**OKTAL : Jurnal Ilmu Komputer dan Sains**
Volume 1, No. 06, Juni (2022)
E-ISSN 2828-2442 (media online)
Hal 758-762

# Analisa dan Implementasi Kriptografi File Dokumen Dengan Metode Algoritma Advanced Encryption Standard (AES) Berbasis Web

**Riyan Wahyu Pratama[1], Teti Desyani[2]**

[1]Fakultas Teknik, Program Studi Teknik Informatika, Universitas Pamulang, Tangerang Selatan, Indonesia
Email: [1]Ryanwahyu53@gmail.com , [2]Tetidesyani@gmail.com

**Abstrak**− Keamanan dan kerahasiaan saat melakukan pertukaran data dan informasi menjadi hal yang sangat penting pada era teknologi informasi dan komunikasi saat ini, oleh karena itu dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah kriptografi. Terdapat cukup banyak metode algoritma pada kriptografi salah satunya yaitu metode algoritma *Advanced Encryption Standard* (AES), merupakan algoritma kriptografi yang dapat digunakan untuk mengamakan data. Dengan adanya implementasi sistem kriptografi sehingga dapat mengurangi kemungkinan suatu resiko kejahatan keamanan data karena pesan atau file dan dokumen terlindungi. Adapun hasil yang didapatkan dari penelitian ini yaitu implementasi sebuah sistem kriptografi file dokumen dengan menggunakan metode algoritma *Advanced Encryption Standard* (AES) kemudian diproses, sehingga sistem dapat melakukan sebuah enkripsi dan dekripsi..

**Kata Kunci:** Keamanan Data, Kriptografi, Advanced Encryption Standard (AES)

**Abstract**−*Security and confidentiality when exchanging data and information are very important in the current era of information and communication technology, therefore a branch of science has been developed that studies ways to secure data or known as cryptography. There are quite a number of algorithmic methods in cryptography, one of which is the Advanced Encryption Standard (AES) algorithm, which is a cryptographic algorithm that can be used to secure data. With the implementation of a cryptographic system so as to reduce the possibility of a data security crime risk because messages or files and documents are protected. The results obtained from this study are the implementation of a document file cryptography system using the Advanced Encryption Standard (AES) algorithm method and then processed, so that the system can perform encryption and decryption.*

**Keywords**: *Data Security, Cryptography, Advanced Encryption Standard (AES)*

## 1. PENDAHULUAN

Keamanan dan kerahasiaan saat melakukan pertukaran data dan informasi menjadi hal yang sangat penting pada era teknologi informasi dan komunikasi saat ini, oleh karena itu dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah kriptografi.

Menurut (Basyiah dan kawan-kawan, 2017), Dalam kriptografi terdapat dua konsep utama yaitu enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi/data “pesan asli” (*plaintext*) yang hendak dikirim diubah atau menjadi bentuk yang hampir tidak dikenali “pesan acak” (*ciphertext*) sebagai informasi atau data awalnya menggunakan algoritma tertentu. Sedangkan dekripsi adalah mengubah kembali bentuk tersamar dari informasi atau data pesan tersebut menjadi informasi awal..

Dengan metode algoritma Advanced Encryption Standard (AES) perlu diterapkan, sehingga dapat mengurangi kemungkinan suatu resiko kejahatan keamanan data karena pesan atau file dan dokumen terlindungi.

## 2. METODOLOGI PENELITIAN

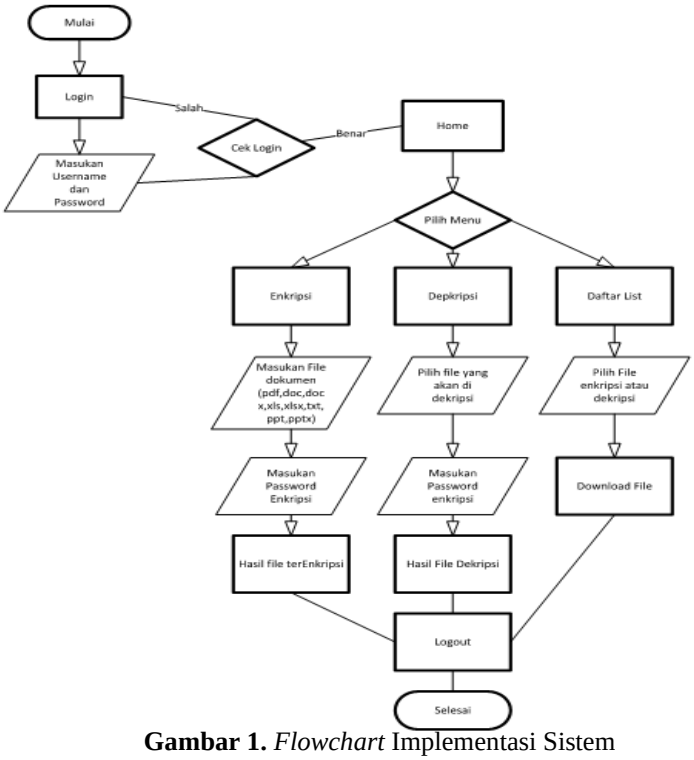
### 2.1 Metode Algoritma *Advanced Encryption Standard* (AES)

Algoritma *Advanced Encryption Standard* (AES) adalah suatu algoritma block chiper dan mempunyai sifat simetri yang menggunakan kunci simetri pada waktu proses enkripsi dan dekripsi . Pada tahun 2001, AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh NIST (*National Institute of Standard and Technology*) sebagai pengganti algoritma DES (*Data*

**OKTAL : Jurnal Ilmu Komputer dan Sains**
Volume 1, No. 06, Juni (2022)
E-ISSN 2828-2442 (media online)
Hal 758-762

*Encryption Standard*) yang sudah berakhir masa penggunaannya. Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit. (Asri Prameshwari, Nyoman Putra Sastra, 2018.

### 2.2. *Flowchart* Implementasi Sistem




**Gambar 1.** *Flowchart* Implementasi Sistem

Pada gambar diatas merupakan flowchart sistem usulan ini diusulkan beberapa hal yang menjadi batasan masalah yang akan diberikan solusi atau alternatif dengan maksud memberikan kemudahan dan keamanan dalammengirim dokumen melaui media email, whatsapp dan lain-lain.

Pada tabel 1. menjelaskan beberapa masalah pada sistem sebelumnya dan juga solusi untuk permasalahanya sebagai berikut :

**Tabel 1.** Masalah dan Solusi

| Masalah | Solusi |
|---|---|
| Sistem pengiriman dokumen sebelumnya dilakukan secara manual dengan menngirim melalui *e-mail* dan *WhatsApp* | Membuatkan sistem keamanan dokumen yang tidak dapat dilihat oleh orang lain |
| Dokumen yang dikirimkan masih dapat dilihat oleh orang lain untuk saat ini | Dokumen yang dikirimkan tidak akan dapat dilihat oleh orang lain |

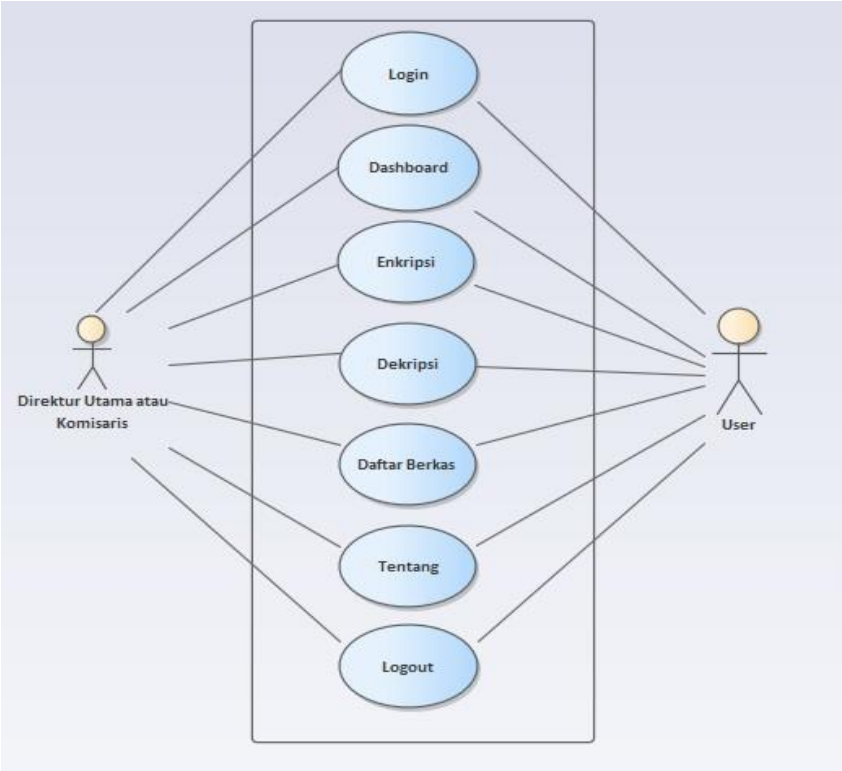
OKTAL : Jurnal Ilmu Komputer dan Sains
Volume 1, No. 06, Juni (2022)
E-ISSN 2828-2442 (media online)
Hal 758-762

# 3. ANALISA DAN PEMBAHASAN

Pada bab ini akan menjelaskan mengenai Analisa dan Perancangan sistem yang di usulkan pada CV. Prima Glanze Utama.

## 3.1 Analisa Sistem Yang Diusulkan

### 3.1.1 *Usecase* Diagram




**Gambar 2.** *Usecase* Diagram

Pada gambar diatas, terdapat 3 aktor dimana direktur utama atau komisaris dan user/client sebagai pengguna sistem. Dalam sistem mempunyai 7 use case diagram, dimana yang pertama adalah use case login ini kedua aktor harus melakukan login terlebih dahulu untuk bisa menggunakan sistem enkripsi dokumen ini, yang kedua adalah use case dashboard dimana ketiga aktor ini bisa melihat total user, total dokumen yang sudah di enkripsi maupun dideksripsi, yang ketiga adalah use case enkripsi dimana ketiga aktor bisa melakukan enkripsi dokumen, yang keempat adalah use case dekripsi dimana ketiga aktor bisa melakukan pengenkripsian data dokumen, yang ke lima use case daftar berkas, dimana ketiga aktor dapat melihat status file yang sudah terenkripsi maupun yang terdekripsi, dan ketiga aktor dapat mengunduh hasil dokumen yang sudah terenkripsi atau yang sudah terdekripsi, yang ke enam use case tentang, dimana use case ini berisi tentang implementasi sistem kriptografi untuk pengamanan data dokumen, yang ketujuh use case logout dimana ketiga aktor dapat keluar dari sistem kriptografi.

## 3.2 Pembahasan

Pengujian kuesioner merupakan pengujian yang dilakukan secara objektif dimana diuji secara langsung ke lapangan yaitu yang bertempat di CV. Prima Glanze Utama dengan membuat kuesioner mengenai kepuasan pengguna dengan mengambil sampel sebanyak 2 orang yaitu Direktur Utama dengan Komisaris dari CV. Prima Glanze Utama. Dari hasil

OKTAL : Jurnal Ilmu Komputer dan Sains
Volume 1, No. 06, Juni (2022)
E-ISSN 2828-2442 (media online)
Hal 758-762

kuesioner tersebut dilakukan perhitungan untuk dapat diambil kesimpulan terhadap penilaian aplikasi enkripsi dekripsi dokumen. Kuesioner ini terdiri dari 5 pernyataan (contoh kuesioner dapat dilihat pada lampiran) dengan menggunakan skala likert dengan skala 1 sampai 5, dengan ketentuan skala untuk tiap pertanyaan.

# 4. IMPLEMENTASI

## 4.1 Implementasi Sistem

### 4.1.1 Implementasi Perangkat Keras

Untuk menjalankan website yang telah dirancang maka dibutuhkan perangkat keras sebagai tempat untuk menerapkannya. Adapun perangkat keras yang dibutuhkan tersebut adalah sebagai berikut :

**Tabel 2.** Perangkat Keras

| No | Nama | Spesifikasi Minimum |
|---|---|---|
| 1. | Sistem Operasi | Windows 7 64bit |
| 2. | Processor | AMD C-70 1.00 GHz (Atau serata) |
| 3. | RAM | 2 GB |
| 4. | Monitor | 11.3” Radeon™ HD Graphics |

### 4.1.2 Implementasi Perangkat Lunak

Perangkat lunak yang digunakan untuk mengimplementasikan sistem yaitu sebagai berikut :

**Tabel 3.** Perangkat Lunak

| No. | *Tools* | *Software* Pendukung |
|---|---|---|
| 1. | Web Browser | Google Chrome Version 97.0 |
| 2. | XAMPP | XAMPP for Windows 7.4.27 |
| 3. | PHP | PHP 7.4.23 |
| 4. | Data Base | Maria DB 10.4.21 |

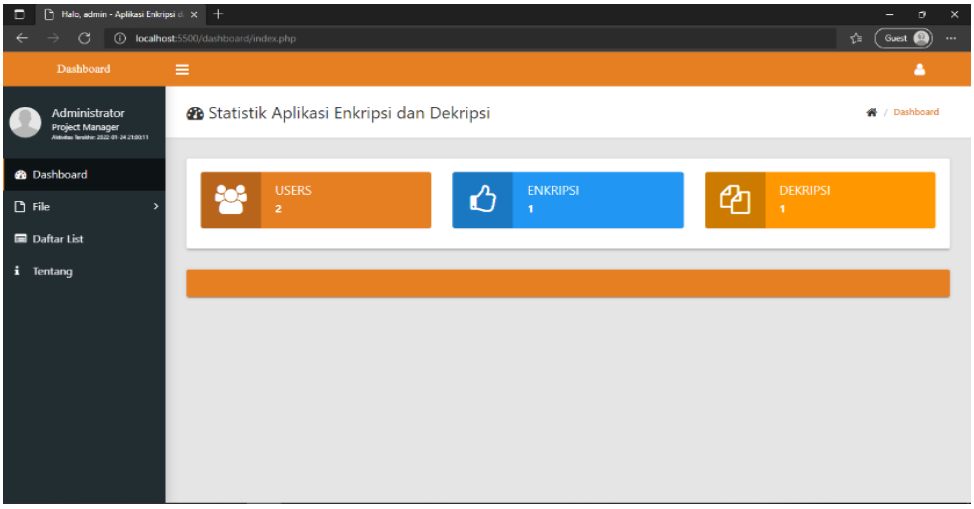
## 4.2 Tampilan Antarmuka

a. Halaman *Login*


**Gambar 3.** Halaman *Login*

**OKTAL : Jurnal Ilmu Komputer dan Sains**
Volume 1, No. 06, Juni (2022)
E-ISSN 2828-2442 (media online)
Hal 758-762

b. Halaman *Dashboard*




**Gambar 4.** Halaman *Dashboard*

## 5. KESIMPULAN

Berdasarkan hasil pengujian yang telah dilakukan terhadap Analisa dan Implementasi Kriptografi File Dokumen Dengan Metode Algoritma *Advanced Encryption Standard* (AES) Berbasis Web (Studi kasus: CV.Prima Glanze Utama) maka dapat disimpulkan bahwa proses enkripsi dimulai dari menentukan chiper key, kemudian dimasukan sebagai *AddRoundKey*, dilanjutkan dengan proses *SubByte*, *ShitfRows*, *MixColloums* kemudian dijadikan *Output.*Penerapan algoritma *Advanced Encryption Standard* (AES) pada dokumen, memecahkan kata per-kata ke dalam *array* untuk dienkripsi. Aplikasi yang diimplementasikan dapat diakses di komputer, *smartphone*, dan tablet selagi *device* tersebut memiliki web *browser*.

## REFERENCES

Asri Prameshwari, N. (September 2018). IMPLEMENTASI ALGORITMA ADVANCED ENCERYPTION STANDARD (AES) 128 UNTUK ENKRIPSI DAN DEKRIPSI FILE DOKUMEN. Junal Eksplora Informatika, Vol.8, No.2.

Binanda Wicaksana, M. (Mei 2020). PENERAPAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) UNTUK PENGAMANAN BERKAS SOAL UJIAN. Volume 10 Number 1. Page. 25-34.

Endra, A. (2018). E-Report Berbasis Web Menggunakan Metode Model View Controller Untuk Mengetahui Peningkatan Perkembangan Prestasi Anak Didik. Jurnal Sistem Informasi Dan Telematika, 9(3), 15–22.

Electronic Publication, Information from the internet

Visual Studio Code. (2017, Juni 23). Visual Studio Code Getting Started. Retrieved fromhttps://code.visualstudio.com/docs].

Monograph, edited book, book

Abdulloh. (2018). 7 in 1 Pemrograman Web untuk Pemula. Jakarta: Elex Media Komputindo.

Budiharto, W. (2014). Teori dan Implementasi. Yogyakarta: Penerbit Andi.