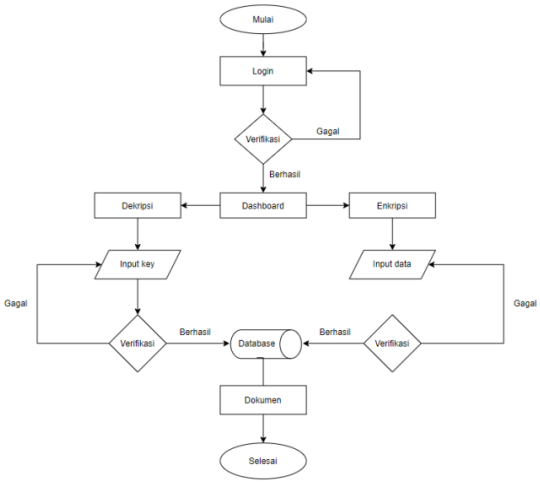
dan aplikasi yang akan dibuat. Setelah itu melakukan penulisan kode program lalu melakukan uji coba pada aplikasi untuk mengetahui seberapa cepat dalam melakukan proses enkripsi dan dekripsi dokumen dengan menggunakan aplikasi yang telah dibuat. Tahap terakhir adalah menentukan kesimpulan dan saran bagi peneliti berikutnya yang tertarik untuk melakukan pengembangan aplikasi tersebut. Berikut adalah model alur penelitian yang telah dibuat :.



Gambar 2. Alur Penelitian

2.1.1. Rancangan Analisa Sistem

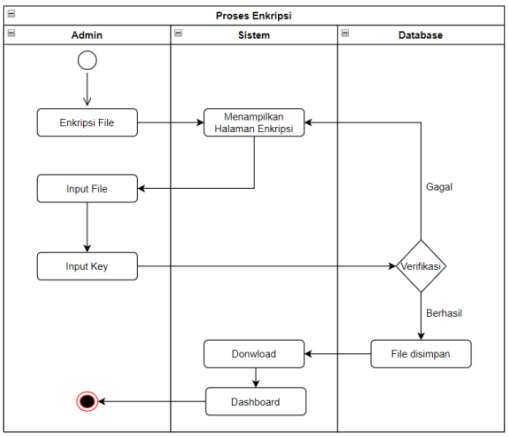
Tujuan dari rancangan analisa sistem ini yaitu, untuk menentukan spesifikasi dari sistem agar sesuai dengan kebutuhan pengguna dan dapat menetapkan spesifikasi yang dibutuhkan untuk merancang sistem baru atau memperbaiki sistem yang telah ada sebelumnya. Dalam hal ini *flowchart* dapat membantu untuk mengidentifikasi dan mengatasi masalah yang ada pada sistem dan membantu untuk perencanaan sistem yang akan dirancang. *Flowchart* adalah rancangan dalam tahapan proses[7]. Berikut adalah *flowchart* rancangan sistem aplikasi yang telah dibuat :.



Gambar 3. Rancangan Alur Sistem Aplikasi.

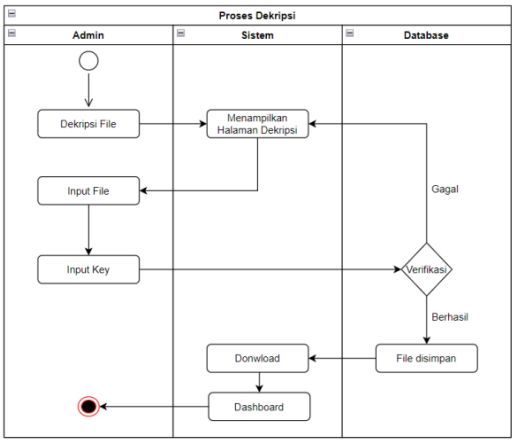
2.1.2. Desain Sistem Aplikasi

Desain sistem aplikasi dapat membantu menentukan perangkat keras dan dapat pula membantu dalam mendefinisikan arsitektur sistem secara keseluruhan[8]. Berikut adalah rancangan desain *actifity* diagram proses enkripsi yang telah dibuat :



Gambar 4. Desain Sistem Enkripsi

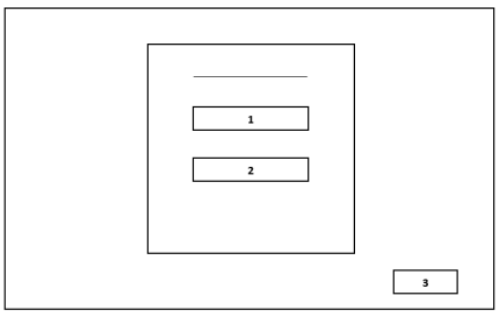
Selain desain sistem enkripsi peneliti juga membuat desain sistem dekripsi. Berikut adalah rancangan desain *actifity* diagram proses dekripsi yang telah dibuat :



Gambar 5. Desain Sistem Dekripsi

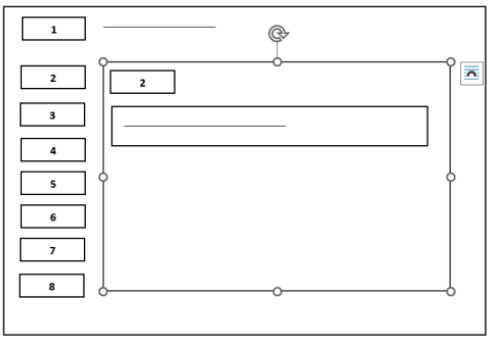
2.1.3. Rancangan Desain Sistem Aplikasi

Desain aplikasi adalah dokumen yang menjelaskan secara ringkas bagaimana aplikasi ini akan dirancang sesuai hasil dari analisis pemersalahan yang ada pada balai desa Manggis. Ringkasan tersebut hanya akan berisikan informasi tentang tampilan antarmuka, fitur dan fungsionalitas, dan alur kerja aplikasi. Berikut adalah gambar desain aplikasi :



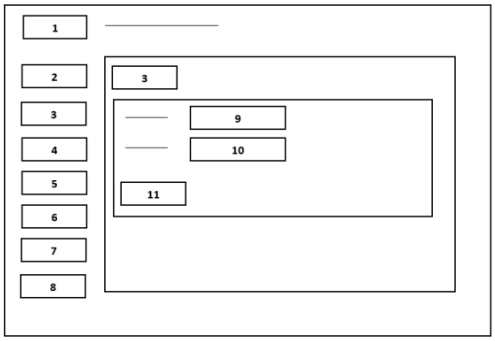
Gambar 6. Tampilan Halaman *Login*

Berikut keterangan dari gambar 6 ialah, pada kolom nomor 1 digunakan untuk memasukkan *username* (NIP), pada kolom nomor 2 digunakan untuk memasukkan *password*, dan pada kolom nomor 3 digunakan untuk tombol *login.*



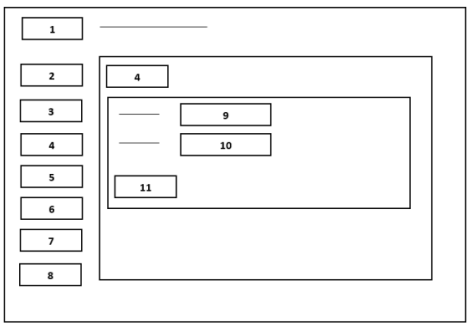
Gambar 7. Tampiran Beranda (*Dashboard*)

Keterangan pada gambar 7 ialah, pada kolom nomor 1 digunakan untuk logo aplikasi, pada kolom nomor 2 digunakan untuk tombol home, pada kolom nomor 3 digunakan untuk menu *encrypt*, pada kolom nomor 4 digunakan untuk menu *decrypt*, pada kolom 5 digunakan untuk menu *list file*, pad kolom nomor 6 digunakan untuk menu *help*, pada kolom nomor 7 digunakan untuk menu *about*, dan pada kolom nomor 8 digunakan untuk tombol *logout*.



Gambar 8. Tampilan Proses *Encrypt*

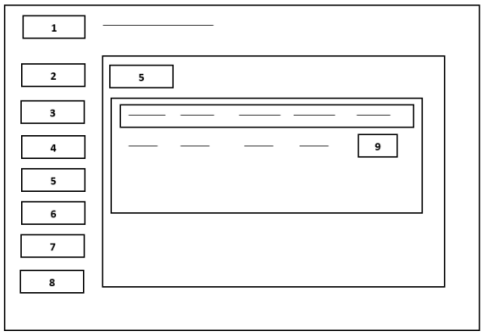
Keterangan pada gambar 8 ialah, pada kolom nomor 1 digunakan untuk logo aplikasi, pada kolom nomor 2 digunakan untuk tombol home, pada kolom nomor 3 digunakan untuk menu *encrypt*, pada kolom nomor 4 digunakan untuk menu *decrypt*, pada kolom 5 digunakan untuk menu *list file*, pad kolom nomor 6 digunakan untuk menu *help*, pada kolom nomor 7 digunakan untuk menu *about*, pada kolom nomor 8 digunakan untuk tombol *logout*, pada kolom nomor 9 digunakan untuk tombol upload *file* yang akan dienkripsi, pada kolom nomor 10 digunakan untuk memasukkan *key* atau *password*, dan pada kolom nomor 11 digunakan untuk *submit*.



Gambar 9. Tampilan Proses *Decrypt*

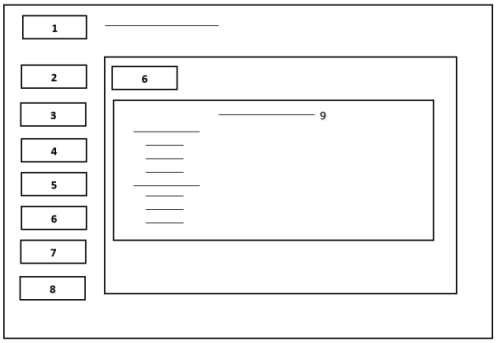
Keterangan pada gambar 9 ialah, pada kolom nomor 1 digunakan untuk logo aplikasi, pada kolom nomor 2 digunakan untuk tombol home, pada kolom nomor 3 digunakan untuk menu *encrypt*, pada kolom nomor 4 digunakan untuk menu

decrypt, pada kolom 5 digunakan untuk menu *list file*, pad kolom nomor 6 digunakan untuk menu *help*, pada kolom nomor 7 digunakan untuk menu *about*, pada kolom nomor 8 digunakan untuk tombol *logout*, pada kolom nomor 9 digunakan untuk tombol upload *file* yang akan didekripsi, pada kolom nomor 10 digunakan untuk memasukkan *key* atau *password* yang telah dibuat ketika mengenkripsi file, dan pada kolom nomor 11 digunakan untuk *submit*



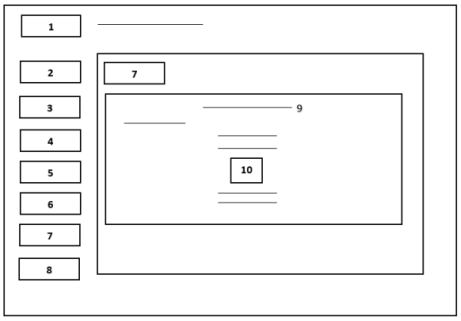
Gambar 10. Tampilan Menu *List File* Yang Telah Dienkripsi

Keterangan pada gambar 10 ialah, pada kolom nomor 1 digunakan untuk logo aplikasi, pada kolom nomor 2 digunakan untuk tombol home, pada kolom nomor 3 digunakan untuk menu *encrypt*, pada kolom nomor 4 digunakan untuk menu *decrypt*, pada kolom 5 digunakan untuk menu *list file*, pad kolom nomor 6 digunakan untuk menu *help*, pada kolom nomor 7 digunakan untuk menu *about*, pada kolom nomor 8 digunakan untuk tombol *logout*, dan pada kolom nomor 9 digunakan untuk tombol menghapus *list file* yang telah dienkripsi.



Gambar 11. Tampilan Menu *Help*

Keterangan pada gambar 11 ialah, pada kolom nomor 1 digunakan untuk logo aplikasi, pada kolom nomor 2 digunakan untuk tombol home, pada kolom nomor 3 digunakan untuk menu *encrypt*, pada kolom nomor 4 digunakan untuk menu *decrypt*, pada kolom 5 digunakan untuk menu *list file*, pad kolom nomor 6 digunakan untuk menu *help*, pada kolom nomor 7 digunakan untuk menu *about*, pada kolom nomor 8 digunakan untuk tombol *logout*, dan pada kolom nomor 9 ialah teks cara penggunaan aplikasi.



Gambar 12. Tampilan Menu *About*

Keterangan pada gambar 12 ialah, pada kolom nomor 1 digunakan untuk logo aplikasi, pada kolom nomor 2 digunakan untuk tombol home, pada kolom nomor 3 digunakan untuk menu *encrypt*, pada kolom nomor 4 digunakan

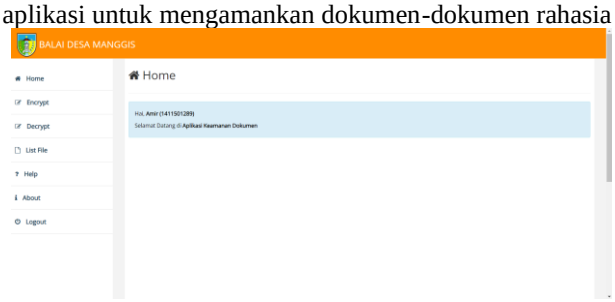
untuk menu *decrypt*, pada kolom 5 digunakan untuk menu *list file*, pad kolom nomor 6 digunakan untuk menu *help*, pada kolom nomor 7 digunakan untuk menu *about*, pada kolom nomor 8 digunakan untuk tombol *logout*, pada kolom nomor 9 ialah teks aplikasi dibuat oleh peneliti dan dibimbing oleh dosen pembimbing, dan pada kolom nomor 10 ialah logo Universitas Islam Kadiri Kediri.

3. HASIL DAN PEMBAHASAN

Penelitian ini menghasilkan aplikasi enkripsi dan dekripsi berbasis web yang digunakan untuk mengamankan dokumen rahasia desa. Bahasa pemrograman yang digunakan ialah menggunakan *php native* dengan *MySQL* yang digunakan untuk basis datanya. PHP adalah bahasa server-side scripting dan pemrograman *open-source* sehingga pengguna bebas menggunakan bahasa pemrograman PHP[9]. Berikut adalah implementasi dari hasil rancangan desain aplikasi yang telah dibuat sebagai berikut :

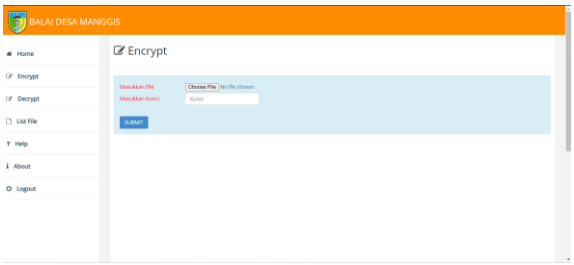
Gambar 13. Tampilan Halaman *Login*

Pada gambar 13 yaitu tampilan halaman login, halaman login berfungsi untuk mengatur proses identifikasi sebelum pengguna menggunakan aplikasi untuk mengamankan dokumen-dokumen rahasia desa.



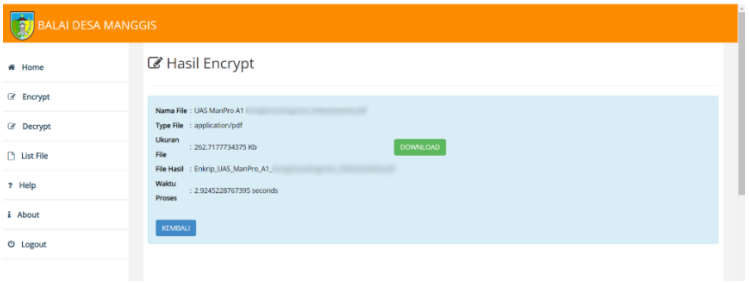
Gambar 14. Tampilan Beranda (Dashboard)

Pada gambar 14 yaitu tampilan beranda (dashboard) dari aplikasi, pada beranda (dashboard) memiliki beberapa menu yaitu, menu *home*, menu *encrypt*, menu *decrypt*, menu *list file*, menu *help*, menu *about* dan menu *logout*.



Gambar 15. Tampilan Menu *Encrypt*

Pada gambar 15 yaitu, tampilan menu *encrypt* yang digunakan untuk mengenkripsi dokumen-dokumen rahasia desa. Pengguna harus menginputkan file word, pdf, excel dan pdf yang akan dienkripsi pada kolom masukkan file, kemudian pengguna harus memasukkan key atau kunci sebagai password dan kemudian pengguna dapat menekan tombol submit untuk memproses mengamankan file tersebut.

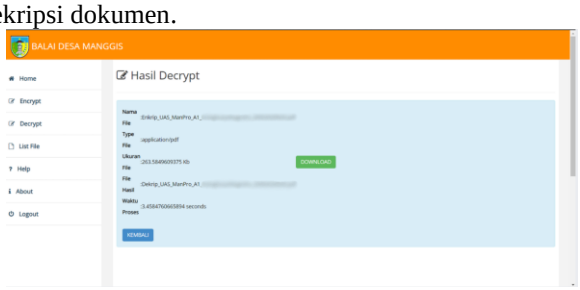


Gambar 16. Tampilan Proses *Encrypt*

Pada gambar 16 setelah proses enkripsi selesai, pengguna dapat memilih opsi download untuk menyimpan hasil dokumen yang telah dienkripsi atau memilih opsi kembali untuk mengenkripsi dokumen yang lainnya

Gambar 17. Tampilan Menu *Decrypt*

Pada gambar 17 yaitu, tampilan menu decrypt yang digunakan untuk menerjemahkan atau membuka dokumen yang telah dienkripsi sebelumnya. Pengguna harus menginputkan file yang akan didekripsi pada kolom masukkan file, kemudian pengguna harus memasukkan key atau kunci yang telah dibuat sebelumnya sebagai password yang bertujuan agar dokumen yang telah dienkripsi sebelumnya dapat dibuka kembali. Kemudia pengguna dapat menekan tombol submit untuk memproses dekripsi dokumen.

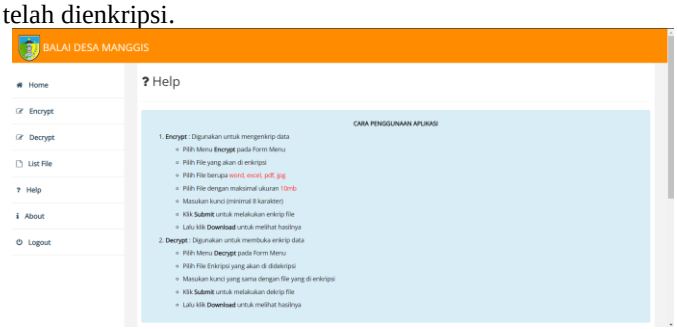


Gambar 18. Tampilan Proses *Decrypt*

Pada gambar 18 setelah proses dekripsi selesai, pengguna dapat memilih opsi download untuk menyimpan hasil dokumen yang telah didekripsi atau memilih opsi kembali untuk mengdekripsikan dokumen yang lainnya.

Gambar 19. Tampilan Menu *List file*

Pada gambar 19 yaitu, tampilan menu *list file* yang dapat digunakan pengguna untuk mengetahui dokumen apa saja yang telah dienkripsi, mengetahui password dokumen yang telah dienkripsi dan pengguna juga dapa menghapus list dokumen yang telah dienkripsi.



Gambar 20. Tampilan Menu Help

Pada gambar 20 yaitu, tampilan menu help yang dapat digunakan untuk memudahkan pengguna untuk mengetahui cara penggunaan aplikasi untuk mengamankan dokumen-dokumen rahasia desa.

Gambar 21. Tampilan Menu *About*

Pada gambar 21 yaitu, tampilan menu about yang berisikan informasi aplikasi dibuat oleh peneliti dan dibimbing oleh dosen pembimbing 1 dan dosen pembimbing 2.

3.1 Tampilan Berkas Setelah Enkripsi dan Dekripsi

Saat file atau dokumen dienkripsi terdapat perubahan pada isi *file* atau dokumen, sehingga file atau dokumen tidak dapat dibaca oleh orang yang tidak mengetahui *key* atau kunci dari *file* atau dokumen yang telah dienkripsi. Berikut adalah salah satu contoh yaitu, *file* atau dokumen APBDes dengan format *pdf* yang telah dienkripsi dan didekripsi.

Gambar 22. Dokumen APBDes Sebelum Dienkripsi

Sebelum berkas pdf dienkripsi isi dokumen akan menampilkan data seperti yang terdapat pada gambar 22 data masih bisa dibaca normal, selanjutnya adalah tampilan berkas setelah dienkripsi.

Gambar 23. Tampilan Dokumen APBDes Setelah Dienkripsi

Setelah dienkripsi dokumen akan menampilkan data yang bersifat acak atau kode-kode seperti pada gambar 23 sehingga tidak memungkinkan dokumen dapat dibaca sebelum dilakukannya proses didekripsi.

3.2 Pengujian *Avalanche Effect*

Avalanche Effect (AE) adalah perubahan kecil *bit* (misalnya, satu *bit*) baik pada plaintext maupun *key*/kunci yang akan menyebabkan perubahan signifikan terhadap hasil dari *ciphertext*. AE dapat digunakan sebagai metrik untuk menganalisis kinerja dan keamanan dari suatu algoritma enkripsi kriptografi[10]. Pada penelitian ini dilakukan analisis keamanan enkripsi AES berupa besar AE terhadap Panjang kunci enkripsi metode AES yaitu AES-128,AES-192, dan AES-256

$$Avalanche\ Effect \frac{Perubahan\ Bit}{Jumlah\ Panjang\ Kunci}\ X\ 100\% =$$

Tabel 1. Pengujian Avalanche Effect

Panjang Kunci	Nilai Avalanche Effect
AES-128	47,8%
AES-192	48,3%
AES-256	54,5%

Pada pengujian yang telah dilakukan, tabel 1 menunjukkan nilai rata-rata Avalanche Effect untuk tiap-tiap panjang kunci metode AES. Dari hasil pengujian AE pada metode AES-256 mendapatkan nilai yang lebih baik dari metode AES-128 dan AES-192. Hal itu menunjukkan bahwa perbandingan jumlah panjang kunci pada tiap metode AES sangat mempengaruhi hasil untuk mengamankan dokumen, dilihat dari hasil perubahan bit pada hasil enkripsi. Hal itu menunjukkan bahwa metode pengamanan data yang digunakan penulis yaitu AES-256 dapat dipastikan keamanannya untuk mengamankan dokumen rahasia desa.

3.3 Pengujian Kecepatan Proses Enkripsi dan Dekripsi

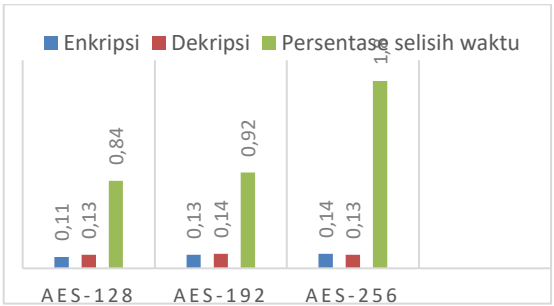
Pengujian ini berfungsi untuk mengetahui selisih waktu proses enkripsi dan dekripsi atau untuk mengetahui selisih waktu kecepatan proses pengkodean data yang menggunakan panjang kunci metode AES-128, AES-192, dan AES-256[11].

$$Rasio\ Kecepatan = \frac{Waktu\ Enkripsi}{Waktu\ Dekripsi} =$$

Tabel 2. Pengujian Rasio Kecepatan

Metode	Dokumen	Enkripsi	Dekripsi	Persentase Selisih Waktu
AES-128	Ujicoba.docx	0,11 detik	0,13 detik	0,84 detik
AES-192	Ujicoba.docx	0,13 detik	0,14 detik	0,92 detik
AES-256	Ujicoba.docx	0,14 detik	0, 13 detik	1,8 detik

Pada pengujian rasio kecepatan enkripsi dan dekripsi menunjukkan nilai persentase selisih waktu metode AES-128 membutuhkan waktu dekripsi lebih lama dari saat proses enkripsi yaitu 0,84 detik, metode AES-192 membutuhkan waktu dekripsi lebih lama dari enkripsi yaitu 0,92 detik, dan untuk metode AES-256 membutuhkan waktu lebih lama untuk enkripsi dari pada dekripsi yaitu 1,8 detik.



Gambar 24. Diagram Persentase Selisih Waktu

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, maka dapat diambil kesimpulan terhadap aplikasi Keamanan Dokumen Rahasia Desa Manggis Menggunakan Metode AES sebagai berikut :

1. Hasil dari penelitian ini berupa aplikasi berbasis web yang sangat mudah digunakan, untuk mengamankan dokumen rahasia desa. Dari beberapa langkah penelitian yang telah dilakukan oleh penulis, aplikasi ini dapat dijalankan dengan baik sehingga dapat membantu perangkat desa untuk mengamankan dokumen-dokumen yang bersifat rahasia.

2. Dari hasil pengujian AE pada tiap metode AES, AES-256 (54,5%) mendapatkan nilai yang lebih baik dari metode AES-128 (47,8%) dan AES-192 (48,3%). Hal itu menunjukkan bahwa metode pengamanan data yang digunakan penulis yaitu AES-256 dapat dipastikan keamanannya untuk mengamankan dokumen rahasia desa.

Adapun beberapa saran yang diharapkan dapat menjadi bahan pertimbangan lebih lanjut dalam upaya untuk mengembangkan sistem dimasa yang akan datang adalah sebagai berikut :

1. Penambahan format file agar aplikasi ini dapat digunakan untuk mengamankan semua file yang tidak terfokuskan pada file dengan format word,excel,pdf dan jpg.
2. Perubahan batas maksimal file yang dapat dienkripsi lebih dari 10mb.
3. Perubahan PHP dengan framework laravel agar dapat meningkatkan kecepatan proses enkripsi.

DAFTAR PUSTAKA

[1] Y. B. Utomo and D. Erwanto, "Analisa Teknik Steganografi dan Steganalysis Pada File Multimedia Menggunakan Net Tools dan Hex Editor," 2019.

[2] Firda Nurelia Syah Putri, Yudo Bismo Utomo, and Harso Kurniadi, "Analisa Celah Keamanan Pada Website Pemerintah Kabupaten Kediri Menggunakan Metode Penetration Testing Melalui Kali Linux," Online, 2023.

[3] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *Jurnal Pendidikan Sains dan Komputer*, vol. 2, no. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.

[4] A. Saepudin, R. Aryanti, E. Fitriani, and D. Ardiansyah, "Perancangan Sistem E-Commerce Menggunakan Model Rapid Application Development Pada Pengurus Cabang Judo Karawang," *Paradigma - Jurnal Komputer dan Informatika*, vol. 23, no. 1, pp. 27–34, 2021.

[5] I. A. R. Simbolon, I. Gunawan, I. O. Kirana, R. Dewi, and S. Solikhun, "Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar," *Journal of Computer System and Informatics (JoSYC)*, vol. 1, no. 2, pp. 54–60, 2020.

[6] M. M. Lucini, P. J. Van Leeuwen, and M. Pulido, "Model error estimation using the expectation maximization algorithm and a particle flow filter," *SIAM-ASA Journal on Uncertainty Quantification*, vol. 9, no. 2, pp. 681–707, 2021, doi: 10.1137/19M1297300.

[7] I. M. W. Gede Wisnu Bhaudhayana, "Implementasi Algoritma Kriptografi Aes 256 Dan Metode Steganografi Lsb Pada Gambar Bitmap," *Angewandte Chemie International Edition, 6(11), 951–952.*, vol. 3, no. 1, pp. 10–27, 2018.

[8] Y. Christian and Heri, "Penerapan Metodologı Waterfall dalam Pengembangan Communıty Based Websıte untuk Membagıkan Cerıta Hıdup dan Kebıjaksanaan Manula," *COMBINES: Conference on Management, Business, Innovation, Education and Social Science*, vol. 1, no. 1, pp. 616–622, 2021.

[9] D. W. Hoffman, "No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title".

[10] Istianah, Hapipah, and E. Oktaviana, "3 1,2,3," *Jurnal Kreaktifitas Pengabdian Kepada Masyarakat (PKM)*, vol. 3, no. April, pp. 119–126, 2020.

[11] R. V. H. Chandra, A. Kusyanti, and M. Data, "Analisis Performa Proses Enkripsi dan Dekripsi Menggunakan Algoritme AES-128 Pada Berbagai Format File," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 3, no. 1, pp. 481–486, 2019.