KRESNA: Jurnal Riset dan Pengabdian Masyarakat
Volume 4, Nomor 1, Mei, 2024, Hal: 12-22 E-ISSN: 2809-6509

Implementasi Algoritme AES-256 dan AES-GCM untuk Mengamankan Dokumen Pada Sistem Data Rekam Medis Klinik Mulya

Implementation of Aes-256 dnd AES-GCM Algorithms to Secure Documents in The Medical Record Data System at Mulya Clinic

R.M. Hilmy Hernandi[1], Joko Christian Chandra[2]

[1,2]Fakultas Teknologi Informasi
Universitas Budi Luhur
Email: [1*]r.muh.hilmy.h@gmail.com, [2]joko.christian@budiluhur.ac.id
(* corresponding author)

Abstrak

Dalam era digitalisasi pada saat ini banyak sekali aspek – aspek yang sedang dikembangkan mau di sektor yang dinaungi oleh pemerintahan atau pun oleh pihak swasta yang bertujuan untuk membangun sistem yang lebih modern. Selain berkembang di sektor ekonomi, keamanan, teknologi, pendidikan dan transportasi ada satu sektor yang sedang dikembangkan yang awalnya masih menggunakan metode manual sekarang sedang dikembang ke arah digitalisasi, yaitu di sektor kesehatan seperti dalam hal Sistem Informasi Manajemen Rumah Sakit. Klinik mulya ini didirikan oleh ibu Gita Gardenia S.E pada tahun 1991. Di klinik mulya, saat ini masih menggunakan metode manual dalam penyimpanan dan pengelolahan data rekam medis pasien. Oleh sebab itu peneliti melakukan penelitian dengan menerapkan algoritme AES-256 dan AES-GCM untuk mengamankan file atau dokumen data rekam medis pasien dalam sistem berupa sebuah website. Dalam penelitian ini, peneliti melakukan penerapan sebuah metode kualitatif yang berisikan proses pengumpulan data, analisis kebutuhan dan penerapan algoritme AES. Setelah sistem berhasil dibuat, maka hasil pengujian dengan menggunakan metode *blackbox testing*, peneliti mendapatkan hasil bahwa semua fitur dari proses pengujian berjalan sesuai dengan fungsional. Pada proses pengujian enkripsi file rekam medis telah terjadinya perubahan pada file asli nya yang ukuran sizenya menjadi lebih besar dan pada proses pengujian deskripsi mendapatkan hasil bahwa ukuran file kembali menjadi ukuran aslinya. . Selain terjadi perubahan terhadap data tipe file tersebut perubahan juga terjadi pada panjang data file asli yang berubah menjadi sangat panjang sehingga file tersebut menjadi tidak normal sehingga keamanan isi dari file tersebut menjadi lebih aman dari kondisi file normalnya. Panjang data file bisa menjadi normal ketika terjadi proses deskripsi sehingga isi file bisa di baca kembali.

Kata Kunci: kriptografi, AES, rekam medis.

Abstract

In the current era of digitalization, there are numerous aspects being developed in sectors overseen by both the government and private entities, aiming to build more modern systems. Apart from advancements in economic, security, technology, education, and transportation sectors, there is one sector currently undergoing development that initially relied on manual methods but is now transitioning towards digitalization, particularly in the healthcare sector such as Hospital Management Information Systems. Klinik Mulya was founded by Mrs. Gita Gardenia S.E in 1991. Currently, Klinik Mulya still employs manual methods in storing and managing patient medical records. Therefore, researchers conducted a study by implementing AES-256 and AES-GCM algorithms to secure files or documents of patient medical records in a website-based system. In this study, researchers applied a qualitative method consisting of data collection processes, needs analysis, and implementation of AES algorithms. After successfully creating the system, testing was conducted using blackbox testing method, and researchers found that all features of the testing process functioned as intended. In the encryption testing process, changes occurred in the original

file, increasing its size, while in the decryption testing process, the file size reverted to its original size. Besides changes in the file type data, changes also occurred in the length of the original file data, becoming significantly longer, making the file abnormal, hence enhancing the security of its content compared to its normal state. The file's length can return to normal during the decryption process, allowing the file's content to be read again.

Keywords: *Cryptographic,* AES, medical record.

1. PENDAHULUAN

Dalam era digitalisasi, banyak sektor seperti ekonomi, keamanan, teknologi, pendidikan, dan transportasi tengah dikembangkan menuju sistem yang lebih modern. Di antara sektor tersebut, sektor kesehatan, khususnya dalam Sistem Informasi Manajemen Rumah Sakit, mengalami perubahan dari metode manual ke arah digitalisasi. Meski pemerintah mendorong digitalisasi, banyak rumah sakit atau klinik, termasuk Klinik Mulya, masih menggunakan metode manual dalam penyimpanan dan pengelolaan data rekam medis, mengakibatkan waktu pencarian yang lama dan minimnya keamanan data. Permintaan eksternal terhadap data rekam medis, seperti untuk keperluan pekerjaan dan pendataan kesehatan juga meningkat.

Berdasarkan permasalahan tersebut penelitian ini berfokus pada penerapan kriptografi dengan algoritme AES 256 dan AES GCM untuk meningkatkan keamanan dan privasi yang terotentikasi, menghilangkan kekhawatiran atas keamanan dan privasi data rekam medis di databases pada website sesuai dengan standar yang ditetapkan pemerintah yang di cantumkan pada peraturan menteri kesehatan republik indonesia nomor 46 tahun 2022 tentang rekam medis.

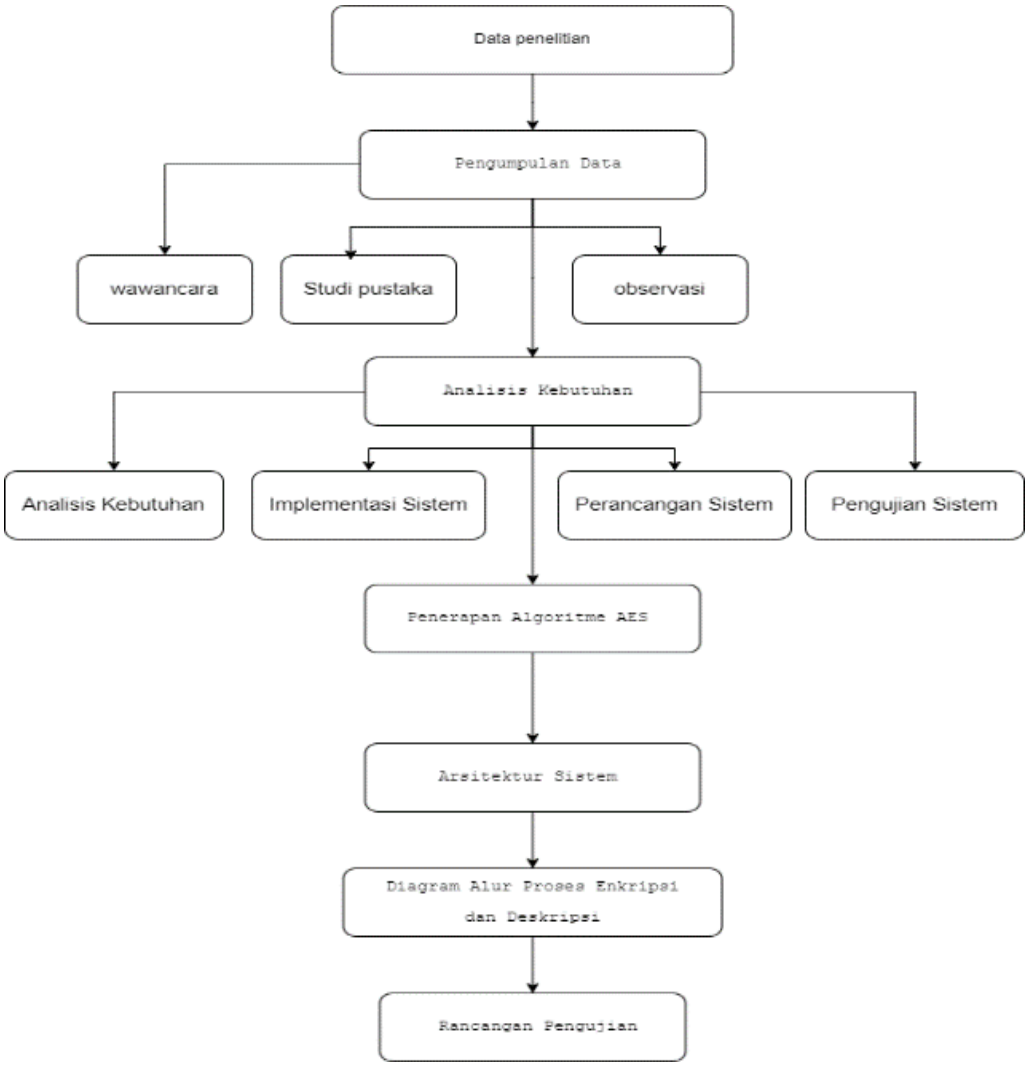
Dengan terdapatnya permasalahan tersebut penelitian ini memiliki tujuan untuk mengembangkan sistem dengan pendekatan *waterfall* dan menerapkan algoritme kriptografi berbasis website dengan menggunakan algoritme AES 256 dan AES GCM sebagai alat keamanan dan privasi pada dokumen atau file.

Data rekam medis adalah dokumen yang berisikan data identitas pasien, pemeriksaan, pengobatan, tindakan dan pelayanan lain yang telah diberikan kepada pasien [1].

Kriptografi (*Cryptography*) berasal dari bahasa Yunani yaitu dari kata *kryptos* yang artinya tersembunyi. Kriptografi dapat diartikan sebagai tulisan yang dirahasiakan atau dapat diartikan juga sebagai suatu ilmu ataupun seni yang mempelajari bagaimana sebuah data, informasi dan dokumen dikonversi kebentuk tertentu yang sulit untuk dimengerti [2]. Menurut [3], umumnya, kriptografi dapat diartikan sebagai bidang ilmu tentang penyandian untuk keamanan dan kerahasiaan suatu data atau dokumen. Namun, perlu diingat bahwa kriptografi bukan berarti hanya memberikan keamanan informasi, tapi lebih ke arah teknik - tekniknya Pada kriptografi memiliki beberapa bagian – bagian penting dalam proses seperti plaintext, ciphertext, enskripsi, deskripsi, kunci publik dan kunci privat. Enkripsi merupakan proses dimana informasi atau data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu [4]. Deskripsi Proses untuk mengembalikan bentuk semula dari sebuah objek atau isi objek dari hasil enskripsi. Kunci rahasia yang sama digunakan oleh pengirim dan penerima dalam melakukan enkripsi dan deskripsi pesan [5]. Kunci publik merupakan sebuah kunci yang bersifat terbuka atau sebuah kunci yang hanya di berikan oleh pemilik objek yang bersifat rahasia tersebut.

2. METODE PENELITIAN

Pada tahapan metode penelitian ini, proses tersebut dapat dilihat pada gambar 1 berikut:



Gambar 1: Metode Penelitian

2.1 Data Penelitian

Dalam penelitian ini data yang digunakan atau didapatkan berasal dari klinik mulya berupa sebuah file hasil pemindaian dari data rekam medis pasien yang terbaru. Klinik mulya beralamat Kompleks, depan Baso Titoti, Jl. KH Hasyim Ashari Jl. Ciledug Indah 2 Noft.10, RT.001/RW.005, Sudimara Pinang, Kec. Pinang, Kota Tangerang, Banten.

2.2 Pengumpulan Data

Dalam proses pengumpulan data ini, peneliti menggunakan sebuah metode kualitatif yang dimana proses pengumpulan data tersebut akan dilakukan dengan beberapa cara yang dimana bisa dilihat dibawah ini.

a. Wawancara
   Merupakan sebuah metode yang melakukan pengajuan sebuah pertanyaan kepada narasumber yang mengetahui sumber data yang di perlukan dalam penelitian.
b. Observasi
   Merupakan sebuah metode dalam pengumpulan data yang bertujuan untuk pengamatan sebuah objek yang sedang di teliti. Objek yang diteliti dalam penelitian ini berupa sebuah objek berupa dokumen yang berisikan data rekam medik dari pasien klinik mulya. Proses observasi dalam penelitian ini akan melingkupi cara penyimpinan, keamanan dan hak akses terhadap dokumen yang berisikan data rekam medis dengan cara menggunaan algoritma AES-256 dan AES-GCM.

c. Studi pustaka.
Pada proses ini dilakukan dengan cara mencari informasi atau referensi dari jurnal online, kumpulan skirpsi di perpustakaan Universitas Budi Luhur dan buku atau e-book. Referensi yang digunakan dalam penelitian ini adalah sebuah referensi yang memuat tentang kriptografi, algoritma AES dan rekam medis supaya berkaitan dengan penelitian ini.

2.3 Analisis Kebutuhan

Dalam proses analisis kebutuhan ini, peneliti menggunakan sebuah cara untuk melakukan analisis kebutuhan, cara tersebut dapat dilihat dibawah ini.

a. Analisis kebutuhan
Pada analisis kebutuhan di Klinik Mulya ini membutuhkan sebuah sistem yang dimana data rekam medis ini dapat di simpan dan diakses dengan mudah tetapi memiliki sistem keamanan yang dapat melindungi data tersebut sehingga pemilik data tersebut tidak merasa khawatir data yang dimilikinya tercuri oleh pihak luar.
b. Perancangan sistem
Dalam proses perancangan sistem ini berfungsi untuk memberikan informasi secara jelas apa saja yang bisa dilakukan oleh pihak yang diijinkan untuk mengakses sistem yang berupa sebuah website ini dengan memberikan informasi yang berupa sebuah gambar.
c. Implementasi sistem
Dalam proses implentasi ini akan dilaksanakan ketikan perancangan sistem yang dibuat oleh peneliti sudah dianggap sesuai dengan hasil dari analisis kebutuhan sesuai dengan kebutuhan atau permasalahan yang dialami oleh Klinik Mulya.
d. Pengujian sistem
Dalam proses pengujian ini akan dilaksanakan ketika tahap implementasi sudah selesai dengan cara melihat dua tahapan sebelumnya dan apakah hasilnya sesuai atau tidak. Dalam proses ini akan menggunakan metode blackbox testing dengan cara melihat hasil dari outputnya.

2.4 Penerapan Algoritme AES

Pada proses penerapan algoritme AES ini, peneliti akan menggunkan dua jenis algoritme yang berbeda yang dimana akan menerapakan sebuah algoritme tanpa mode dan algoritme dengan mode.

a. Algoritme AES 256

Pada algoritma AES tanpa mode ini akan melakukan beberapa tahapan dalam proses enkripsi dan deskripsinya. Tahapan – tahapan yang akan dilakukan seperti menggunakan panjang kunci 256 bit, perubahan objek asli menjadi objek yang terenkripsi dan perubahan objek terenkripsi menjadi sebuah objek asli dengan cara proses deskripsi.

Pada proses enkripsi algoritma AES tanpa mode bisa dilihat dibawah ini.

1) *SubBytes*
Menurut [7], SubBytes merupakan transformasi byte yang dilakukan dengan cara mensubstitusikan atau mengganti setiap byte dari state dengan byte yang berada pada tabel s-box AES.
2) *Shiftrows*
Menurut [7], *Shiftrows* adalah transformasi yang melakukan pergeseran nilai byte pada tiga baris terakhir dari array state.
3) *MixColumns*
MixColumns mengoperasikan setiap elemen yang berada dalam satu kolom pada state [8].
4) *Addroundkey*
Addroundkey akan melakukan xor antara state sekarang dengan round key [8].

Pada proses deskripsi algoritma AES tanpa mode bisa dilihat dibawah ini.

1) *Invshiftrows*
Invshiftrows dimana terjadi pergeseran ke sebalah kanan pada baris 2, 3, dan 4. Pergeseran tersebut merupakan kebalikan dari transformasi *shiftrows* [9].
2) *Invsubbytes*

Invsubbytes juga merupakan transformasi bytes yang berkebalikan dengan transformasi *subbytes* [8]. Pada Invsubbytes, tiap elemen pada state dipetakan dengan menggunakan tabel inverse s-box [8].

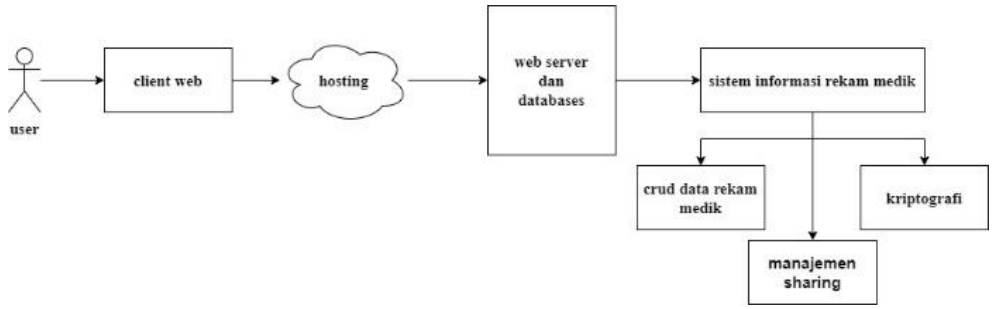
3) *Invmixcolumns*
Invmixcolumns setiap kolom dalam state dikalikan dengan matrik perkalian dalam AES [8].
4) *Addroundkey*
Addroundkey merupakan transformasi inverse addroundkey tidak berbeda dengan transformasi *addroundkey* karna dalam transformasi ini hanya dilakukan operasi penambahan sederhana dengan operasi bitwise XOR [8].

b. Algoritme AES GCM

Pada algoritme AES dengan mode GCM ini akan melakukan beberapa tahapan dalam proses enkripsi dan deskripsinya. Tahapan – tahapan yang akan dilakukan pada penelitian ini menggunakan panjang kunci 256 bit, proses *inisialisasi vektor, autentikasi tag,* perubahan objek asli menjadi objek yang terenkripsi dan perubahan objek terenkripsi menjadi sebuah objek asli dengan cara proses deskripsi. Pada algoritme AES dengan mode GCM Merupakan sebuah jenis mode AES yang sama seperti AES tanpa mode yang memiliki 3 jenis panjang kunci dari 128, 169 dan 256. AES GCM adalah model enkripsi blok yang memberikan kecepatan tinggi pada proses enkripsi terautentikasi dan integrasi data. AES-GCM memiliki dua fungsi utama yakni enkripsi blok cipher dengan menggunakan metode AES CTR dan autentikasi AES-GCM pada penyandiannya [10].

2.5 Arsitektur Sistem

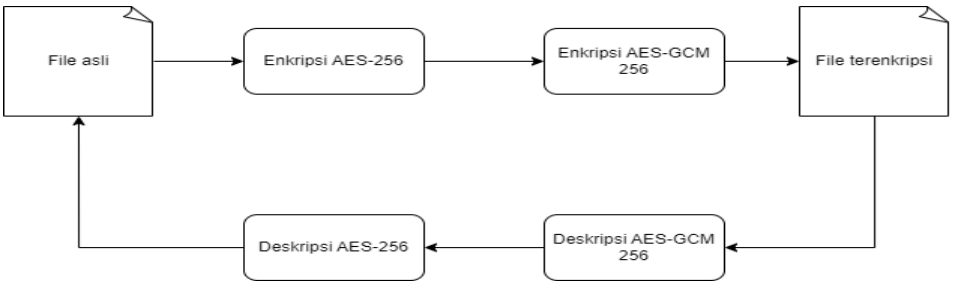
Arsitektur sistem merupakan sebuah skema atau gambaran proses kerja sebuah sistem. Arsitektur sistem dalam penelitian ini bisa dilihat di Gambar 2 berikut:



Gambar 2: Arsitektur System

2.6 Diagram Alur Proses Enkripsi Dan Deskripsi

Pada diagram arsitektur proses enkripsi dan deskripsi ini akan menjelaskan tentang proses enkripsi dan deskripsi. Untuk proses enkripsi akan di lakukan pertama kali dengan AES 256 tanpa mode lalu melakukan enkripsi dengan AES GCM dan untuk proses deskripsi nya akan dilakukan secara terbalik yang dimana proses pertama akan di lakukan dengan AES GCM lalu deskripsi akhirnya dengan AES 256. Pada proses tersebut bisa dilihat melalui gambar 3 berikut:



Gambar 3: Diagram Arsitektur Proses Enkripsi dan Deskripsi

2.7 Rancangan pengujian

Pada proses rancangan pengujian ini, peneliti menerapkan metode *blackbox testing* dalam proses pengujian yang dimana akan menghasilkan sebuah hasil pengujian dalam fungsional pada sistem berbasis website ini.

3. HASIL DAN PEMBAHASAN

3.1 Implementasi metode

Pada proses ini peneliti akan menerapkan algoritme AES 256 tanpa metode dan AES dengan mode GCM yang dimana proses tersebut akan melakukan enkripsi dan deskripsi sebuah file berupa gambar atau pdf. Pada penerapan metode ini peneliti akan menggunakan sebuah library yang bernama crypto yang open source. Pada penerapan metode ini bisa dilihat melalui algoritme dan flowchart proses enkripsi, deskripsi, gambar proses upload rekam medis dan gambar proses unduh file rekam medis pasien.

3.2 Algoritme AES 256 Dan AES GCM

Pada algoritme ini, peneliti akan menampilkan algoritme dan *flowchart* dari AES 256 tanpa mode dan AES dengan mode gcm dalam proses enkripsi dan deskripsi.

a. Algoritme dan *Flowchart* Enkripsi AES 256 Dan AES GCM

Pada tahapan enkripsi pada algoritme AES 256 dan AES GCM ini peneliti akan menampilkan algoritme pada tabel 1 dan tabel 2 serta *flowchart* pada Gambar 4 dan 5 dari proses enkripsi berikut ini.

1) Algoritme enkripsi AES 256

Pada bagian algoritme enkripsi AES 256 ini akan diproses pertama kali dalam proses enkripsi pada penelitian ini, peneliti akan menampilkan proses dari enkripsi tersebut dan bisa dilihat di Tabel ini.

Tabel 1. Algoritme eEnkripsi AES 256

1. Start
2. file
3. Inisialisai algoritma dan key
4. Create keyBuffer
5. Create cipher
6. Enkripsi data
7. Return enkripsi data
8. End

2) Algoritme Enkripsi AES GCM

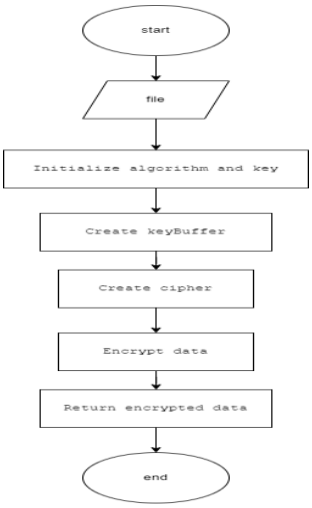
Pada tahapan ini, akan terjadi ketika proses enkripsi pada algoritme AES tanpa mode berhasil dijalankan dengan benar. Pada proses ini bisa dilihat dibagian Tabel 2 ini.

Tabel 2. Algoritme AES GCM

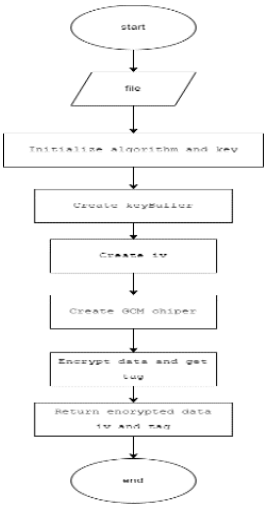
1. Start
2. File
3. Inisialisai algoritma dan key
4. Create keyBuffer
5. Create iv
6. Create gcm chiper
7. Enkripsi data dan get tag
8. Return enkripsi data, iv dan tag
9. End

3) *Flowchart* Enkripsi AES 256 Dan AES GCM

Pada *flowchart* AES 256 dan AES dengan mode GCM akan di tampilkan pada tabel 4 dan tabel 5. Untuk gambar enkripsi *flowchart* AES 256 bisa dilihat pada gambar dan *flowchart* enkripsi AES dengan mode GCM bisa lihat dilihat pada gambar 4 dan gambar 5 ini:



Gambar 4: Algoritme Enkripsi AES 256



Gambar 5: Algoritme Enkripsi AES GCM

b. Algortime Dan *Flowchart* Deskripsi AES GCM Dan AES 256

Pada tahapan deskripsi pada *algoritme* dan *flowchart* AES GCM dan AES 256 ini peneliti akan menampilkan *algoritme* dan *flowchart* dari proses deskripsi ini dan bisa dilihat pada Tabel 3 dan Tabel 4 serta Gambar 6 dan Gambar 7 berikut:

1) Algoritme deskripsi AES GCM

Pada bagian algoritme deskripsi AES GCM ini akan menjalakan proses pertama deskripsi dikarenakan algoritme ini melakukan proses enkripsi setelah AES tanpa mode berhasil melakukan proses enkripsi tersebut. Pada proses dekripsi pada AES GCM bisa dilihat pada Tabel 3 ini.

Tabel 3. Algoritme Deskripsi AES GCM

1. Start 2. File 3. Inisialisasi algoritma, key, iv dan tag 4. Create keyBuffer 5. Create gcm decipher 6. Set authentication tag 7. Deskripsi data 8. Return deskripsi data 9. end

2) Algoritme deskripsi AES 256

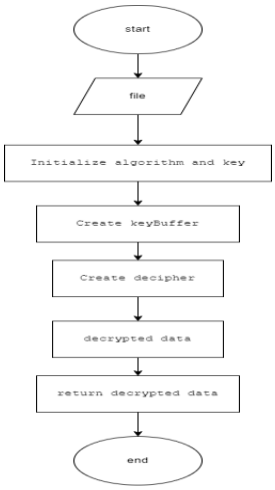
Pada bagian algoritme deskripsi AES 256 ini akan menjalakan proses deskripsi setelah proses deskripsi AES GCM berhasil dijalankan. Pada proses dekripsi pada AES 256 bisa dilihat pada Tabel 4 ini.

Tabel 4. Algoritme Deskripsi AES 256

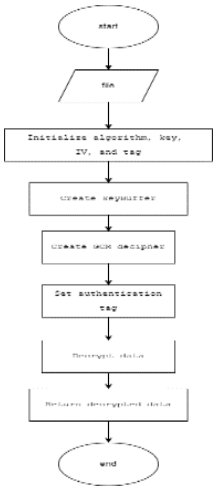
1. Start 2. File 3. Inisialisasi algoritma dan key 4. Create keyBuffer 5. Create decipher 6. Deskripsi data 7. Return deskripsi data 8. End

3) *Flowchart* deskripsi AES GCM dan deskripsi AES 256

Pada *flowchart* AES GCM dan AES 256 akan di tampilkan Gambar 6 dan Gambar 7 ini. Untuk gambar *flowchart* dedskripsi AES 256 bisa dilihat pada gambar dan untuk gambar flowchart deskripsi AES dengan mode GCM bisa lihat dilihat pada Gambar 6 dan Gambar 7 ini:



Gambar 6: Algoritme Deskripsi AES 256



Gambar 7: Algoritme Deskripsi AES GCM

3.3 Pengujian

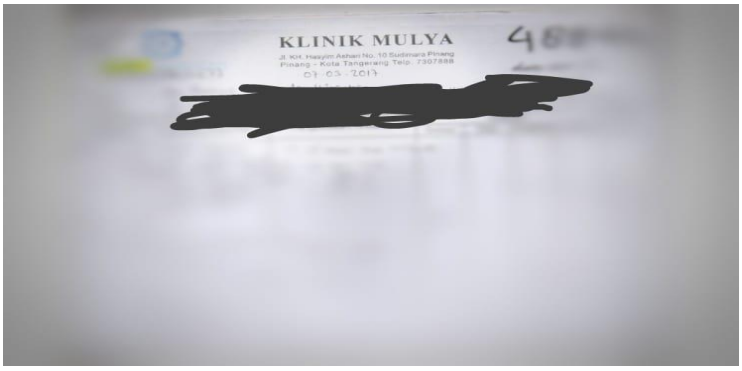
Setelah sistem yang berbasis website ini telah selesai dibuat maka langkah selanjutnya adalah proses pengujian pada setiap fitur yang tersedia. Dalam proses pengujian ini peneliti menggunakan metode *Blackbox testing* yang dimana proses pengujian hanya terfokus terhadap proses input dan output yang sudah di tentukan oleh peneliti. Proses penelitian ini bisa dilihat melalui tabel 5 berikut ini:

Tabel 1. Tabel Pengujian

No	Komponen pengujian	Masukan	Hasil pengujian
1	Login	Pengguna dapat memasukan inputan dan sistem melakukan pengecekan apakah username dan password benar.	berhasil
2	Manajemen user	Dalam proses manajemen user, admin bisa melakukan create, delete dan edit user.	berhasil
3	Pemberian akses	Dalam proses pemberian akses admin bisa mengatur kepada siapa akses diberikan dan pengaturan tanggal untuk mengatur munculnya file tersebut.	berhasil
4	Add dokumen rekam medis	Dalam proses add dokumen rekam medis, akan terjadi proses pengejekan dari size, ektensi dan tipe file. Size yang diijinkan sebesar 4mb, ektensi gambar dan pdf dan tipe file nya gambar atau pdf, Jika diluar ketentuan diatas akan dinyatakan gagal.	berhasil
5	Upgrade dokumen rekam medis	Dalam proses upgrade dokumen rekam medis, akan terjadi proses pengejekan dari size, ektensi dan tipe file. Size yang diijinkan sebesar 4mb, ektensi gambar dan pdf dan tipe file nya gambar atau pdf Jika diluar ketentuan diatas akan dinyatakan gagal.	Berhasil
6	Unduh dokumen rekam medis	Pada proses unduh dokumen rekam medis yang di share kepada permintaan. kondisi file dalam proses unduh telah berhasil terdeskripsi dengan benar.	berhasil
7	Fungsi enkripsi dokumen	Pada proses enkripsi pada file telah terjadinya perubah size ukuran dari size asli ke size telah terenkripsi yang dimana file yang telah di enkripsi memiliki ukuran yang lebih besar dari file aslinya.	berhasil
8	Fungsi deskripsi dokumen	Pada proses deskripsi pada file telah terjadinya perubahan size yang dimana kembali ke ukuran semula.	berhasil

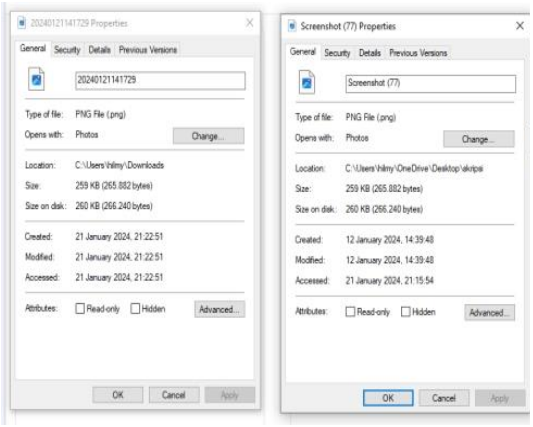
a. Objek Dalam Pengujian

Berikut ini merupakan objek yang berupa sebuah gambar yang digunakan dalam proses pengujian penelitian ini. Objek ini berupa foto yang berisikan rekam medis pasien dari klinik mulya. Objek bisa dilihat pada Gambar 8 ini:

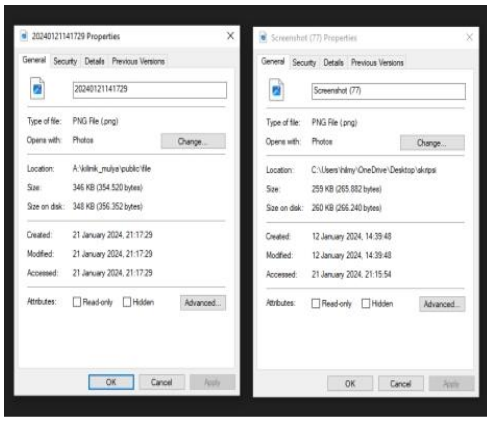


Gambar 8: Objek Pengujian

Pada Gambar 9 dan Gambar 10 merupakan gambar hasil dari proses pengujian pada enkripsi dan deskripsi AES-GCM dengan AES-256. Untuk foto sebelah kiri merupakan foto hasil dari enkripsi dan sebelah kanan file asli dan Untuk foto sebelah kiri merupakan foto hasil dari deskripsi dan sebelah kanan file asli.



Gambar 9: Deskripsi



Gambar 10: enkripsi

3.4 Hasil Analisis

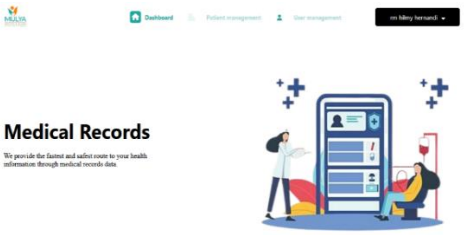
Setelah proses pengujian yang dilakukan oleh peneliti terhadap sistem yang berbasis website ini, peneliti melakukan analisa pengujian terhadap fungsional pada sistem yang penelti buat. Berdasarkan hasil pengujian sebelumnya sistem berjalan sesuai dengan fungsionalnya. Peneliti melakukan pengujian dari tahap penambahan pasien, penambahan user, proses enkripsi file, proses deskripsi file, hapus rekam medis, hapus user, unduh file, menambah rekam medis dan pemberian akses terhadap pasien dan dinas kesehatan. Untuk proses pengecekan file berupa ukuran yang maksimal 4 mb, jenis file dan ektensi file berjalan dengan baik. Hasil yang didapatkan dari proses enkripsi adalah terjadinya perubahan pada ukuran pada file yang dimana ukurannya menjadi lebih besar dari ukuran aslinya. Selain terjadinya perubahan terhadap ukuran dari sebuah size dari sebuah file, file mengalami perubahan pada data file yang awalnya bertipe buffer menjadi tipe data string yang disebabkan oleh hasil dari enkripsi tersebut. Selain terjadi perubahan terhadap data tipe file tersebut perubahan juga terjadi pada panjang data file asli yang berubah menjadi sangat panjang sehingga file tersebut menjadi tidak normal sehingga keamanan isi dari file tersebut menjadi lebih aman dari kondisi file normalnya. Panjang data file bisa menjadi normal ketika terjadi proses deskripsi sehingga isi file bisa di baca kembali. Untuk mengetahui hasil nya tesebut bisa dilihat pada tabel 5 berikut ini.

Tabel 6. Tabel Hasil Enkripsi File

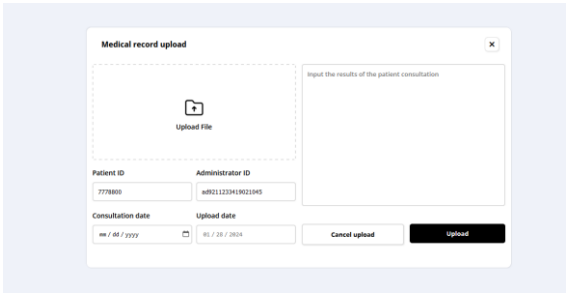
No	Nama file	Panjang data file normal	Panjang data file tidak normal (hasil enkripsi)
1	20240321142626.jpg	155417 byte	266396 karakter
2	20240321145537.jpg	80651 byte	133480 karakter

3.5 Tampilan Layar

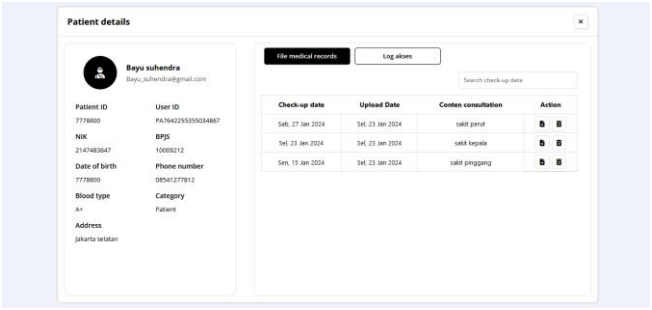
Pada tahapan tampilan layar ini, peneliti akan menampilkan beberapa gambar dari halaman awal, proses add rekam medis yang dimana terjadinya proses enkripsi pada file dokumen rekam medis pasien dan gambar halaman detail pasien yang dimana akan terjadinya proses deskripsi file dengan cara menekan tombol unduh. Gambar tersebut bisa dilhat pada Gambar 11 dan Gambar 12 berikut ini.



Gambar 11. Gambar Tampilan Awal



Gambar 12. Gambar Halamann Add Medical Record



Gambar 13. Detail Pasien

4. KESIMPULAN

Berdasarkan dari hasil analisa dan pengujian pada penelitian yang dilakukan oleh peneliti yang bersumber dari permasalahan tersebut maka bisa mengambil sebuah kesimpulan bahwa sistem berbasis website untuk mengamankan file dan pengelolan rekam medis pasien telah berhasil dibuat mengikuti metodologi *waterfall* dan metode pengujian *blackbox testing* dan dengan adanya sistem ini peneliti berhasil menerapkan dan melakukan proses enkripsi dan deskripsi dengan algoritme AES 256 dan AES GCM sehingga data rekam medis milik klinik mulya akan memiliki keamanan yang tinggi sehingga pihak luar tidak bisa mengetahui isi file daru rekam medis tersebut.

Selain menghasilkan sebuah kesimpulan dari penelitian ini, peneliti memberikan sebuah saran untuk mengembangkan desain atau tampilan website ini dan mengupdate sistem akses yang lebih aman lagi untuk melakukan share.

DAFTAR PUSTAKA

[1] E. Rahmawati, S. Saifudin, C. Kesuma, dan A. N. Rais, "Rancang Bangun Sistem Informasi Rekam Medik Studi Kasus: UPTD Puskesmas Padamara Kabupaten Purbalingga," *Indones. J. Softw. Eng.*, vol. 6, no. 1, hal. 133–144, 2020.

[2] L. D. Simatupang dan K. Khairil, "Pengamanan Dokumen Teks Dengan Menerapkan Kombinasi

Algoritma Kriptografi Klasik," *J. Tek. Inform. UNIKA St. Thomas*, vol. 07, hal. 133–140, 2022.
[3] A. D. Saputra dan M. Syafrullah, "Algoritme AES-256 Untuk Keamanan Basis Data Penilaian Pegawai Pada PT. Buana Jaya Korindo," *Pros. Semin. Nas*, September, hal. 295–301, 2022.
[4] A. Amrulloh dan E. I. H. Ujianto, "Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher," *J. CoreIT*, vol. 5, no. 2, hal. 71–77, 2019.
[5] Noviyanti. P dan Mira, "Analisa Algoritma Kriptografi Klasik Caesar Cipher Viginere Cipher dan Hill Cipher – Study Literature," *J. Inf. Technol.*, vol. 2, no. 1, hal. 23–30, 2022.
[6] Yusfrizal, "Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android," *JTIK (Jurnal Tek. Inform. Kaputama)*, vol. 3, no. 2, hal. 29–37, 2019.
[7] H. Saputra Djong dan S. Siswanto, "Implementasi Kriptografi Dengan Menggunakan Metode Rc4 Dan Aes-256 Untuk Mengamankan File Dokumen Pada PTVarnion Technology Semesta," *Semin. Nas. Mhs. Fak. Teknol. Inf. Jakarta-Indonesia*, no. September, hal. 149–158, 2022.
[8] J. Prayudha, _ S., dan _ I., "Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES)," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 18, no. 2, hal. 119, 2019.
[9] A. . Putra, Herfina, S. Maryana, dan A. Setiawan, "Implementasi Algoritma AES (Advance Encryption Standard) Rijndael Pada Aplikasi Keamanan Data," *Jurnal Ilmiah Penelitian Teknologi informasi & Komputer*, vol. 1, no. 2. hal. 46–51, 2020.
[10] J. Jamaluddin, N. F. Saragih, R. J. Simamora, R. Siringoringo, dan E. N. Purba, "Konsep Pengamanan Video Conference Dengan Enkripsi Aes-Gcm Pada Aplikasi Zoom," *METHOMIKA J. Manaj. Inform. dan Komputerisasi Akunt.*, vol. 4, no. 2, hal. 109–113, 2021.