JURNAL SURYA ENERGY| ISSN (p): **2528-7400**| ISSN (e): **2615-871X**
DOI : https://doi.org/10.32502/jse.v8i1.6461 Vol. 8 | No. 1 | Halaman 35 - 51
[September] [2023]

Penerapan Algoritma *Advance Encryption Standard* (AES) Untuk Pengamanan *File* Pada Aplikasi Berbasis WEB

Fifmianti Bibiola[1], Toibah Umi Kalsum[2], Hendri Alamsyah[3]
[1,2,3]*Program Studi Rekayasa Sistem Komputer Universitas Dehasen Bengkulu*
fifmiantibibiola@gmail.com[1], cicik.umie@gmail.com[2], hendri.alamsyah@unived.ac.id[3]

Received 17 Juli 2023 | *Revised 0*4 September 2023 | *Accepted* 21 September 2023

ABSTRAK

Penelitian ini memiliki tujuan yaitu agar dapat menerapkan algoritma *Advanced Encryption Standard* (AES) dalam mengamankan *file* sehingga informasi didalamnya menjadi aman dan tidak dapat dipahami oleh sembarang orang. Penerapan Algoritma *Advanced Encryption Standard* (AES) dibuat menggunakan Bahasa Pemrograman PHP dan database MySQL yang dapat diakses melalui link http://fifmiantiaes.online/. Dengan adanya Aplikasi pengamanan *file* menggunakan algoritma *Advanced Encryption Standard* (AES) berbasis web dapat meningkatkan keamanan file dari pihak yang tidak berwewenang. Berdasarkan hasil pengujian yang telah dilakukan diperoleh bahwa sistem berhasil melakukan proses enkripsi dan dekripsi menggunakan Algoritma *AES*, dimana *file* dokumen tersimpan di dalam server dalam bentuk enkripsi, dan waktu proses enkripsi tergantung dari ukuran *file* dokumen, semakin besar ukuran *file*, maka semakin lama proses enkripsi yang diperlukan.

Kata kunci: *Algoritma Advanced Encryption Standard* (AES), Pengamanan *File*, Aplikasi, Berbasis Web

This research has a goal, namely to be able to apply the Advanced Encryption Standard (AES) algorithm in securing files so that the information inside is safe and cannot be understood by just anyone. The application of the Advanced Encryption Standard (AES) Algorithm is made using the PHP Programming Language and MySQL database which can be accessed via the http://fifmiantiaes.online/ link. With a file security application using the web-based Advanced Encryption Standard (AES) algorithm, it can increase file security from unauthorized parties. Based on the results of the tests that have been carried out, it is found that the system succeeded in carrying out the encryption and decryption process using the AES Algorithm, where the document files are stored on the server in encrypted form, and the encryption process time depends on the size of the document file, the larger the file size, the longer the encryption process required.

Keywords: Advanced Encryption Standard (AES) Algorithm, File Security, Application, Web-Based

I. PENDAHULUAN

Keamanan data adalah salah satu faktor yang utama dalam menjaga kerahasiaan informasi terutama yang berisi informasi sensitif yang hanya boleh diketahui isinya oleh pihak yang berhak saja (Putra & Ginting, 2017). Terlebih lagi apabila pengirimannya dijalankan melalui jaringan publik, jika data tersebut tidak diamankan terlebih dahulu, maka akan sangat mudah disadap dan diketahui isi informasinya oleh berbagai pihak yang tidak memiliki kepentingan.

Dengan berkembangnya teknologi dibidang jaringan, pengiriman pesan atau data *file* juga sudah dapat dilakukan menggunakan media jaringan (Darwis & Kisworo, 2017). Maka informasi tersebut harus membutuhkan sebuah keamanan dan kerahasiaan karena bisa saja informasi tersebut menyimpan hal rahasia atau menjadi dokumen berharga yang harus diawasi kerahasiaannya. Salah satu upaya yang dapat dilakukan untuk menyelamatkan *file* dokumen tersebut adalah dengan menggunakan sistem kriptografi (Pabokory, Astuti, & Kridalaksana, 2016). Kriptografi adalah salah satu teknik yang dipakai guna mengubah *file* yang dapat dimengerti manusia ke bentuk yang tidak dimengerti oleh manusia. Penggunaan kriptografi dalam proses pengiriman *file* menjadi hal yang wajib belakangan ini. Hal ini disebabkan oleh karena penggunaan kriptografi dapat menjadi suatu keamanan tambahan untuk proses pengamanan *file* tersebut.

Pada kriptografi terdapat beberapa algoritma yang bisa dipakai guna melakukan suatu proses kriptografi, salah satunya diantaranya ialah algoritma *Advanced Encryption Standard* (AES). *Advanced Encryption Standard* (AES) adalah algoritma yang memakai kunci dan masukan dengan panjang 128 bit. Setiap masukan 128 bit *plaintext* dimasukan ke dalam *state* yang berbentuk bujur sangkar berukuran 4 x 4 *byte*. State ini nantinya akan di *XOR* dengan *key* dan selanjutnya diolah 10 kali dengan substitusi-transformasi *liniear-addkey*.

Penelitian yang telah dilakukan oleh (Azhari, Mulyana, Perwitosari, & Ali, 2022) adalah implementasi pengamanan data pada dokumen menggunakan algoritma kriptografi *Advanced Encryption Standard* (AES)

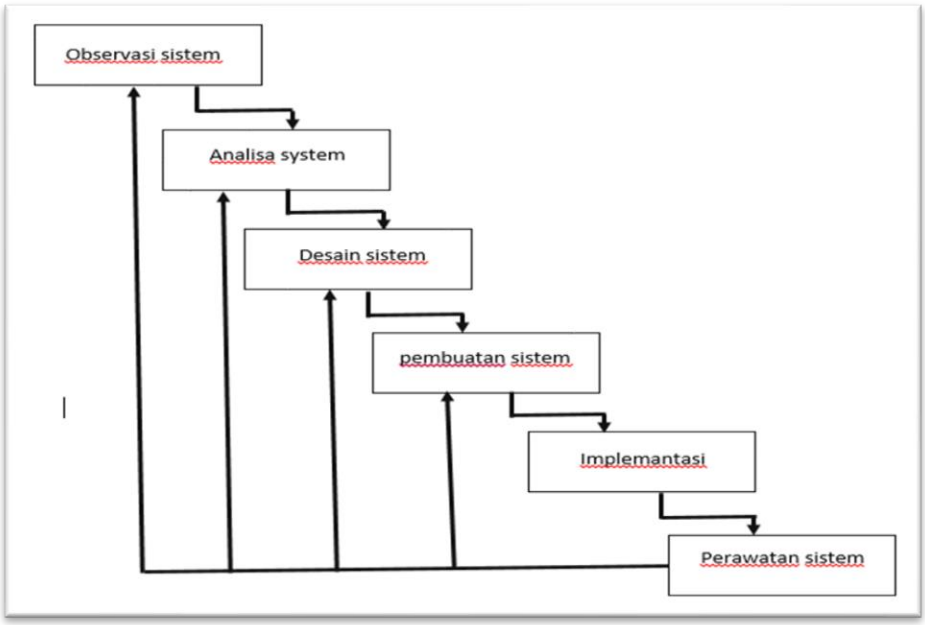
memperoleh hasil keamanan pada data atau dokumen hasil seleksi para peserta JAMKESMAS sehingga dapat lebih maksimal karena data yang di simpan telah terenkripsi dan hanya bisa dilihat keaslian *file* tersebut jika *file* tersebut telah di deskripsi. Selain *file* yang sudah di enkripsi maka akan berubah ekstensi menjadi "AES" dan *file* yang sudah di dekripsi akan kembali menjadi ekstensi seperti semula tanpa mengubah *file* keaslian data tersebut. Penelitian lainnya juga sudah dilakukan oleh (Azanuddin, Yakub, & Prayudha, 2022) berupa implementasi keamanan citra menggunakan algoritma AES-128 dengan aplikasi *client-server* dengan hasil proses enkripsi citra digital menggunakan algoritma AES 128 bit memberikan *output cipherimage* yang memiliki tingkat keamanan yang baik.

Dari dua penelitian di atas, akan dilakukan pembuatan aplikasi berbasis web dengan bahasa pemrograman PHP, *database MySQL* dan diakses melalui jaringan *web hosting*, sehingga dapat diakses kapan dan dimana saja, sehingga *user* tidak perlu melakukan proses instalasi pada komputer yang menggunakan aplikasi pengamanan *file* dengan format *pdf, doc, txt*.

II. METODE PENELITIAN

A. Metode *Waterfall*

Metode *waterfall* akan digunakan pada penelitian ini, adapun gambar 1 di bawah akan menjelaskan tahapan yang terdapat pada metode *waterfall* tersebut.



Gambar 1. Metode *Waterfall*

Pada gambar 1 dapat terlihat tahapan yang diperlukan pada metode *waterfall*. Adapun penjelasan dari tahapan metode *waterfall* adalah sebagai berikut:

1. Observasi Sistem
   Pada tahapan pertama yang dilakukan adalah melakukan observasi terhadap yang sudah menggunakan algoritma *Advanced Encryption Standard (AES)* dalam teknologi pengamanan *file*. Observasi yang dilakukan tentang tampilan, cara kerja program dan juga bagaimana mereka memproses data menggunakan algoritma *Advanced Encryption Standard (AES).*
2. Analisis Sistem
   Pada tahapan kedua yang dilakukan adalah analisis sistem dari yang sudah ada, di mana yang dianalisis adalah cara kerja, tampilan dan alur proses.
3. Desain Sistem
   Selanjutnya setelah dilakukan observasi dan analisa, maka akan dilakukan proses mendesain sistem enkripsi dan dekripsi algoritma *Advanced Encryption Standard (AES)* dengan memakai bahasa pemprograman PHP.
4. Pembuatan Sistem
   Pada tahapan keempat ialah pembuatan sistem, di mana tahapan ini akan dibuat sistem dengan memakai bahasa pemprograman PHP.
5. Implementasi

Pada tahapan kelima ialah implementasi sistem, dimana akan dilakukan proses perancangan aplikasi telah dibuat.

6. Perawatan Sistem
   Pada tahapan keenam akan dilakukan analisa kesalahan atau *error* yang terdapat pada program, kemudian akan dilakukan perbaikan.

B. Instrumen Perangkat Keras dan Perangkat Lunak

Pada penelitian ini, akan digunakan alat dan bahan yang terdiri dari perangkat lunak dan perangkat keras:

1. Perangkat Keras (*Hardware*)
   Instrumen perangkat keras (*Hardware*) yang dipakai pada penelitian seperti tabel 1.

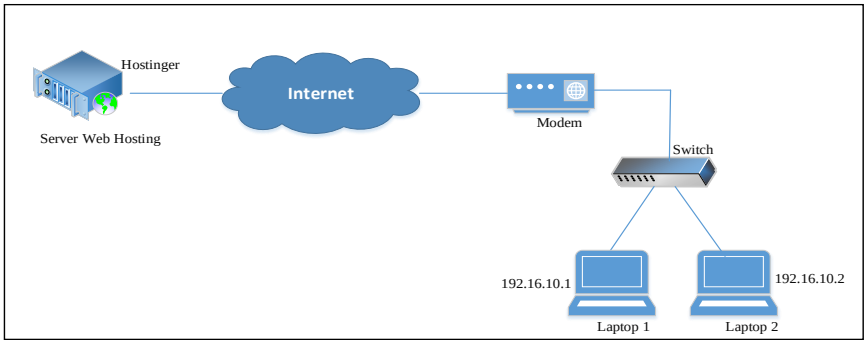
Tabel 1. Perangkat Keras (*Hadware*)

No	Kebutuhan	Perangkat	Spesifikasi
1	2 Unit laptop	Lenovo G40	Intel(R) Core i7-5500V 4 GB DDR3 1 TB HDD DVDRW, Bluetooth, Wifi, NIC VGA AMD Radeon R5-M2302GB Camera, 14 WXGA
2		HP Notebook 14-G008AURev	AMD E1-2100 APU with Radeon (TM) HD Grafik 1.00 GHz Installed RAM 2.00 GB 64-bit operating system, x64-based processor

2. Perangkat Lunak (*Software*)
   Adapun perangkat lunak (*software*) yang dipakai sebagai berikut:
   a. Sistem linux Ubuntu server 20.04
   b. PHP
   c. PHP My Admin
   d. Apache
   e. MySQL
   f. Server web hosting

C. Diagram Blok Global

Adapun diaram blok global pada rangkaian ini sebagai berikut :



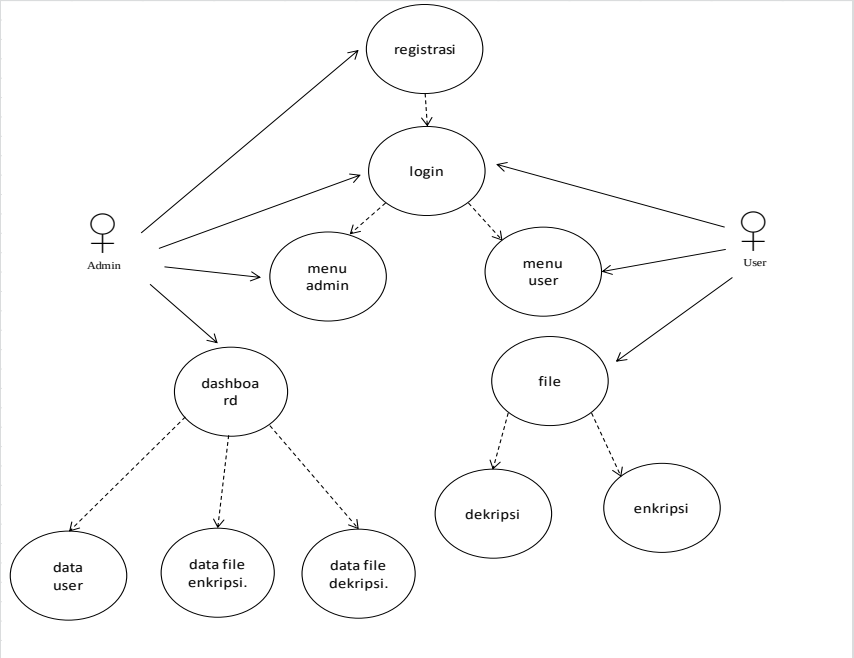
Gambar 2. Diagram Global Alat

Berdasarkan gambar 2 yang merupakan diagram global alat dapat terlihat bahwa pada rangkaian perancangan penelitian ini dibangun aplikasi keamanan *file* berbasis web, yang dapat diakses melalui jaringan internet, dengan penggujian memakai 2 unit laptop. Laptop satu digunakan sebagai user dan laptop 2 digunakan sebagai admin.

D. Desain Sistem

1. *Use case*

Gambar berikut dibawah ini merupakan desain sistem dengan *Use case*:

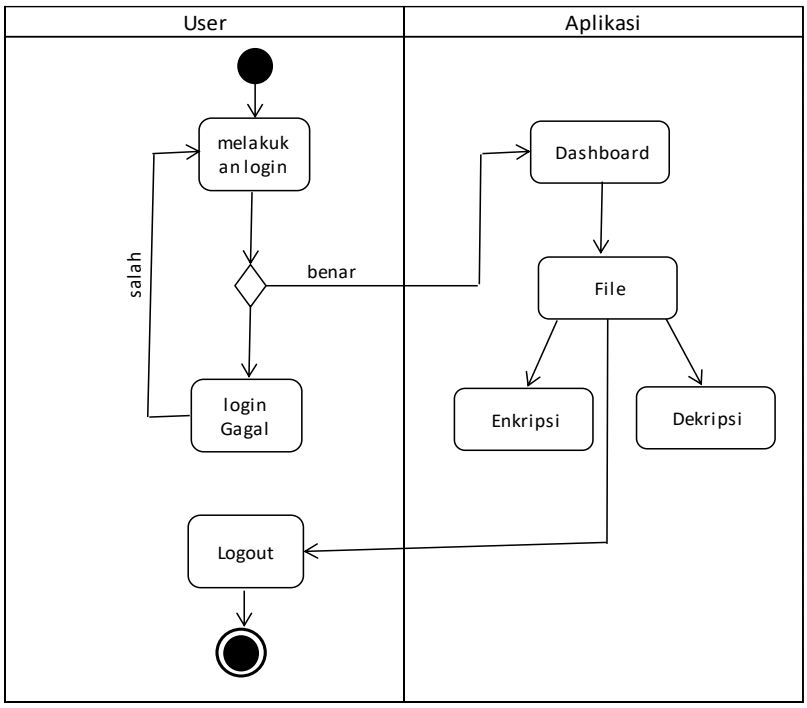


Gambar 3. *Use Case* Diagram

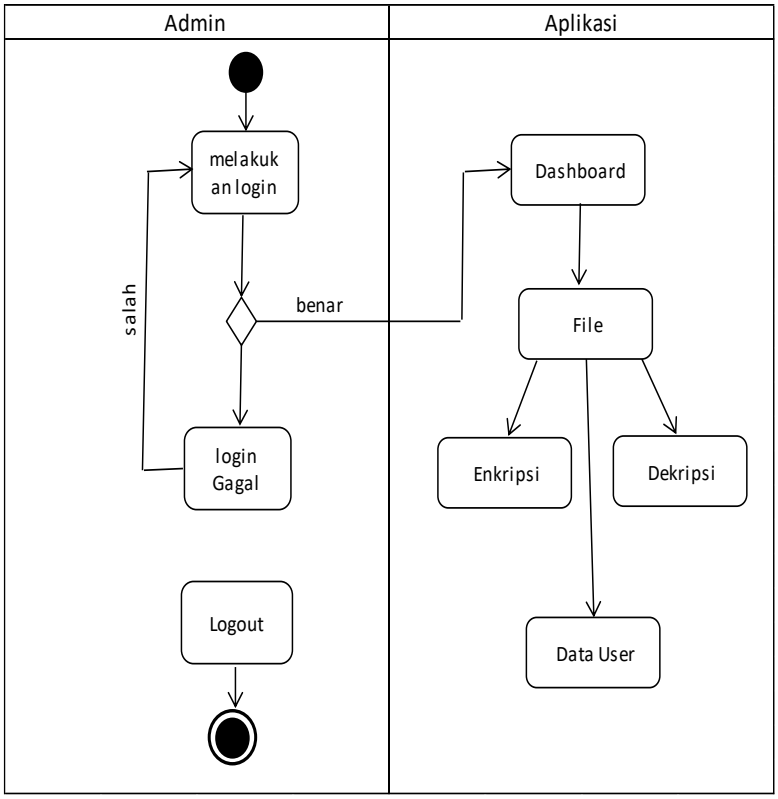
Pada gambar 3 tersebut terlihat bahwa admin dan *user* yang akan dapat mengakses aplikasi. Setiap user akan melakukan *login* pada aplikasi terlebih dahulu. Jika *login* sebagai admin maka, admin data mengelola data *user* dan data *file*. Namun jika *login* sebagai *user* dapat menginput *file* yang akan dienkripsi dan dekripsikan.

2. *Akctivity* Diagram

Activity diagram menggambarkan aktivitas *user* di mana aplikasi tersebut melibatkan *user*, admin dan aplikasi. Adapun activity diagram pada gambar 4 dan 5 sebagai berikut:



Gambar 4. *Activity* Diagram *User*

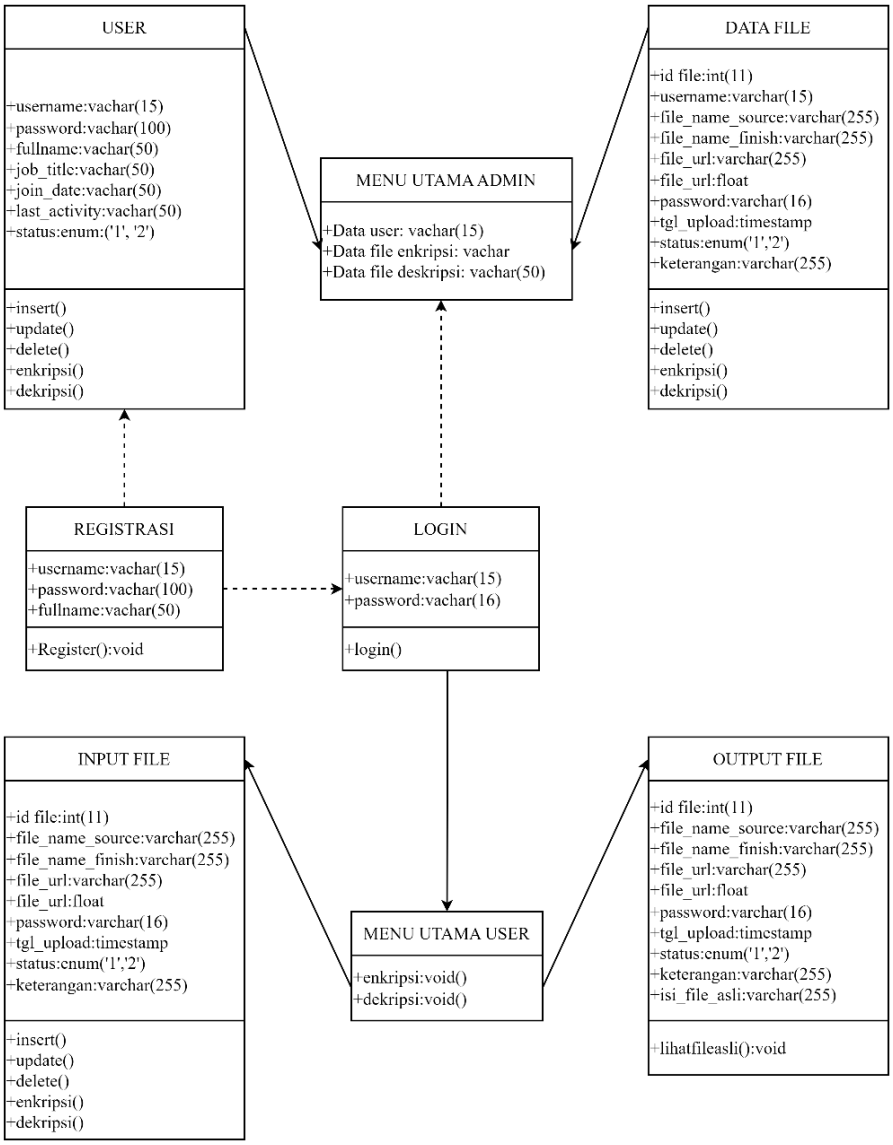


Gambar 5. ***Activity*** **Diagram** ***Admin***

Pada gambar 5 diatas apat terlihat bahwa blok *logout* memperoleh *input* dari *dashboard*.

3. ***Class*** **Diagram**

Class diagram atau diagram kelas adalah salah satu jenis diagram struktur pada UML (*Unified Modeling Language*) yang menggambarkan dengan jelas struktur serta deskripsi *class*, atribut, metode, dan hubungan dari setiap objek yang ditunjukkan pada gambar 6. *Class diagram* bersifat statis, dalam artian diagram kelas bukan menjelaskan apa yang terjadi jika kelas-kelasnya berhubungan, melainkan menjelaskan hubungan apa yang terjadi. Desain model dari diagram kelas ini sendiri dibagi menjadi dua bagian. Bagian pertama merupakan penjabaran dari database. Bagian kedua merupakan bagian dari modul MVC, yang memiliki *class interface*, *class control*, dan *class entity*.

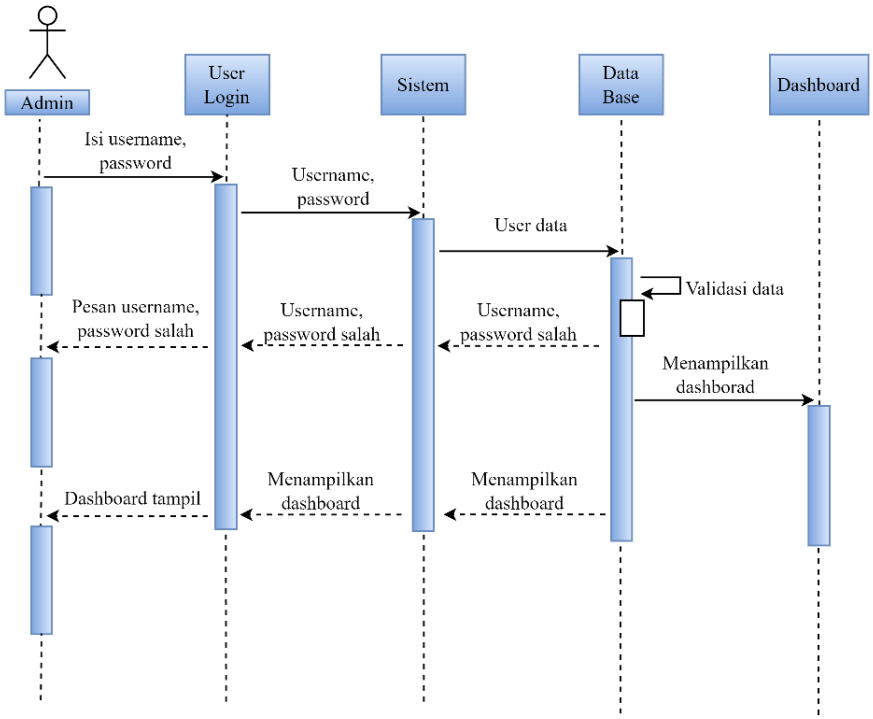


Gambar 6. *Class Diagram*

4. *Sequence* Diagram

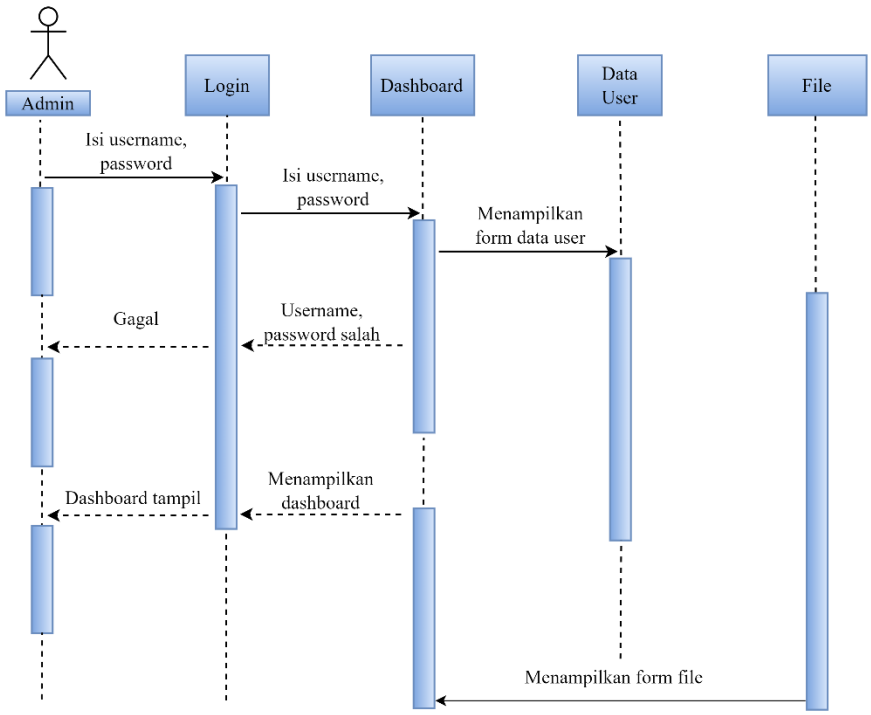
Sequence diagram atau diagram urutan menggambarkan keterhubungan antara *user* terhadap objek aplikasi yaitu sebuah diagram yang digunakan untuk menjelaskan dan menampilkan interaksi antar objek-objek dalam sebuah sistem secara terperinci. Gambar 7 merupakan *Sequence Diagram User*, di mana nantinya akan menggambarkan proses *login* dari *user*. Selain itu *sequence* diagram juga akan menampilkan pesan atau perintah yang dikirim, beserta waktu pelaksanaannya. Objek-objek yang berhubungan dengan berjalannya proses operasi biasanya diurutkan dari kiri ke kanan.

JURNAL SURYA ENERGY| ISSN (p): **2528-7400**| ISSN (e): **2615-871X**
DOI : https://doi.org/10.32502/jse.v8i1.6461 Vol. 8 | No. 1 | Halaman 35 - 51
[September] [2023]



Gambar 7. *Sequence Diagram User*

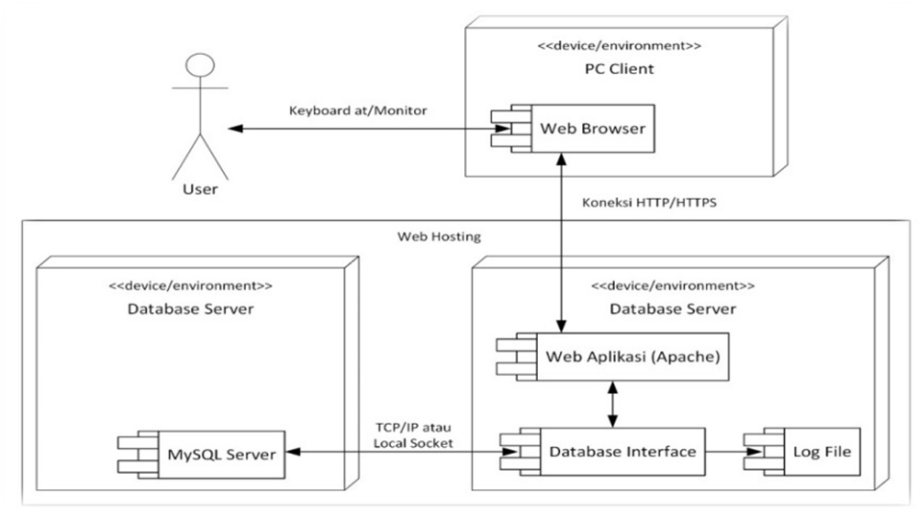
Selanjutnya gambar 8 merupakan *Sequence Diagram User*, di mana nantinya akan menggambarkan proses *login* dari admin. Admin diharapkan dapat memasukkan username dan password yang benar agar dapat masuk ke halaman akun admin.



Gambar 8. *Sequence* Diagram admin

5. *Deployment* Diagram

Berdasarkan gambar 9 dapat terlihat jenis *Deployment* diagram yang digunakan pada penelitian. *Deployment* diagram merupakan jenis diagram UML (*Unified Modeling Language*). Fungsinya untuk menggambarkan, memvisualisasikan, menspesifikasikan serta mendokumentasikan suatu proses yang terjadi dalam sebuah sistem berbasis OOP (*Object Oriented Programming*) yang akan dibangun. *Deployment* diagram sendiri adalah jenis diagram yang statis, artinya tidak akan mengalami perubahan, ketika kita merancang diagram tersebut.



Gambar 9. *Deployment* Diagram

6. Rancangan Program

Rancangan program yang akan digunakan pada penelitian ini terdiri dari:

1. Tampilan Halaman Log in
2. Tampilan *Registrasi User*
3. Administrator
4. *User*

7. Prinsip Kerja Sistem

Prinsip kerja sistem algoritma *Advanced Encryption Standard (AES),* diterapkan pada pengaman *file*, Sistem pembuatan pengamanan *file* ini menggunakan bahasa pemprograman PHP, di mana akan menyajikan *file* berupa karakter huruf, dan angka dari *file* dokumen dengan format (*pdf, docx, doc*). Yang nantinya menggunakan metode perancangan sistem *waterfall. Advanced Encryption Standard (AES)* sendiri merupakan sebuah algoritma kriftografi yang bekerja sebagai mengenkripsikan dan mendekripsikan sebuah *file* yang akan diujikan. Enkripsi dan dekripsi berbagai *file* menggunakan algoritma AES, di mana *Script* (bahasa pemrograman) berfungsi untuk mengubah *website* statis menjadi lebih dinamis dan interaktif bagi *user* (pengguna *website*).

8. Metode Pengujian Sistem

Pada proses pengujian akan dilakukan dengan menggunakan metode *blackbox,* di mana metode *blackbox* merupakan satu metode yang digunakan dalam menentukan kesalahan dan mendemonstrasikan fungsional sistem saat dioperasikan. Selanjutnya akan diketahui apakah *input* diterima dengan benar dan *output* yang dihasilkan telah sesuai dengan yang diharapkan sehingga dapat membuktikan kebenarannya. Tabel 2 merupakan rancangan pengujian yang dilakukan pada sistem.

Tabel 2. Pengujian dan Analisa

No	Jenis Pengujian	Kriteria	Hasil
1	Pengujian Enkripsi	Melakukan Enkripsi *File* dengan format pdf, docx, doc pada aplikasi berbassis web	Sistem berhasil melakukan proses enkripsi menggunakan Algoritma AES terhadap *file* dokumen asli sehingga *file* dokumen tersebut diacak dan tidak dapat dibaca.
2	Pengujian Deskripsi	Melakukan deskripsi *file* pada aplikasi berbasis web	Sistem berhasil melakukan proses dekripsi menggunakan Algoritma AES terhadap

			file dokumen terenkripsi sehingga *file* dokumen tersebut kembali seperti semula dan dapat dibaca.
3	Pengujian Keamanan *File*	Melakukan *Sniffing* menggunakan aplikasi *wireshark*	*File* yang tersimpan di dalam server dalam bentuk enkripsi dan aman dari serangan *sniffing*.
4	Pengujian waktu yang dibutuhkan dalam proses enksipsi	Waktu proses enkripsi	Waktu yang dibutuhkan dalam proses enkripsi tergantung dari ukuran *file* enkripsi, semakin besar ukuran *file* enkripsi, maka semakin lama proses enkripsi yang terjadi. Pada penujian yang dilakukan besar ukuran *file* enkripsi 30976 *bytes* dengan waktu diperlukan selama 0.00114 detik.

III. HASIL DAN PEMBAHASAN

A. HASIL

Bahasa Pemrograman *PHP* dan *database MySQL* digunakan untuk dalam pembuatan penerapan Algoritma *Advanced Encryption Standard* (AES) Untuk Pengamanan *File* pada aplikasi berbasis *web*. Aplikasi pengamanan *file* ini dapat diakses secara *online* melalui *link http://fifmiantiaes.online/* melalui internet, sehingga dapat mempermudah *user* dalam mengakses aplikasi dimana pun dan kapan pun.

Pada aplikasi pengamanan *file* menggunakan algoritma *Advanced Encryption Standard* (AES) ini, terdapat 2 hak akses yaitu *administrator* dan *user* yang memiliki fungsi berbeda-beda. Hak akses *administrator* dapat memanajemen *user* yang telah melakukan registrasi baik untuk aktivasi *user* atau menghapus *user* tersebut, selain itu administrator dapat melihat berkas *file-file* enkripsi yang telah di *upload* oleh semua *user*. Sedangkan hak akses *user* dapat melihat biodata *user*, melakukan *upload file* yang akan di enkripsi dan tersimpan di server, dan dapat *download file-file* enkripsi untuk dilakukan dekripsi agar *file* tersebut dapat dibaca kembali seperti semula.

1. Hak Akses *Administrator*

Hak akses *administrator* dapat memanajemen *user* yang telah melakukan registrasi baik untuk aktivasi *user* atau menghapus *user* tersebut, selain itu *administrator* dapat melihat berkas *file-file* enkripsi yang telah di *upload* oleh semua *user*. Adapun algoritma *Advanced Encryption Standard* (*AES*) berbasis *web* untuk hak akses *administrator* dipakai dalam antarmuka aplikasi pengamanan *file* antara lain :

a. Halaman Menu Utama *Administrator*
Halaman Menu Utama *Administrator m*erupakan halaman yang dapat diakses *administrator* setelah sukses *login*. Pada menu utama memiliki sub menu yang dapat diakses yaitu *dashboard*, *user*, daftar *file* enkripsi, dan *logout*. Gambar 10 di bawah ini merupakan halaman menu utama *administrator*

Gambar 10. Halaman Menu Utama *Administrator*

b. Halaman *User*
Halaman *User* merupakan halaman yang dapat diakses oleh *administrator* untuk melakukan aktivasi *user* baru yang mendaftar dan juga dapat menghapus *user-user* tersebut. Adapun halaman *user* seperti Gambar 11.

Gambar 11. Halaman *User*

Pada Gambar 11 tersebut terdapat aksi yang dapat dilakukan yaitu Aktif, Tidak Aktif, dan Hapus yang memiliki fungsi berbeda-beda. Pada saat registrasi status aktif akan digunakan untuk mengaktifkan *user* sehingga *user* dapat mengakses aplikasi dengan *username* dan *password* yang digunakan. Status tidak aktif digunakan untuk menonaktifkan *user* agar *user* tidak dapat mengakses aplikasi dengan *username* dan *password* yang digunakan pada saat registrasi. Status hapus digunakan menghapus data *user* pada *database*.

c. Halaman Daftar *File Enkripsi*

Halaman daftar *file Enkripsi* adalah halaman yang bisa diakses oleh *administrator* guna melihat dan menghapus daftar *file* enkripsi yang telah berhasil di *upload* oleh setiap *user* yang terdaftar. Adapun halaman daftar *file* enkripsi seperti Gambar 12.

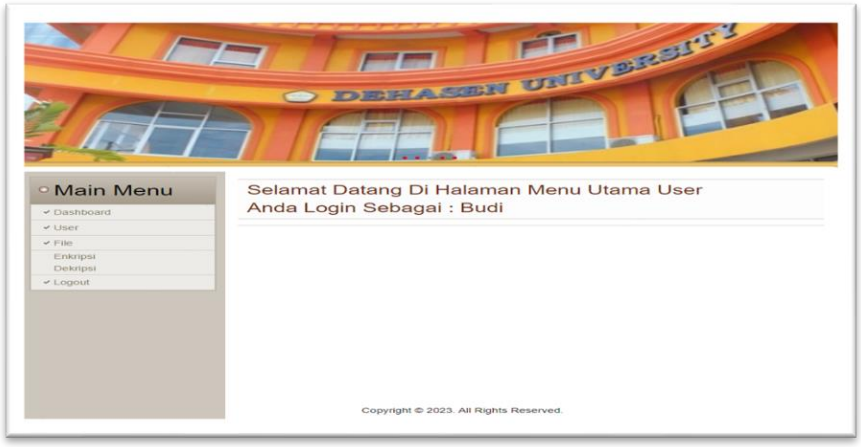
Gambar 12. Halaman Daftar *File* Enkripsi

2. Hak Akses *User*

Hak akses *user* dapat melihat biodata *user*, melakukan *upload file* yang akan di enkripsi dan tersimpan di server, dan dapat *download file-file* enkripsi untuk dilakukan dekripsi agar *file* tersebut dapat dibaca kembali seperti semula. Algoritma *Advanced Encryption Standard* (AES) berbasis web akan digunakan untuk hak akses *user* pada antarmuka aplikasi pengamanan *file*, antara lain:

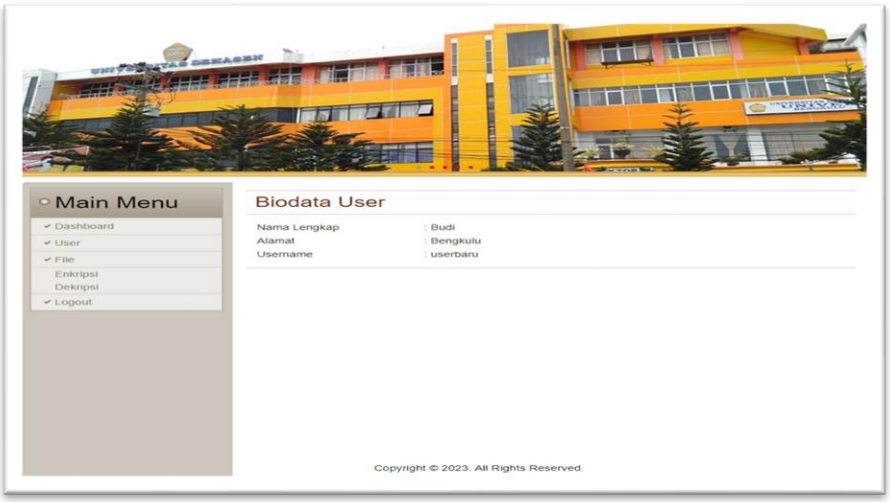
a. Halaman Menu Utama *User*

Halaman menu utama *user* merupakan halaman yang dapat diakses oleh *user* ketika berhasil melakukan *login*. Pada menu utama *user* terdapat sub menu yang dapat diakses yaitu halaman *dashboard*, *user*, *file* enkripsi, *file dekripsi* dan logout. Adapun halaman menu utama *user* seperti Gambar 13



Gambar 13. Halaman Menu Utama *User*

b. Halaman *User*
Halaman *user* merupakan halaman yang dapat diakses *user* untuk mengetahui informasi biodata *user*. Adapun halaman *user* seperti Gambar 14.



Gambar 14. Halaman *User*

c. Halaman *File* Enkripsi
Halaman *file* enkripsi merupakan halaman yang dapat diakses oleh *user* untuk *upload file* enkripsi ke dalam *server* dengan cara memilih *file* dokumen asli terlebih dahulu, memasukkan *password* untuk enkripsi *file* dokumen asli tersebut, dan memberikan keterangan dari *file* dokumen yang akan dienkripsi, setelah itu klik tombol enkripsi, maka secara otomatis aplikasi akan melakukan proses enkripsi pada *file* dokumen asli dan menyimpan *file* enkripsi ke dalam *server*. Adapun halaman *file* enkripsi seperti Gambar 15.

Gambar 15. Halaman *File* Enkripsi

Jika proses enkripsi berhasil maka aplikasi akan memberikan informasi dari hasil proses enkripsi tersebut, seperti Gambar 16.

Gambar 16. Informasi Hasil Proses Enkripsi

d. Halaman *File* Dekripsi

Halaman *file* dekripsi merupakan halaman yang dapat diakses oleh *user* untuk melihat *file-file* enkripsi yang telah tersimpan ke dalam *server*. Adapun halaman *file dekripsi* seperti Gambar 17.

Gambar 17. Halaman *File* Dekripsi

Pada Gambar 17 tersebut, terdapat aksi yang dapat dilakukan oleh *user* pada setiap *file* enkripsi yang telah di *upload* ke *server*, dimana *user* dapat *download file* enkripsi dan juga melakukan dekripsi pada *file* enkripsi tersebut. Jika ingin melakukan dekripsi pada *file* enkripsi, klik dekripsi, kemudian *user* harus memasukkan *password* yang benar, agar mendapatkan *file* dokumen yang asli. Adapun halaman dekripsi seperti Gambar 18.

Gambar 18. Halaman Dekripsi

B. PEMBAHASAN

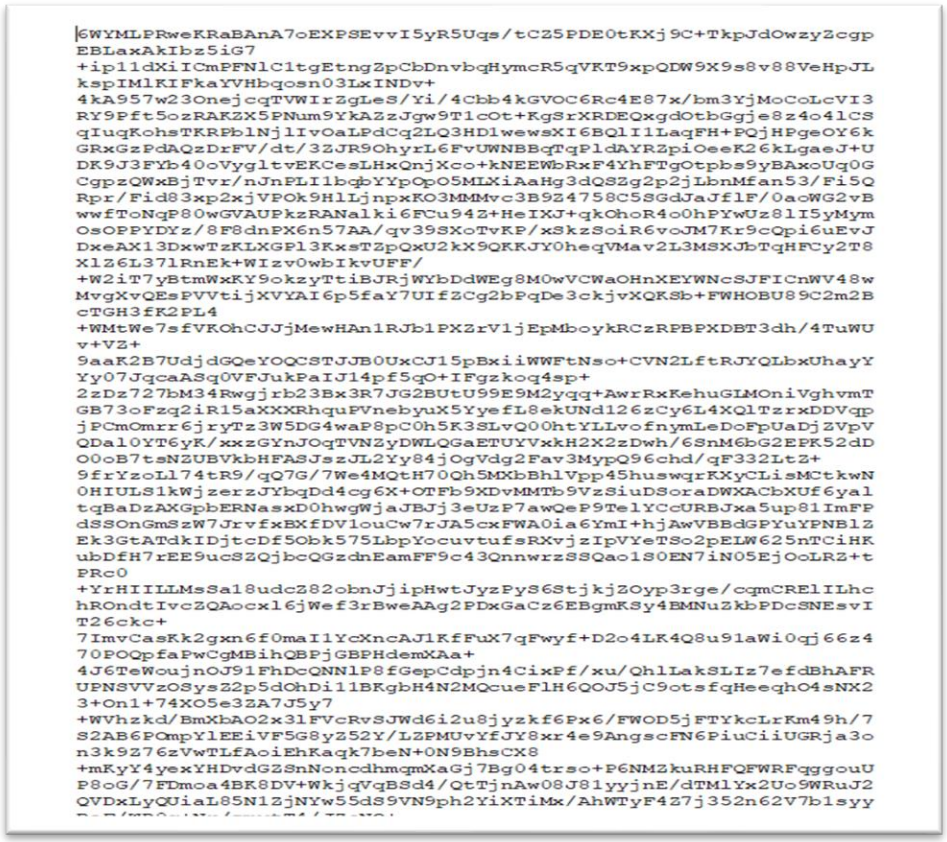
Pengujian dilakukan dengan cara menguji coba fungsionalitas dari aplikasi pengamanan *file* memakai algoritma *Advanced Encryption Standard* (*AES*) berbasis *web*. Dalam pengujian sistem ini terdapat 4 jenis pengujian yang dilakukan. Pengujian dilakukan dengan cara menguji coba fungsionalitas dari aplikasi pengamanan *file* memakai algoritma *Advanced Encryption Standard* (*AES*) berbasis *web***.**

Tabel 3. Hasil Pengujian

No	Jenis Pengujian	Kriteria	Hasil
1	Pengujian Enkripsi	Melakukan Enkripsi *File* dengan format pdf, docx, doc pada aplikasi berbasis web	Sistem telah berhasil melakukan proses enkripsi memakai Algoritma *AES* terhadap *file* dokumen asli sehingga *file* dokumen tersebut diacak dan tidak dapat dibaca
2	Pengujian Deskripsi	Melakukan deskripsi *file* pada aplikasi berbasis web	Sistem telah berhasil melakukan proses dekripsi memakai Algoritma *AES* terhadap *file* dokumen terenkripsi sehingga *file* dokumen tersebut kembali seperti semula dan dapat dibaca
3	Pengujian Keamanan *File*	Melakukan *Sniffing* menggunakan aplikasi *wireshark*	*File* yang tersimpan di dalam *server* dalam bentuk enkripsi dan aman dari serangan *sniffing*
4	Pengujian waktu yang dibutuhkan dalam proses enkripsi	Waktu proses enkripsi	Waktu yang dibutuhkan dalam proses enkripsi tergantung berdasarkan ukuran *file* enkripsi, makin besar ukuran *file* enkripsi, maka akan makin lama proses enkripsi yang terjadi. Pada penujian yang dilakukan besar ukuran *file* enkripsi 30976 *bytes* dengan waktu diperlukan selama 0.00114 detik.

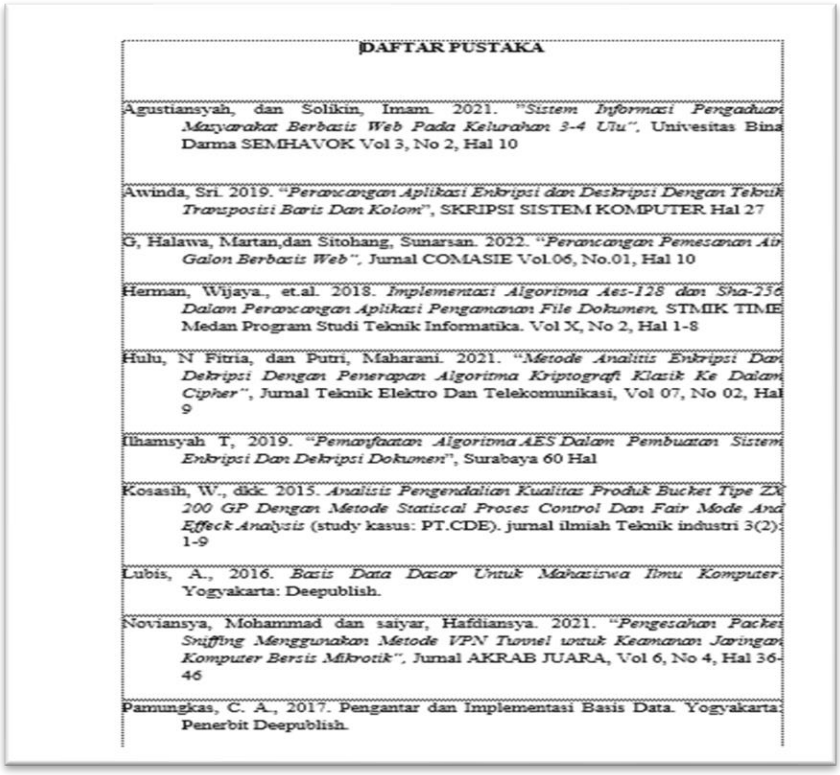
Berdasarkan 4 jenis pengujian sistem yang sudah dilakukan tersebut di atas sehingga dapat disimpulkan bahwa fungsional dari aplikasi pengamanan *file* memakai algoritma *Advanced Encryption*

Standard (AES) berbasis web telah berjalan dengan baik dan aplikasi dapat mengamankan *file* dokumen asli melalui Algoritma *Advanced Encryption Standard* (AES).



6WYMLPRweKRaBAnA7oEXPSEvvI5yR5Uqs/tCZ5PDE0tKXj9C+TkpJdOwzyZcgp
EBLaxAkIbz5iG7
+ip11dXiICmPFNlC1tgEtngZpCbDnvbqHymcR5qVKT9xpQDW9X9s8v88VeHpJL
kspIMlKIFkaYVHbqosn03LxINDv+
4kA957w23OnejcqTVWIrZgLeS/Yi/4Cbb4kGVOC6Rc4E87x/bm3YjMoCoLcVI3
RY9Pft5ozRAKZX5PNum9YkAZzJgw9T1cOt+KgSrXRDEQxgdOtbGgje8z4o41CS
qIuqKohsTKRPblNj1IvOaLPdCq2LQ3HD1wewsXI6BQlI1LaqFH+PQjHPgeOY6k
GRxGzPdAQzDrFV/dt/3ZJR9OhyrL6FvUWNBBqTqPldAYRZpiOeeK26kLgaeJ+U
DK9J3FYb40oVyg1tvEKCesLHxQnjXco+kNEEWbRxF4YhFTgOtpbs9yBAxoUq0G
CgpzQWxBjTvr/nJnPLI1bqbYYpOpO5MLXiAaHg3dQSZg2p2jLbnMfan53/Fi5Q
Rpr/Fid83xp2xjVPOk9HlLjnpxKO3MMMvc3B9Z4758C5SGdJaJflF/0aoWG2vB
wwfToNqP80wGVAUPkzRANalki6FCu94Z+HeIXJ+qkOhoR4o0hPYwUz8lI5yMym
OsOPPYDYz/8F8dnPX6n57AA/qv39SXoTvKP/x8kzSoiR6voJM7Kr9cQpi6uEvJ
DxeAX13DxwTzKLXGPl3KxsTZpQxU2kX9QKKJY0heqVMav2L3MSXJbTqHFCy2T8
Xlz6L37lRnEk+WIzv0wbIkvUFF/
+W2iT7yBtmWxKY9okzyTtiBJRjWYbDdWEg8M0wVCWaOHnXEYWNcSJFICnWV48w
MvgXvQEsPVVtijXVYAI6p5faY7UIfZCg2bPqDe3ckjvXQKSb+FWHOBU89C2m2B
cTGH3fK2PL4
+WMtWe7sfVKOhCJJjMewHAn1RJb1PXZrV1jEpMboykRCzRPBPXDBT3dh/4TuWU
v+VZ+
9aaK2B7UdjdGQeYOQCSTJJB0UxCJ15pBxiiWWFtNso+CVN2LftRJYQLbxUhayY
Yy07JqcaASq0VFJukPaIJ14pf5qO+IFgzkoq4sp+
2zDz727bM34Rwgjrb23Bx3R7JG2BUtU99E9M2yqq+AwrRxKehuGLMOniVghvmT
GB73oFzq2iR15aXXXRhquPVnebyuX5YyefL8ekUNd126zCy6L4XQlTzrxDDVqp
jPCmOmrr6jryTz3W5DG4waP8pC0h5K3SLvQ00htYLLvofnymLeDoFpUaDjZVpV
QDal0YT6yK/xxzGYnJOqTVNZyDWLQGaETUYVxkH2X2zDwh/6SnM6bG2EPK52dD
O0oB7tsNZUBVkbHFASJszJL2Yy84jOgVdg2Fav3MypQ96chd/qF332LtZ+
9frYzoLl74tR9/qQ7G/7We4MQtH70Qh5MXbBhlVpp45huswqrKXyCLisMCtkwN
0HIULS1kWjzerzJYbqDd4cg6X+OTFb9XDvMMTb9VzSiuDSoraDWXACbXUf6yal
tqBaDzAXGpbERNasxD0hwgWjaJBJj3eUzP7awQeP9TelYCcURBJxa5up81ImFP
dSSOnGmSzW7JrvfxBXfDV1ouCw7rJA5cxFWA0ia6YmI+hjAwVBBdGPYuYPNBlZ
Ek3GtATdkIDjtcDf5Obk575LbpYocuvtufsRXvjzIpVYeTSo2pELW625nTCiHK
ubDfH7rEE9ucSZQjbcQGzdnEamFF9c43QnnwrzSSQao1S0EN7iN05EjOoLRZ+t
PRc0
+YrHIILLMsSa18udcZ82obnJjipHwtJyzPyS6StjkjZOyp3rge/cqmCRElILhc
hROndtIvcZQAocx16jWef3rBweAAg2PDxGaCz6EBgmKSy4BMNu2kbPDcSNEsvI
T26ckc+
7ImvCasKk2gxn6f0maI1YcXncAJ1KfFuX7qFwyf+D2o4LK4Q8u91aWi0qj66z4
70POQpfaPwCgMBihQBPjGBPHdemXAa+
4J6TeWoujnOJ91FhDcQNNlP8fGepCdpjn4CixPf/xu/QhlLakSLIz7efdBhAFR
UPNSVVzOSysZ2p5dOhDi11BKgbH4N2MQcueFlH6QOJ5jC9otsfqHeeqhO4sNX2
3+On1+74XO5e3ZA7J5y7
+WVhzkd/BmXbAO2x3lFVcRvSJWd6i2u8jyzkf6Px6/FWOD5jFTYkcLrKm49h/7
S2AB6POmpYlEEiVF5G8yZ52Y/LZPMUvYfJY8xr4e9AngscFN6PiuCiiUGRja3o
n3k9276zVwTLfAoiEhKaqk7beN+0N9BhsCX8
+mKyY4yexYHDvdGZSnNoncdhmqmXaGj7Bg04trso+P6NMZkuRHFQFWRFqggouU
P8oG/7FDmoa4BK8DV+WkjqVqBSd4/QtTjnAw08J81yyjnE/dTMlYx2Uo9WRuJ2
QVDxLyQUiaL85N1ZjNYw55dS9VN9ph2YiXTiMx/AhWTyF4Z7j352n62V7b1syy

Gambar 19. Isi *File* Dokumen Setelah Di Enkripsi



DAFTAR PUSTAKA

Agustiansyah, dan Solikin, Imam. 2021. *"Sistem Informasi Pengaduan Masyarakat Berbasis Web Pada Kelurahan 3-4 Ulu"*. Univesitas Bina Darma SEMHAVOK Vol 3, No 2, Hal 10

Awinda, Sri. 2019. *"Perancangan Aplikasi Enkripsi dan Deskripsi Dengan Teknik Transposisi Baris Dan Kolom"*, SKRIPSI SISTEM KOMPUTER Hal 27

G, Halawa, Martan,dan Sitohang, Sunarsan. 2022. *"Perancangan Pemesanan Air Galon Berbasis Web"*, Jurnal COMASIE Vol.06, No.01, Hal 10

Herman, Wijaya., et.al. 2018. *Implementasi Algoritma Aes-128 dan Sha-256 Dalam Perancangan Aplikasi Pengamanan File Dokumen*, STMIK TIME Medan Program Studi Teknik Informatika. Vol X, No 2, Hal 1-8

Hulu, N Fitria, dan Putri, Maharani. 2021. *"Metode Analitis Enkripsi Dan Dekripsi Dengan Penerapan Algoritma Kriptografi Klasik Ke Dalam Cipher"*, Jurnal Teknik Elektro Dan Telekomunikasi, Vol 07, No 02, Hal 9

Ilhamsyah T, 2019. *"Pemanfaatan Algoritma AES Dalam Pembuatan Sistem Enkripsi Dan Dekripsi Dokumen"*, Surabaya 60 Hal

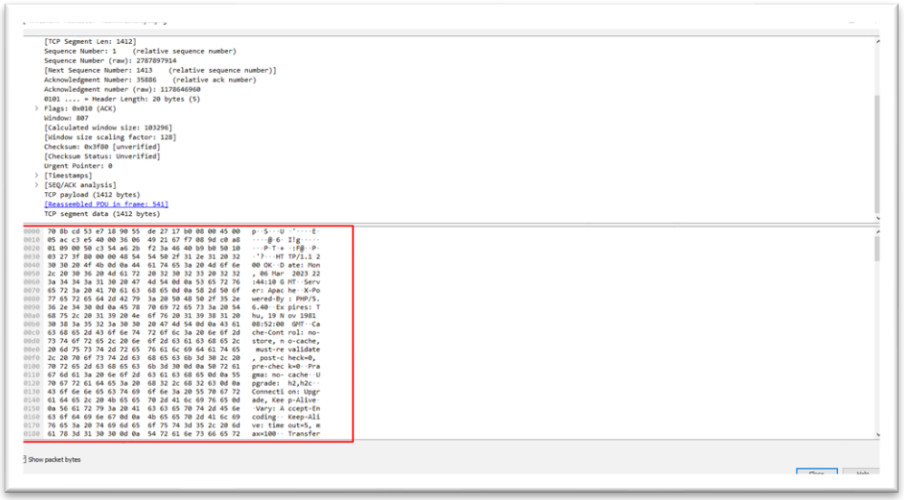
Kosasih, W., dkk. 2015. *Analisis Pengendalian Kualitas Produk Bucket Tipe ZX 200 GP Dengan Metode Statiscal Proses Control Dan Fair Mode And Effeck Analysis* (study kasus: PT.CDE). jurnal ilmiah Teknik industri 3(2): 1-9

Lubis, A., 2016. *Basis Data Dasar Untuk Mahasiswa Ilmu Komputer*. Yogyakarta: Deepublish.

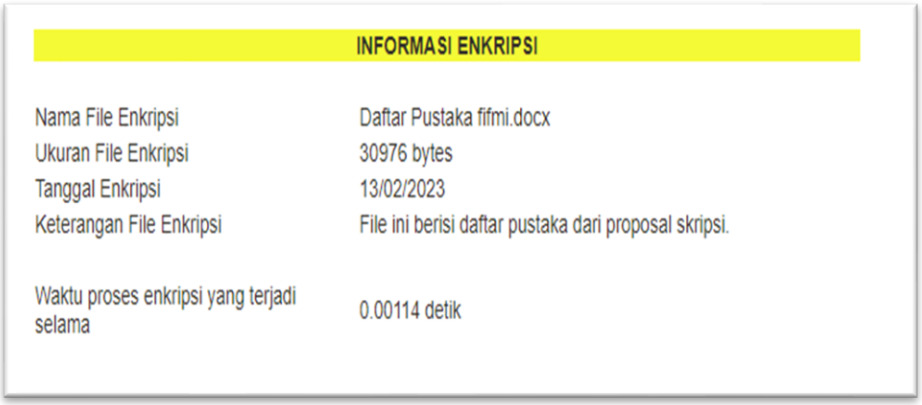
Noviansya, Mohammad dan saiyar, Hafdiansya. 2021. *"Pengesahan Packet Sniffing Menggunakan Metode VPN Tunnel untuk Keamanan Jaringan Komputer Bersis Mikrotik"*, Jurnal AKRAB JUARA, Vol 6, No 4, Hal 36-46

Pamungkas, C. A., 2017. Pengantar dan Implementasi Basis Data. Yogyakarta: Penerbit Deepublish.

Gambar 20. Isi *File* Dokumen Setelah Di Dekripsi



Gambar 21. Hasil *Capture Wireshark* (1)



Gambar 22. Pengujian Waktu Proses Enkripsi

3. KESIMPULAN DAN SARAN

A. KESIMPULAN

Setelah dilakukan pengujian dan analisa dari pembahasan yang ada, maka dapat ditarik beberapa kesimpulan diantaranya adalah sebagai berikut:

1. Bahasa Pemrograman PHP dan *database MySQL* dapat digunakan pada penerapan Algoritma *Advanced Encryption Standard* (*AES*) Untuk Pengamanan *File* pada aplikasi berbasis *web*. Aplikasi pengamanan *file* ini dapat diakses secara *online* melalui *link http://fifmiantiaes.online/* melalui internet, sehingga dapat mempermudah *user* dalam mengakses aplikasi dimana pun dan kapan pun.
2. Dengan adanya Aplikasi pengamanan *file* memakai algoritma *Advanced Encryption Standard* (*AES*) berbasis *web* dapat meningkatkan keamanan *file* dari pihak yang tidak berwewenang.
3. Aplikasi pengamanan *file* memakai algoritma *Advanced Encryption Standard* (*AES*) ini, terdapat 2 hak akses yaitu *Administrator* dan *User* yang memiliki fungsi berbeda-beda.
4. Hak akses administrator dapat memanajemen *user* yang telah melakukan registrasi baik untuk aktivasi *user* atau menghapus *user* tersebut, selain itu administrator dapat melihat berkas *file-file* enkripsi yang telah di *upload* oleh semua *user*.
5. Hak akses *user* dapat melihat biodata *user*, melakukan *upload file* yang akan di enkripsi dan tersimpan di *server*, dan dapat *download file-file* enkripsi untuk dilakukan dekripsi agar *file* tersebut dapat dibaca kembali seperti semula.
6. Pada pengujian sistem yang sudah dilakukan, dapat dinyatakan bahwa fungsional dari aplikasi pengamanan *file* memakai algoritma *Advanced Encryption Standard* (*AES*) berbasis *web* telah berjalan dengan baik dan aplikasi dapat mengamankan *file* dokumen asli melalui Algoritma *Advanced Encryption Standard* (*AES*).

B. SARAN

Ada beberapa saran yang dapat diusulkan untuk penelitian selanjutnya agar diperoleh hasil yang lebih maksimal diantaranya adalah sebagai berikut:

1. Untuk kemudian hari diharapkan dapat diterapkan dan dilakukan pengembangan aplikasi yang dapat diakses melalui *website* sebagai aplikasi keamanan *file* dengan Algoritma *Advanced Encryption Standard* (AES) ataupun aplikasi lainnya.
2. Aplikasi ini dikembangkan dengan memberikan batasan ukuran *file*-nya. Maka disaran kan jika ukuran *file*-nya terlalu besar saat aplikasi ini di jalankan, maka akan muncul pemberitahuan apakah masih mau melanjutkan untuk menyelesaikan prosesnya atau di batalkan.

DAFTAR PUSTAKA

Azanuddin, A., Yakub, S., & Prayudha, J. (2022). Implementasi Keamanan Citra Menggunakan Algoritma AES-128 dengan Aplikasi Client-Server. *Jurasik (Jurnal Riset Sistem Informasi dan Teknik Informatika* , 51-61 (diakses pada 01 Juli 2023).

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*, 163-171 (diakses pada 01 Juli 2023).

Darwis, D., & Kisworo, K. (2017). Teknik Steganografi untuk Penyembunyian Pesan Teks Menggunakan Algoritma End of Life . *Jurnal Sistem Informasi dan Telematika* (diakses pada 01 Juli 2023).

Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2016). Implementasi Kriptografi Pengamanan Data pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer*, 20-31 (diakses pada 01 Juli 2023).

Putra, D. I., & Ginting, G. (2017). Perancangan Aplikasi Penyandian Data Text Menggunakan Metode Symmetric Stream Cipher. *Pelita Informatika: Informasi dan Informatika*, 84-87 (diakses pada 01 Juli 2023).