

Implementasi Aplikasi Enkripsi Dekripsi File Dokumen Menggunakan Algoritma Aes Pada *Cloud Computing* (Studi Kasus Prodi Teknologi Rekayasa Komputer Jaringan)

Risma Arifa¹, Husaini², Fachri Yannuar Rudi F³

^{1,2,3} Jurusan Teknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe
Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA

¹rismaarifa778@gmail.com, ²husaini@pnl.ac.id

³fachri@pnl.ac.id

Abstrak— Perkembangan teknologi sangat dibutuhkan oleh kehidupan manusia dalam setiap kegiatannya. Ilmu teknologi yang semakin berkembang khususnya dalam bidang ilmu komputer dan semakin meningkatnya penggunaan komputer dalam kehidupan sehari-hari. Selama ini pengguna banyak merasa tidak aman dalam proses pengiriman dan penyimpanan data melalui komputer. Untuk mengatasi permasalahan itu dapat dilakukan enkripsi dan dekripsi dengan memanfaatkan metode AES. Penelitian ini bertujuan mengetahui waktu yang dibutuhkan sistem dalam mengunggah dan mengunduh file dokumen melalui *cloud*. Dalam penelitian ini digunakan sebuah metode AES atau algoritma enkripsi yang dirancang untuk mengenkripsi dan mendekripsi informasi dengan tingkat keamanan yang tinggi. Melalui implementasi aplikasi ini, dapat diketahui cara melindungi data yang ditransfer antara perangkat dan *cloud*, serta data yang disimpan di *cloud*, dengan menggunakan algoritma AES untuk enkripsi dan dekripsi. Dengan demikian, keamanan data dan privasi akan terjaga dengan baik. Pengujian dilakukan pada file berukuran 1,63 mb, waktu yang dibutuhkan untuk melakukan *upload* file yaitu 0,0203 detik dan waktu yang dibutuhkan untuk melakukan *download* file yaitu 0,0078 detik. Aplikasi ini memiliki kinerja yang sangat cepat dalam pengunggahan dan pengunduhan file, waktu yang dibutuhkan berdasarkan ukuran setiap file. Semakin besar ukuran file yang akan di unggah atau diunduh, maka semakin lama waktu yang dibutuhkan. Berdasarkan penelitian tersebut, aplikasi ini memiliki kinerja yang baik dalam melakukan *transfer* file serta aman dalam menjaga keamanan file dokumen.

Kata kunci— *Advanced Encryption Standard (AES), Cloud Computing, File Dokumen, Kriptografi*

Abstract— *Technological developments are needed by human life in every activity. Technological science is increasingly developing, especially in the field of computer science and the increasing use of computers in everyday life. So far, many users feel unsafe in the process of sending and storing data via computer. To overcome this problem, encryption and decryption can be carried out using the AES method. This research aims to determine the time required for the system to upload and download document files via the cloud. In this research, an AES method or encryption algorithm is used which is designed to encrypt and decrypt information with a high level of security. Through the implementation of this application, it can be seen how to protect data transferred between devices and the cloud, as well as data stored in the cloud, by using AES algorithm for encryption and decryption. In this way, data security and privacy will be well maintained. The test was carried out on a file measuring 1.63 MB, the time required to upload the file was 0.0203 seconds and the time required to download the file was 0.0078 seconds. This application has very fast performance in uploading and downloading files, the time required is based on the size of each file. The larger the file size to be uploaded or downloaded, the longer it will take. Based on this research, this application has good performance in transferring files and is safe in maintaining the security of document files.*

Keywords— *Advanced Encryption Standard (AES), Cloud Computing, Document Files, Cryptography*

I. PENDAHULUAN

Perkembangan teknologi sangat dibutuhkan oleh kehidupan manusia dalam setiap kegiatannya. Ilmu teknologi yang semakin berkembang khususnya dalam bidang ilmu komputer dan semakin maraknya penggunaan sistem komputer. Seperti penggunaan jaringan internet dalam berbagi dan bertukar informasi. Perkembangan ini

pun sangat berpengaruh terhadap keamanan jaringan komputer khususnya pengamanan file dokumen. Keamanan file dokumen diperlukan untuk menjaga agar informasi yang tersimpan tidak dapat dibaca atau dibuka oleh pihak yang tidak berhak[1]

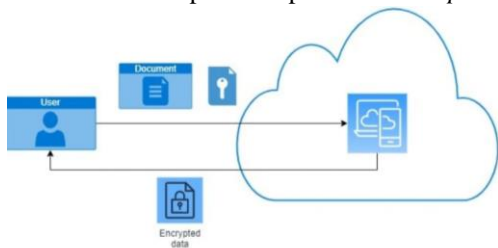
Banyaknya penyadapan dokumen penting dan rahasia dapat menyebabkan keamanan dalam bertukar informasi pada internet menjadi sangat rendah dan rentang terhadap

penyalahgunaan. Dengan meningkatnya tuntutan keamanan informasi berupa dokumen, maka dibutuhkan suatu sistem layanan keamanan jaringan komputer berupa enkripsi dokumen pada cloud computing menggunakan teknik kriptografi[2] Dengan meningkatnya tuntutan keamanan informasi berupa dokumen, maka dibutuhkan suatu sistem layanan keamanan jaringan komputer berupa enkripsi dokumen pada cloud computing menggunakan teknik kriptografi. AES menggunakan kunci simetris yang sama untuk enkripsi dan dekripsi, yang berarti kunci yang sama digunakan untuk mengamankan data dan mendekripsinya Kembali[3]

Implementasi aplikasi ini, peserta studi kasus akan mengerti bagaimana cara melindungi data yang ditransfer antara perangkat dan cloud, serta data yang disimpan di cloud, dengan menggunakan algoritma AES untuk enkripsi dan dekripsi. Dengan demikian, keamanan data dan privasi akan terjaga dengan baik.

II. METODOLOGI PENELITIAN

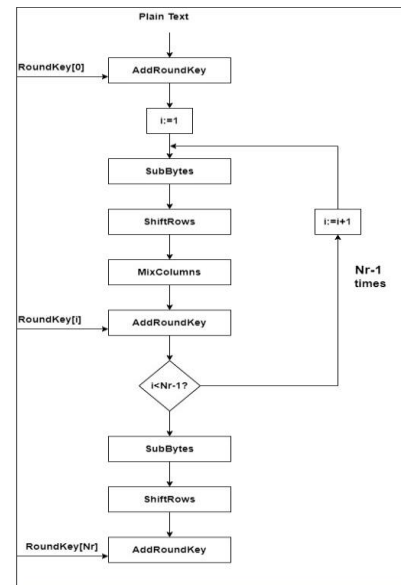
Arsitektur enkripsi/dekripsi dalam cloud computing merujuk pada infrastruktur dan teknologi yang digunakan untuk melindungi keamanan data yang disimpan dan diproses di lingkungan komputasi awan. Ini melibatkan penggunaan teknik enkripsi dan dekripsi data untuk mengamankan informasi saat disimpan, ditransfer, dan diakses dalam lingkungan cloud dapat dilihat pada gambar 1 Arsitektur Enkripsi/Dekripsi Cloud Computing.



Gambar 1 Arsitektur Enkripsi/Dekripsi Cloud Computing

A. Rancangan Flowchart Algoritma AES

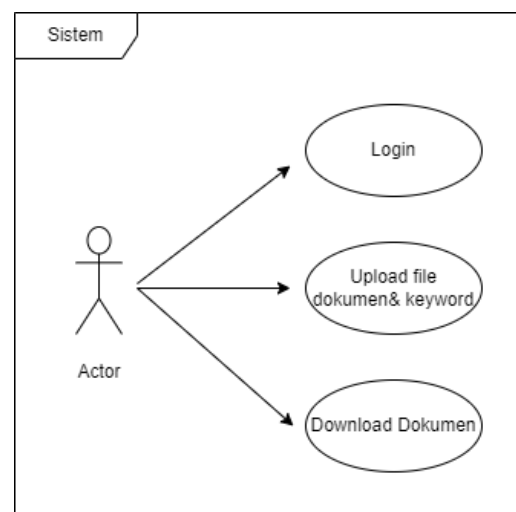
Flowchart algoritma AES terdiri dari serangkaian langkah-langkah yang menggambarkan proses enkripsi dan dekripsi data menggunakan algoritma AES.



Gambar 2 Flowchart AES

B. Rancangan Use Case Diagram

Pada tahapan ini dilakukan rancangan use case diagram yang digunakan untuk menggambarkan fungsional dari aplikasi enkripsi file dokumen. seperti pada gambar 3.



Gambar 3. Use Case Diagram Aplikasi enkripsi file dokumen

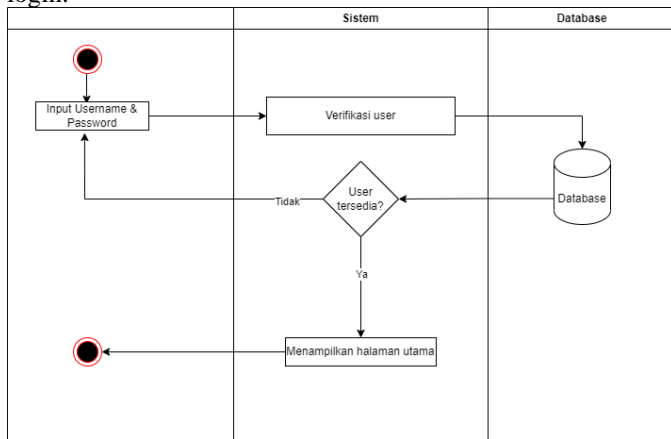
C. Diagram Activity

Pada tahapan diagram activity akan menjelaskan urutan dari aktifitas dari suatu proses setiap sebuah sistem yang terdapat pada sebuah perangkat lunak yang akan dirancang

1. Diagram Activity Login

Pada gambar 4 diagram activity login, user memasukkan inputan username & password pada halaman login aplikasi. tersedia maka sistem akan kembali ke halaman

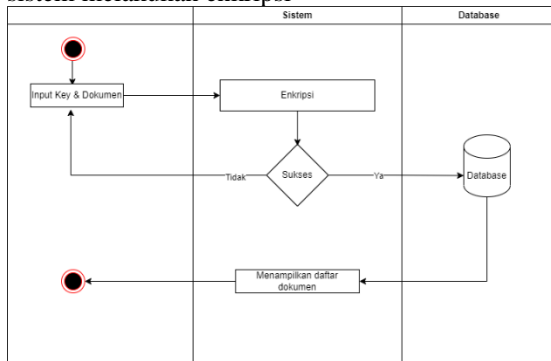
login.



Gambar 4 Diagram Activity login

2. Diagram Activity Upload Dokumen

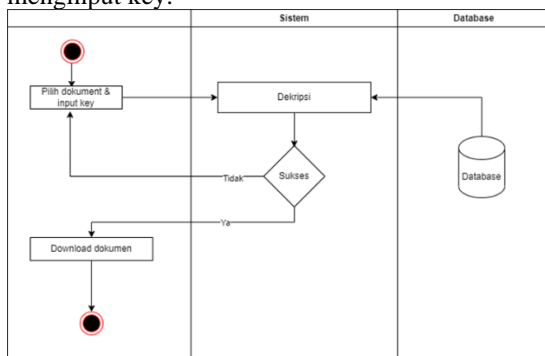
Pada gambar 5 diagram activity upload dokumen, user mengupload dokumen dan menginput key, kemudian sistem melakukan enkripsi



Gambar 5 Diagram Activity Upload Dokumen

3. Diagram Activity Download dokumen

Pada gambar 6 diagram activity download dokumen, user memilih dokumen yang akan didownload kemudian menginput key.



Gambar 3 Diagram Activity Download dokumen

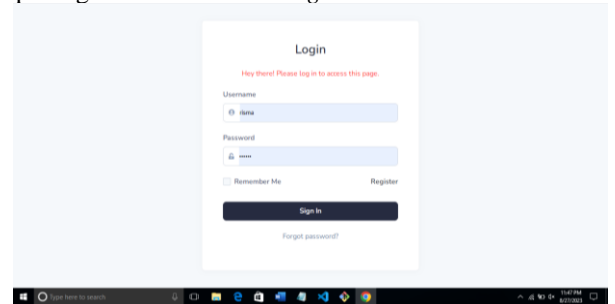
III. HASIL DAN PEMBAHASAN

A. Implementasi User Interface

Implementasi interface adalah sebuah tampilan pada suatu sistem yang memungkinkan pengguna untuk berinteraksi dengan perangkatnya secara langsung atau melalui jaringan Rangkaian Perangkat

1. Halaman awal aplikasi

Berikut ini merupakan tampilan awal pada aplikasi enkripsi dekripsi dokumen, halaman ini merupakan halaman *register/login* bagi pengguna, seperti pada tampilan gambar 7 halaman *Login*.



Gambar 7 Halaman Login

2. Tampilan halaman utama

Tampilan awal setelah berhasil login ke dalam akun terdiri dari fitur dashboard, Data center seperti pada tampilan gambar 8 Tampilan Halaman Utama



Gambar 8 Tampilan Halaman Utama

3. Halaman Profile

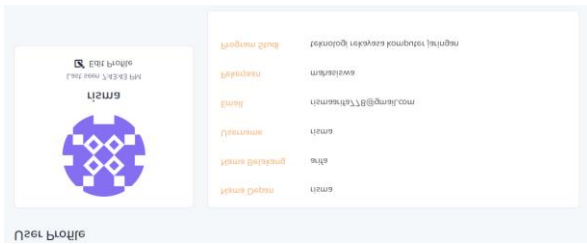
Pada fitur ini pengguna dapat mengisi informasi pribadi pengguna seperti mengisi nama depan, nama belakang, *username*, *email*, pekerjaan dan program studi seperti pada tampilan pada gambar 9 halaman *profile*.



Gambar 9 Halaman Profile

4. Tampilan halaman profil pengguna

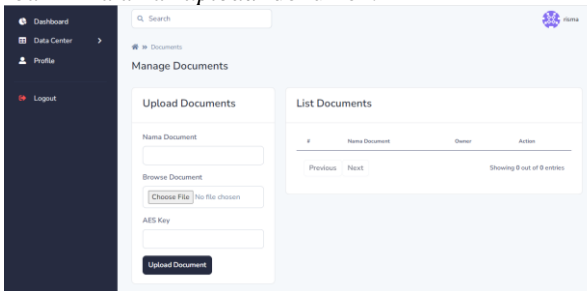
Pada halaman ini menampilkan informasi pribadi dari user berupa nama depan, nama belakang, *username*, *email*, pekerjaan, program studi pada tampilan gambar 10 halaman *profile* pengguna.



Gambar 10 Halaman Profile Pengguna

5. Halaman data Center

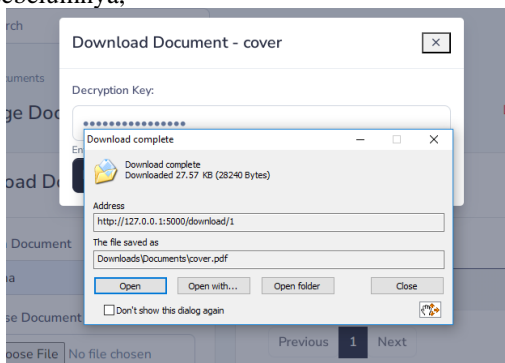
Pada menu halaman ini pengguna dapat mengupload dokumen dengan memberi nama dokumen terlebih dahulu pada kolom "Nama Document" seperti tampilan pada gambar 11 halaman *upload* dokumen.



Gambar 11 Halaman Upload Dokumen

6. *Download File*

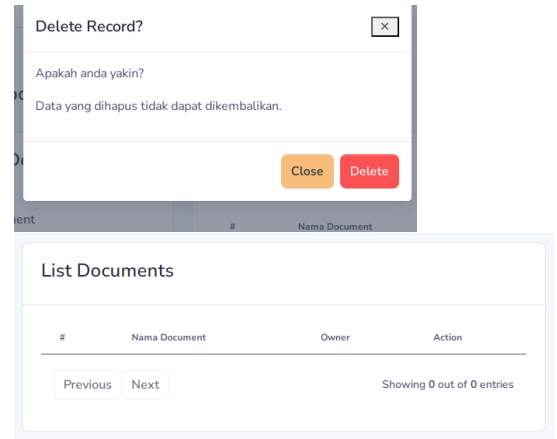
Setelah mengupload dokumen pengguna dapat Mendownload dokumen yang telah diupload sebelumnya,



Gambar 1 Mendownload dokumen

7. Menghapus File

Pada layout terdapat fitur action untuk mendownload dokumen dan untuk menghapus dokumen, ketika menekan button download maka akan muncul pop up untuk mendelete dokumen menekan delete maka dokumen yang telah diupload akan terhapus seperti tampilan pada gambar 13.



Gambar 2 menghapus dokumen

B. Hasil Pengujian

Pengujian Waktu Komputasi

Berikut adalah hasil pengujian upload dan download, pengujian ini dilakukan sebanyak 9 kali pengujian upload dan 9 kali pengujian download yang hasilnya terlihat pada table 1 untuk pengujian *upload* dan table 1 untuk pengujian *download* seperti dibawah ini :

1. Hasil Pengujian *Upload Cloud Computing* (Heroku)

Pengujian upload dokumen pada *cloud computing* dilakukan pada beberapa tipe file dokumen seperti pdf,docx,txt. Pengujian ini dilakukan untuk mengetahui kecepatan waktu upload dokumen berdasarkan ukuran file yang diupload

Ini berarti bahwa untuk mengunggah file dengan nama

No	Nama File	Tipe File	Waktu
1.	Laporan1	pdf	0,0203 seconds
2.	Laporan2	pdf	0,0639 seconds
3.	Laporan3	pdf	0,0077 seconds
4.	Makalah1	Docx	0,0080 seconds
5.	Makalah2	Docx	0,0267 seconds
6.	Makalah3	Docx	0,0059 seconds
7.	Test1	Txt	0,0039 seconds
8.	Test2	Txt	0,0053 seconds
9.	Test3	Txt	0,0036 seconds

"Laporan1" yang memiliki tipe file pdf dan berukuran 1,63 megabyte, diperlukan waktu sekitar 0,0203 detik. Penjelasan serupa berlaku untuk baris-baris selanjutnya dalam tabel tersebut

2. Hasil Pengujian Download *Cloud Computing* (Heroku)Tabel 2 Pengujian *Download cloud Computing*

No	Nama File	Tipe File	Waktu
1.	Laporan1	pdf	0,0078 seconds
2.	Laporan2	pdf	0,0162 seconds
3.	Laporan3	pdf	0,0046 seconds
4.	Makalah1	Docx	0,0054 seconds
5.	Makalah2	Docx	0,0300 seconds
6.	Makalah3	Docx	0,0019 seconds
7.	Test1	Txt	0,0018 seconds
8.	Test2	Txt	0,0032 seconds
9.	Test3	Txt	0,0020 seconds

Pada pengujian pertama, file dengan nama "Laporan1" dalam format pdf berukuran 1,63 mb diunduh dalam waktu 0,0078 detik. Dari tabel ini, dapat dilihat bagaimana ukuran dan jenis file dapat mempengaruhi waktu yang diperlukan untuk mengunduh file. File-file dengan ukuran lebih besar biasanya memerlukan waktu lebih lama untuk diunduh.

IV. SIMPULAN

Berdasarkan hasil analisis data, dapat disimpulkan bahwa "Implementasi Aplikasi Enkripsi Dekripsi File Dokumen Menggunakan Algoritma AES Pada Cloud Computing" berhasil dilakukan dengan simpulan sebagai berikut:

1. Berdasarkan pengujian upload dan download yang telah diberikan, terlihat bahwa pada saat pengujian upload mengunggah file dengan nama "Laporan1" yang memiliki tipe file pdf dan berukuran 1,63 megabyte, diperlukan waktu sekitar 0,0203 detik. Pada pengujian download pertama, file dengan nama "Laporan1" dalam format pdf berukuran 1,63 mb diunduh dalam waktu 0,0078 detik.
2. Ukuran dan jenis file mempunyai peran penting dalam menentukan waktu yang dibutuhkan untuk proses upload dan download. File-file dengan ukuran lebih besar cenderung memerlukan waktu lebih lama untuk diproses.
3. Format atau tipe file juga dapat memengaruhi kecepatan upload dan download, serta potensi kesulitan dalam membuka file setelah diunduh. Evaluasi dari hasil pengujian ini penting untuk memahami perbedaan dalam kinerja proses upload dan download berdasarkan berbagai karakteristik file yang berbeda.

REFERENSI

- [1] Ikhsan, M. *Rancang Bangun Aplikasi Pengamanan Dokumen Sertifikat Menggunakan Algoritma AES-128 BIT Advances Encryption Standard. Rancang Bangun Aplikasi Pengamanan Dokumen Sertifikat Menggunakan Algoritma AES-128 BIT Advances Encryption Standard*, 1(1), 1–8. 2018
- [2] Laia, R. (2020). *Implementasi Algoritma Aes 256 Bit Dan Lsb Untuk Pengamanan dan Penyisipan Pesan Teks Pada File Audio. Pelita Informatika: Informasi dan Informatika*, 8(April), 467–469.
- [3] Saputra Djong, H., & Siswanto, S. (2022). *Implementasi Kriptografi Dengan Menggunakan Metode Rc4 Dan Aes-256 Untuk Mengamankan File Dokumen Pada Pt Varnion Technology Semesta. Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) Jakarta-Indonesia, September*, 149–158.
- [4] Ananda, S. P., & Lukman, S. (2022). *Analisa Metode Kriptografi Modern Advance Encryption Standard (AES) 128 Bit dalam Mengenkripsi dan Mendekripsi File Dokumen Digital. Jurnal Ilmiah Komputasi*, 21(3), 333–344.
- [5] Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). *Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). Jurnal Pendidikan Sains dan Komputer*, 2(01), 163–171.