

**PENERAPAN ALGORITMA AES-256 DAN AES-GCM UNTUK  
MENGAMANKAN DOKUMEN PADA SISTEM DATA REKAM MEDIS  
PADA KLINIK MULYA**

**TUGAS AKHIR**



**Oleh:**

**R. M. HILMY HERNANDI**

**NIM: 1811501798**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNOLOGI INFORMASI  
UNIVERSITAS BUDI LUHUR**

**JAKARTA  
2024**

**PENERAPAN ALGORITMA AES-256 DAN AES-GCM UNTUK  
MENGAMANKAN DOKUMEN PADA SISTEM DATA REKAM MEDIS  
PADA KLINIK MULYA**

**Diajukan untuk memenuhi salah satu persyaratan memperoleh gelar Sarjana  
Komputer (S.Kom)**

**TUGAS AKHIR**



**Oleh:**

**R.M. HILMY HERNANDI**

**NIM: 1811501798**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNOLOGI INFORMASI  
UNIVERSITAS BUDI LUHUR**

**JAKARTA  
2024**



LEMBAR PENGESAHAN



Nama : R.M. Hilmy Hernandi  
Nomor Induk Mahasiswa : 1811501798  
Program Studi : Teknik Informatika  
Bidang Peminatan : Network And Web Security  
Jenjang Studi : Strata 1  
Judul : PENERAPAN ALGORITMA AES-256 DAN AES-GCM UNTUK MENGAMANKAN DOKUMEN PADA DATA REKAM MEDIS KLINIK MULYA

Laporan Tugas Akhir ini telah disetujui, disahkan dan direkam secara elektronik sehingga tidak memerlukan tanda tangan tim penguji.

Jakarta, Selasa 23 Januari

2024 Tim Penguji:

Ketua : Reva Ragam Santika, S.Kom., M.M., M.Kom

Anggota : Pipin Farida Ariyani, S.Kom., M.T.I

Pembimbing : Joko Christian Chandra, S.Kom., M.Kom.

Ketua Program Studi : Dr. Indra, S.Kom., M.T.I

## **Abstrak**

Klinik mulya merupakan sebuah klinik yang memberikan layanan berupa kecantikan, gigi dan umum. 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 pengolahan data rekam medis pasien. Oleh sebab itu peneliti melakukan penelitian dengan menerapkan algoritma AES-256 dan AES-GCM untuk mengamankan file atau dokumen data rekam medis milik pasien dalam sistem sebuah website. Dalam penelitian ini, peneliti melakukan penerapan sebuah metode kualitatif yang berisikan proses pengumpulan data, analisis kebutuhan dan penerapan algoritma 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.

**Keyword: AES-256, AES-GCM dan data rekam medis.**

Xiv + 90 halaman; 84 gambar; 26 tabel;

## SURAT PERNYATAAN TIDAK PLAGIAT DAN PERSETUJUAN PUBLIKASI

### SURAT PERNYATAAN TIDAK PLAGIAT DAN PERSETUJUAN PUBLIKASI

Saya yang bertanda tangan dibawah ini:

Nama : R.M.Hilmy Hernandi  
Nim : 1811501798  
Program Studi : Teknik Informatika  
Bidang Peminatan : Network And Web Security  
Jenjang Studi : Sata Satu (S1)  
Fakultas : Fakultas Teknologi Informasi

Menyatakan bahwa Tugas Akhir yang berjudul:

#### **PENERAPAN ALGORITMA AES-256 DAN AES-GCM UNTUK MENGAMANKAN DOKUMEN PADA SISTEM DATA REKAM MEDIS PADA KLINIK MULYA**

Merupakan:

1. Karya tulis saya, Laporan tugas akhir ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar sarjana, baik di Universitas Budi Luhur maupun di perguruan tinggi lainnya.
2. Karya tulis ini bukan saduran / terjemahan, mumi gagasan, rumusan dan pelaksanaan penelitian / implementasi saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing akademik dan nara sumber di organisasi tempat riset.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Saya menyerahkan hak milik atas karya tulis ini kepada Universitas Budi Luhur, dan oleh karenanya Universitas Budi Luhur berhak melakukan pengelolaan atas karya tulis ini sesuai dengan norma hukum dan etika yang berlaku.
5. Pernyataan ini saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya tulis ini, serta sanksi lainnya sesuai dengan norma yang berlaku di Universitas Budi Luhur dan Undang-Undang yang berlaku.

Jakarta, 21 Januari 2023

  
R.M.Hilmy Hernandi

## **KATA PENGANTAR**

Dengan menyebut Nama Allah Yang Maha Pengasih lagi Maha Penyayang. Puji dan Syukur penulis panjatkan kepada Allah SWT atas Rahmat yang diberikan sehingga Tugas Akhir ini dapat selesai sebagaimana yang diharapkan. Maksud dan Tujuan penyusunan Tugas Akhir ini adalah untuk memenuhi salah satu syarat dalam menyelesaikan jenjang Strata 1 (S1) Fakultas Teknologi Informasi pada program studi Teknik Informatika di Universitas Budi Luhur. Banyak pihak yang telah ikhlas membantu secara langsung maupun tidak langsung dalam penyelesaian Tugas Akhir ini, penulis ucapkan terimakasih yang sebesar-besarnya kepada seluruh pihak yang telah turut andil dalam penyusunan Tugas Akhir, terutama kepada:

1. Allah SWT, atas segala petunjuk dan rahmat-Nya sehingga pada akhirnya penulis dapat menyelesaikan Laporan Tugas Akhir.
2. Ibu dan Ayah serta seluruh keluarga tercinta terimakasih atas Doa restu, perhatian, dan kasih sayang serta dukungan yang telah diberikan kepada penulis.
3. Kepada Rektor Universitas Budi Luhur, bapak Prof. Dr. Agus Setyo Budi, M.Sc.,
4. Kepada Dekan Fakultas Teknologi Informasi Universitas Budi Luhur, bapak Dr. Achmad Solichin, S.Kom, M.T.I.
5. Kepada bapak Joko Christian Chandra, S.Kom., M.Kom., Selaku Lektor program studi Teknik Informatika Universitas Budi Luhur dan juga selaku Dosen Pembimbing yang selalu memberikan bimbingan dan masukan selama penyusunan Tugas Akhir.
6. Kepada bapak Dr. Indra, S.Kom., MTI. Selaku ketua program studi Teknik Informatika Universitas Budi Luhur
7. Seluruh rekan-rekan mahasiswa yang secara langsung maupun tidak langsung, telah turut membantu, memberi motivasi, dan memberi keyakinan kepada penulis dalam penyusunan Tugas Akhir. Semoga Allah SWT membalas kebaikan dan melimpahkan karunia atas segala bantuan yang telah diberikan Amin.

Namun penulis sadar bahwa Tugas Akhir yang telah penulis susun ini masih jauh dari kata sempurna, dan masih terdapat banyak kekurangan dan keterbatasan. Oleh karna itu kritik dan saran sangat diharapkan demi perbaikan di masa mendatang.

Jakarta, 21 januari 2023

Penulis  
Jakarta, 21 januari 2023



## DAFTAR TABEL

Tabel 2. 1 Putaran Kunci Algoritma AES (Hulu dkk.,2020).....	6
Tabel 2. 2 Studi liter.....	14
Tabel 3. 1 Metode pembandingan.....	18
Tabel 3. 2 Rancangan pengujian.....	22
Tabel 3. 3 Tabel user.....	23
Tabel 3. 4 Tabel pasien.....	24
Tabel 3. 5 Tabel rekam medis.....	24
Tabel 3. 6 Tabel akses.....	25
Tabel 3. 7 Tabel kategori user.....	26
Tabel 4. 1 Algoritma login.....	68
Tabel 4. 2 Algoritma forgot password.....	68
Tabel 4. 3 Algoritma add patient dan add user pada admin.....	69
Tabel 4. 4 Algoritma search patient.....	69
Tabel 4. 5 Algoritma add rekam medis.....	70
Tabel 4. 6 Algoritma delete rekam medis.....	70
Tabel 4. 7 Algoritma unduh file rekam medis.....	70
Tabel 4. 8 Algoritma akses rekam medis.....	71
Tabel 4. 9 Algoritma add user.....	71
Tabel 4. 10 Algoritma delete user.....	71
Tabel 4. 11 Algoritma edit user.....	72
Tabel 4. 12 Algoritma enkripsi AES-256.....	72
Tabel 4. 13 Algoritma enkripsi AES-GCM.....	72
Tabel 4. 14 Algoritma deskripsi AES-256.....	73
Tabel 4. 15 Algoritma deskripsi AES-GCM.....	73
Tabel 4. 16 Algoritma redundansi pada halaman medical record.....	73
Tabel 4. 17 Pengujian.....	74




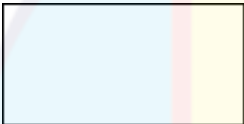

## DAFTAR GAMBAR

Gambar 2. 1 proses enkripsi dan deskripsi simetris.....	5
Gambar 2. 2 proses enkripsi dan deskripsi Asimetris.....	5
Gambar 2. 3 Tabel substitusi S-Box .....	7
Gambar 2. 4 proses shiftrows (Prayudha dkk., 2019).....	8
Gambar 2. 5 proses Mixcolumns (Prayudha dkk.,2019) .....	8
Gambar 2. 6 proses AddRoundKey(Prayudha dkk.,2019) .....	9
Gambar 2. 7 InvShiftRows (Prayudha dkk.,2019).....	9
Gambar 2. 8 InvMixColumns (Prayudha dkk.,2019) .....	10
Gambar 2. 9 metodologi waterfall .....	12
Gambar 2. 10 blackbox testing .....	12
Gambar 2. 11 web server (Ihsan dkk.,2023) .....	13
Gambar 3. 1 arsitektur sistem .....	22
Gambar 3. 2 Diagram arsitektur proses enkripsi dan deskripsi .....	22
Gambar 3. 3 Use case admin.....	26
Gambar 3. 4 Use case diagram nakes .....	27
Gambar 3. 5 Use case diagram pihak luar .....	27
Gambar 3. 6 Entity relationship diagram .....	28
Gambar 3. 7 Logical record structure .....	28
Gambar 3. 8 Rancangan menu sebelum login .....	29
Gambar 3. 9 Rancangan menu setelah login sebagai admin.....	29
Gambar 3. 10 Rancangan menu setelah login sebagai nakes.....	30
Gambar 3. 11 Rancangan menu setelah login sebagai pihak luar.....	30
Gambar 3. 12 Rancangan tampilan awal .....	31
Gambar 3. 13 Rancangan layar login.....	31
Gambar 3. 14 Rancangan layar forgot password .....	32
Gambar 3. 15 Rancangan layar admin dashboard .....	32
Gambar 3. 16 Rancangan layar admin pada menu patient management .....	33
Gambar 3. 17 Rancangan layar menu create patient pada admin .....	33
Gambar 3. 18 Rancangan layar menu detail pasien pada admin .....	34
Gambar 3. 19 Rancangan layar menu log akses pada admin.....	34
Gambar 3. 20 Rancangan layar menu medical pada admin dan nakes.....	35
Gambar 3. 21 Rancangan layar menu akses pada admin.....	35
Gambar 3. 22 Rancangan layar menu user management admin.....	36
Gambar 3. 23 Rancangan layar menu create user admin.....	36
Gambar 3. 24 Rancangan layar menu edit user pada admin.....	37
Gambar 3. 25 Rancangan layar menu dashboard pada nakes .....	37
Gambar 3. 26 Rancangan layar menu dashboard pada pasien dan pihak luar.....	38
Gambar 3. 27 Rancangan layar menu medical record pada pasien dan dinkes .....	38
Gambar 4. 1 flowchart login .....	41
Gambar 4. 2 flowchart forgot password .....	42
Gambar 4. 3 Flowchart add pasien dan add user .....	43
Gambar 4. 4 Flowchart search pasien.....	44
Gambar 4. 5 Flowchart add rekam medis .....	45



Gambar 4. 6 Flowchart delete rekam medis .....	46
Gambar 4. 7 Flowchart unduh file rekam medis.....	47
Gambar 4. 8 Flowchart add akses rekem medis .....	48
Gambar 4. 9 Flowchart add user .....	49
Gambar 4. 10 Flowchart delete user .....	50
Gambar 4. 11 Flowchart edit user.....	51
Gambar 4. 12 Flowchart enkripsi AES .....	52
Gambar 4. 13 Flowchart enkripsi AES-GCM.....	53
Gambar 4. 14 Flowchart deskripsi AES .....	54
Gambar 4. 15 Flowchart deskripsi AES-GCM .....	55
Gambar 4. 16 Flowchart untuk mengatasi redundansi pada halaman medical record.....	56
Gambar 4. 17 Flowchart halaman login.....	57
Gambar 4. 18 Flowchart halaman create pateint dari halaman patient management .....	58
Gambar 4. 19 Flowchart halaman detail pasien dan proses unduh dan delete file .....	59
Gambar 4. 20 Flowchart halaman medical pada menu patient management admin .....	60
Gambar 4. 21 Flowchart halaman akses pada menu patient management admin .....	61
Gambar 4. 22 Flowchart halaman create user pada menu user management admin .....	62
Gambar 4. 23 Flowchart halaman edit user pada menu user management admin.....	63
Gambar 4. 24 Flowchart menu hapus user pada menu user management admin .....	64
Gambar 4. 25 Flowchart halaman detail pasien dan proses unduh dan delete file .....	65
Gambar 4. 26 Flowchart halaman medical pada menu patient management nakes .....	66
Gambar 4. 27 Flowchart popup medical record pada pasien dan dinkes .....	67
Gambar 4. 28 Objek dalam pengujian .....	75
Gambar 4. 29 Gambar pengujian enkripsi .....	75
Gambar 4. 30 Gambar pengujian deskripsi.....	76
Gambar 4. 31 Tampilan layar sebelum login.....	77
Gambar 4. 32 Tampilan layar login .....	77
Gambar 4. 33 Tampilan layar forgot password .....	78
Gambar 4. 34 Tampilan layar setelah login sebagai admin .....	78
Gambar 4. 35 Tampilan layar patient management admin .....	79
Gambar 4. 36 Tampilan layar create patient admin .....	79
Gambar 4. 37 Tampilan layar detail patient admin.....	80
Gambar 4. 38 Tampilan layar log akses di menu detail pada admin .....	80
Gambar 4. 39 Tampilan layar add rekam medis pada admin dan nakes.....	81
Gambar 4. 40 Tampilan layar add akses rekam medis .....	81
Gambar 4. 41 Tampilan layar user management pada admin.....	82
Gambar 4. 42 Tampilan layar add user pada admin .....	82
Gambar 4. 43 Tampilan layar edit user pada admin .....	83
Gambar 4. 44 Tampilan layar dashboard pada nakes .....	83
Gambar 4. 45 Tampilan layar dashboard pada pasien dan dinkes.....	84
Gambar 4. 46 Tampilan layar medical record pada pasien dan dinkes .....	84

DAFTAR SIMBOL

No	Gambar simbol	Nama simbol	Keterangan simbol
1		Terminal	Menggambarkan sebuah awal atau akhir program
2		Decision	Digunakan untuk menanyakan yang memiliki jawaban TRUE/FALSE (YES atau NO)
3		Input/Output	Menggambarkan Input atau Output
4		Proses	Menggambarkan jenis operasi internal seperti inisialisasi atau perhitungan
5		Control Flow	Menunjukkan arah dari aktifitas

## DAFTAR ISI

LEMBAR PENGESAHAN .....	iii
Abstrak.....	iv
SURAT PERNYATAAN TIDAK PLAGIAT DAN PERSETUJUAN PUBLIKASI.....	v
KATA PENGANTAR .....	vi
DAFTAR TABEL.....	vii
DAFTAR GAMBAR .....	viii
DAFTAR SIMBOL .....	x
DAFTAR ISI.....	xi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah .....	2
1.4 Tujuan Penelitian.....	2
1.5 Manfaat penelitian .....	2
1.6 Sistematika Penulisan .....	3
BAB II LANDASAN TEORI.....	4
2.1 Kriptografi .....	4
2.1.1 Algoritma Simetris .....	5
2.1.2 Algoritma Asimetris.....	5
2.2 Kriptografi AES.....	6
2.2.1 Proses Enkripsi.....	6
2.2.2 Proses Deskripsi .....	9
2.2.3 AES-GCM.....	10
2.3 Metodologi Waterfall .....	12
2.4 BlackBox Testing .....	12
2.5 WEB SERVER.....	13
2.6 Data Rekam Medis .....	13
2.7 Studi Literatur.....	14
BAB III METODOLOGI PENELITIAN .....	18
3.1 Data Penelitian.....	18
3.2 Metode perbandingan .....	18
3.3 Penerapan metode.....	19
3.3.1 Pengumpulan Data .....	19
3.3.2 Analisis Kebutuhan .....	20

3.3.3 Penerapan algoritma AES .....	20
3.4 Arsitektur Sistem .....	22
3.5 Diagram Arsitektur Proses Enkripsi Dan Deskripsi .....	22
3.6 Rancangan pengujian.....	22
3.7 Rancangan Basis data .....	23
3.7.1 Spesifikasi Basis Data .....	23
3.7.2 Rancangan kode .....	26
3.7.3 Use Case Diagram.....	26
3.7.4 Entity Relationship Diagram (ERD) .....	28
3.7.5 Logical Record Structure (LRS) .....	28
3.8 Rancangan Menu .....	29
3.9 Rancangan Layar .....	31
3.9.1 Rancangan halaman awal .....	31
3.9.2 Rancangan layar login.....	31
3.9.3 Rancangan layar forgot password .....	32
3.9.4 Rancangan layar Admin dashboard.....	32
3.9.5 Rancangan layar admin pada menu patient management .....	33
3.9.6 Rancangan layar menu create patient pada admin .....	33
3.9.7 Rancangan layar menu detail pasien pada admin .....	34
3.9.8 Rancangan layar menu log akses pada admin.....	34
3.9.9 Rancangan layar menu medical pada admin dan nakes .....	35
3.9.10 Rancangan layar menu akses pada admin .....	35
3.9.11 Rancangan layar menu user management admin .....	36
3.9.12 Rancangan layar menu create user admin .....	36
3.9.13 Rancangan layar menu edit user pada admin .....	37
3.9.14 Rancangan layar menu dashboard pada nakes .....	37
3.9.15 Rancangan layar menu dashboard pada pasien dan dinkes.....	38
3.9.16 Rancangan layar menu medical record pada pasien dan dinkes .....	38
BAB IV HASIL DAN PEMBAHASAN .....	39
4. 1 Lingkungan Percobaan .....	39
4.1.1 Spesifikasi Perangkat Keras .....	39
4.1.2 Spesifikasi Perangkat Lunak .....	39
4. 2 Implementasi Metode .....	39
4. 3 Flowchart .....	41
4.3.1 Flowchart login .....	41
4.3.2 Flowchart forgot password.....	42
4.3.3 Flowchart add pasien dan add user .....	43

4.3.4 Flowchart search pasien	44
4.3.5 Flowchart add rekam medis	45
4.3.6 Flowchart delete rekam medis	46
4.3.7 Flowchart unduh file rekam medis	47
4.3.8 Flowchart add akses rekam medis	48
4.3.9 Flowchart add user	49
4.3.10 Flowchart delete user	50
4.3.11 Flowchart edit user	51
4.3.12 Flowchart enkripsi AES	52
4.3.13 Flowchart enkripsi AES-GCM	53
4.3.14 Flowchart deskripsi AES	54
4.3.15 Flowchart deskripsi AES-GCM	55
4.3.16 Flowchart untuk mengatasi redundansi pada halaman medical record	56
4.3.17 Flowchart halaman login	57
4.3.18 Flowchart halaman create patient dari halaman patient management	58
4.3.19 Flowchart halaman detail pasien dan proses unduh dan delete file	59
4.3.20 Flowchart halaman medical pada menu patient management admin	60
4.3.21 Flowchart halaman akses pada menu patient management admin	61
4.3.22 Flowchart halaman create user pada menu user management admin	62
4.3.23 Flowchart halaman edit user pada menu user management admin	63
4.3.24 Flowchart menu hapus user pada menu user management admin	64
4.3.25 Flowchart halaman detail pasien dan proses unduh dan delete file	65
4.3.26 Flowchart halaman medical pada menu patient management nakes	66
4.3.27 Flowchart popup medical record pada pasien dan dikes	67
4. 4 Algoritma	68
4.4.1 Algoritma login	68
4.4.2 Algoritma forgot password	68
4.4.3 Algoritma add patient dan add user pada admin	69
4.4.4 Algoritma search patient	69
4.4.5 Algoritma add rekam medis	70
4.4.6 Algoritma delete rekam medis	70
4.4.7 Algoritma unduh file rekam medis	70
4.4.8 Algoritma akses rekam medis	71
4.4.9 Algoritma add user	71
4.4.10 Algoritma delete user	71
4.4.11 Algoritma edit user	72
4.4.12 Algoritma enkripsi AES-256	72

4.4.13 algoritma enkripsi AES-GCM.....	72
4.4.14 Algoritma deskripsi AES-256 .....	73
4.4.15 Algoritma deskripsi AES-GCM.....	73
4.4.16 Algoritma redundansi pada halaman medical record .....	73
4. 5 Pengujian .....	74
4.5.1 Objek dalam pengujian.....	75
4.5.2 Gambar pengujian enkripsi .....	75
4.5.3 Gambar pengujian deskripsi.....	76
4. 6 Analisa Pengujian .....	76
4. 7 Tampilan Layar.....	77
4.7.1 Tampilan layar awal sebelum login .....	77
4.7.2 Tampilan layar login .....	77
4.7.3 Tampilan layar forgot password.....	78
4.7.4 Tampilan layar dashboard sebagai admin .....	78
4.7.5 Tampilan layar patient management admin .....	79
4.7.6 Tampilan layar create patient admin .....	79
4.7.7 Tampilan layar detail patient admin.....	80
4.7.8 Tampilan layar log akses di menu detail pada admin .....	80
4.7.9 Tampilan layar add rekam medis pada admin dan nakes.....	81
4.7.10 Tampilan layar add akses rekam medis.....	81
4.7.11 Tampilan layar user management pada admin.....	82
4.7.12 Tampilan layar add user pada admin.....	82
4.7.13 Tampilan layar edit user pada admin .....	83
4.7.14 Tampilan layar dashboard pada nakes .....	83
4.7.15 Tampilan layar dashboard pada pasien dan dinkes .....	84
4.7.16 Tampilan layar medical record pada pasien dan dinkes.....	84
BAB V PENUTUP .....	85
5.1 Kesimpulan.....	85
5.2 Saran .....	85
DAFTAR PUSTAKA .....	86
LAMPIRAN – LAMPIRAN.....	89



## **BAB I PENDAHULUAN**

### **1.1 Latar Belakang**

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 dikembangkan ke arah digitalisasi, yaitu di sektor kesehatan seperti dalam hal Sistem Informasi Manajemen Rumah Sakit. Walaupun pihak pemerintah sedang mengembangkan sistem digitalisasi untuk sektor kesehatan, tetapi masih banyak rumah sakit atau klinik yang masih belum menerapkan Sistem Informasi Manajemen Rumah Sakit yang sedang dibangun oleh pemerintah dikarenakan banyak faktor – faktor yang tidak mendukung penerapan digitalisasi tersebut, seperti halnya klinik tempat peneliti melakukan penelitian.

Klinik mulya merupakan sebuah klinik yang memberikan layanan berupa kecantikan, gigi dan umum. Klinik mulya ini didirikan oleh ibu Gita Gardenia S.E pada tahun 1991. Di klinik mulya, saat ini masih menggunakan metode manual untuk penyimpanan dan pengelolaan data rekam medis pasien, sehingga untuk melakukan pencarian data rekam medis membutuhkan waktu yang relatif lama sehingga menghabiskan waktu sekitar 15 sampai dengan 20 menit. Selain membutuhkan waktu yang lama untuk melakukan pencarian, keamanan pun masih minim karena penyimpanannya secara manual dengan cara disimpan di rak sehingga ketika terjadinya suatu hal seperti bencana alam, kebakaran atau pun pencurian sehingga pihak klinik tersebut tidak memiliki backup pada data rekam medis pasien sehingga ketika dibutuhkan data tersebut sudah tidak ada.

Ada beberapa pihak external yang membutuhkan data rekam medis berupa hasil diagnosa penyakit yang dialami untuk kebutuhan pekerjaan sebagai seorang karyawan dan kebutuhan untuk pendataan oleh pihak dinas kesehatan.

Kriptografi merupakan sebuah ilmu yang mempelajari sebuah teknik enkripsi dan deskripsi yang bertujuan untuk memberikan keamanan informasi pada sebuah objek. Penelitian ini berbeda dengan penelitian lain yang di mana masih banyak yang menggunakan algoritma AES dengan tipe kunci yang pendek seperti penggunaan kunci 128 bit, walaupun bisa dianggap aman, tetapi menurut penulis masih kurang tepat, di karenakan data rekam medis pasien itu sebuah dokumen yang sangatlah sensitif sehingga penulis menerapkan sebuah algoritma AES dengan kunci terpanjang, yaitu 256 bit dan digabungkan dengan AES tipe GCM sehingga menghasilkan sebuah enkripsi dan deskripsi yang terotentikasi sehingga sesuai dengan standar keamanan dan privasi yang di terapkan oleh pemerintah berdasarkan Peraturan Menteri Kesehatan Republik Indonesia Nomor 46 Tahun 2022 tentang Rekam Medis.

Berdasarkan permasalahan yang di atas, penulis memberikan sebuah usulan untuk membuat sebuah sistem yang bisa melakukan pengelolaan data rekam medis pasien dan dengan menerapkan sebuah sistem keamanan dan privasi yang terotentikasi.

Dengan penerapan algoritma kriptografi, maka pengguna tidak perlu khawatir atas keamanan dan privasi terhadap dokumen atau fail data rekam medis yang tersimpan di databases website ini.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang masalah, maka dapat dirumuskan masalah sebagai berikut:

- a. Bagaimana mengamankan dokumen atau file dari data rekam medis pasien sesuai dengan standar keamanan dan privasi dari Peraturan Menteri Kesehatan Republik Indonesia Nomor 46 Tahun 2022 tentang Rekam Medis, dengan mengimplementasikan algoritma kriptografi Advanced Encryption Standar-256 (AES-256) dan algoritma kriptografi Advanced Encryption Standar Galois/Counter Mode (AES-GCM)?
- b. Bagaimana membuat sebuah sistem yang mendukung mekanisme sharing dan keamanan yang tinggi untuk melindungi data rekam medis pasien.

## 1.3 Batasan Masalah

Agar tidak menyimpang dari materi pembahasan, maka akan diberikan beberapa Batasan permasalahan sebagai berikut:

- a. Algoritma kriptografi yang digunakan yaitu Advanced Encryption Standar – 256 (AES-256) dan algoritma kriptografi Advanced Encryption Standar - Galois/Counter Mode (AES-GCM).
- b. Data yang akan diamankan berupa file atau dokumen yang memiliki sebuah ekstensi pdf atau pun gambar dengan ukuran kurang dari 4MB.
- c. Bahasa pemrograman yang digunakan, yaitu bahasa pemrograman Java Script (js).

## 1.4 Tujuan Penelitian

Berdasarkan latar belakang dan rumusan masalah yang telah dijabarkan sebelumnya, maka tujuan dari penulisan ini ialah untuk mengembangkan sistem dengan pendekatan *waterfall* dan menerapkan algoritma kriptografi berbasis website dengan menggunakan algoritma AES-256 dan AES-GCM sebagai alat keamanan dan privasi pada dokumen atau file.

## 1.5 Manfaat penelitian

Ada manfaat dari penulisan ini adalah memberikan solusi atas kebutuhan tempat riset, berupa:

- a. Menghasilkan sebuah website yang memiliki keamanan dan privasi data sesuai dengan standar dari Peraturan Menteri Kesehatan Republik Indonesia Nomor 46 Tahun 2022 tentang Rekam Medis.
- b. Sistem dengan mekanisme share rekam medis untuk pihak luar.
- c. Dengan ada penelitian ini pengguna tidak perlu merasa khawatir terjadinya kebocoran data dari data rekam medis tersebut dikarenakan website ini memiliki keamanan dan privasi pada file atau dokumennya yang kuat.
- d. Dengan adanya website ini pengguna dari sisi pasien bisa dengan mudah mendapatkan hasil diagnosis dokter dengan melengkapi persyaratan dari klinik mulya.

## 1.6 Sistematika Penulisan

Pada sistematika penulisan ini akan menggambarkan mengenai beberapa bab dalam penulisan Tugas Akhir sebagai berikut:

### **BAB I PENDAHULUAN**

Pada bagian bab ini membahas sebuah latar belakang, perumusan masalah, batasan masalah, tujuan penulisan, manfaat penulisan dan sistematika penulisan.

### **BAB II LANDASAN TEORI**

Pada bagian bab ini membahas tentang uraian dari pengertian dan penjelasan dari teori dasar yang mencakup dari metodologi *waterfall*, kriptografi, algoritma kriptografi AES-256 dan algoritma kriptografi AES-GCM dan *blackbox testing* yang digunakan dan beberapa teori yang berhubungan dengan judul yang bersumber pada buku, jurnal dan website yang digunakan sebagai acuan atau landasan penelitian ini.

### **BAB III METODE PENELITIAN**

Pada bagian bab ini penulis membahas tentang pelaksanaan penelitian, penyelesaian terhadap permasalahan yang dihadapi dalam penelitian ini, penerapan teori dasar yang telah dijabarkan pada Bab II mengenai metodologi, kriptografi, algoritma kriptografi AES-256, algoritma kriptografi AES-GCM dan rancangan – racangan yang akan digunakan dalam penelitian.

### **BAB IV HASIL DAN PEMBAHASAN**

Pada bagian bab ini berisikan tentang implementasi program yang telah dirancang oleh penulis dan melakukan uji coba solusi, spesifikasi perangkat lunak dan perangkat keras dalam penelitian ini.

### **BAB V PENUTUP**

Pada bab ini berisikan sebuah kesimpulan hasil penelitian dan saran penulis.

## **BAB II**

### **LANDASAN TEORI**

#### **2.1 Kriptografi**

Kriptografi merupakan sebuah seni keamanan yang bertujuan untuk mengamankan sebuah objek yang bersifat rahasia dengan melalui proses enkripsi dengan cara mengubah objek atau isi objek asli yang awalnya sebagai plaintext berubah menjadi ciphertext dan untuk deskripsi yaitu isi atau objek yang telah berubah menjadi ciphertext akan diubah kembali ke bentuk aslinya atau menjadi plaintext, sehingga hanya pemilik objek dan penerima objek yang bisa mengetahui isi dari objek tersebut.

Selain terdapat sebuah pengertian tentang kriptografi itu sendiri kriptografi memiliki beberapa bagian – bagian penting dalam proses seperti plaintext, ciphertext, enkripsi, deskripsi, key publik atau kunci publik dan key privat atau kunci privat.

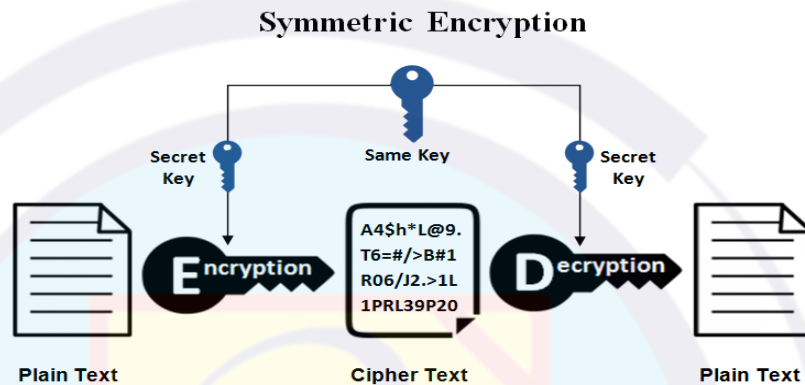
Bagian – bagian dalam proses melakukan proses penerapan algoritma kriptografi:

1. Plaintext  
merupakan sebuah objek atau isi dari objek yang asli sebelum terjadinya perubahan dalam proses enkripsi
2. Ciphertext  
merupakan sebuah objek atau isi dari objek yang sudah terjadinya proses enkripsi
3. Enkripsi  
proses dimana informasi atau data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu (Amrulloh dan Ujianto,2019).
4. Dekripsi  
Proses untuk mengembalikan bentuk semula dari sebuah objek atau isi objek dari hasil enkripsi
5. Kunci rahasia atau key privat  
kunci yang sama digunakan oleh pengirim dan penerima dalam melakukan enkripsi dan deskripsi pesan (Noviyanti dan Mira,2022).
6. Kunci publik atau key publik  
Merupakan sebuah kunci yang bersifat terbuka atau sebuah kunci yang hanya di berikan oleh pemilik objek yang bersifat rahasia tersebut.

Selain bagian – bagian penting dalam kriptografi, kriptografi memiliki dua jenis berdasarkan jumlah kunci yang digunakan.

### 2.1.1 Algoritma Simetris

Menurut Yusfrizal (2019), tentang algoritma simetris merupakan algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsinya. Algoritma kriptografi simetris sering disebut algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma satu kunci, dan mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu. Kelebihan dari algoritma kriptografi simetris adalah waktu proses untuk enkripsi dan dekripsi relatif cepat. Hal ini disebabkan efesiensi yang terjadi pada pembangkit kunci. Proses kerja dari algoritma simetris seperti gambar 2. 1.

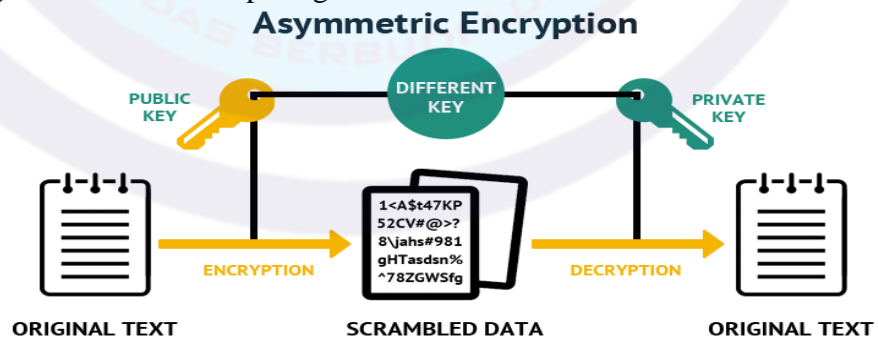


Gambar 2. 1 proses enkripsi dan deskripsi simetris

Ada beberapa algoritma kriptografi yang menggunakan kunci simetris dalam proses enkripsi dan deskripsi seperti AES, DES, 3DES, Blowfish dan RC4.

### 2.1.2 Algoritma Asimetris

Selain terdapat jenis kunci simetris algoritma kriptografi menerapkan sebuah jenis kunci yaitu kunci asimetris. Kunci asimetris merupakan sebuah jenis kunci yang mengabungkan antara kunci publik dengan kunci privat dalam proses enskripsi dan deskripsinya. Proses kerja dari algoritma asimetris seperti gambar 2.2.



Gambar 2. 2 proses enkripsi dan deskripsi Asimetris

Ada beberapa algoritma kriptografi yang menggunakan kunci asimetris dalam proses enkripsi dan deskripsi seperti RSA, DSA dan Diffie-Hellman.



## 2.2 Kriptografi AES

Pemerintah Amerika Serikat dan National Institute of Standards and Technology pada tahun 1997 menetapkan bahwa Algoritma DES yang dikembangkan oleh IBM pada tahun 1970-an dinyatakan sudah tidak begitu kuat dalam keamanan yang disebabkan oleh terjadinya perkembangan teknologi komputer sehingga pihak Amerika Serikat dan National Institute of Standards and Technology membutuhkan sebuah algoritma pengganti DES, sehingga pihak National Institute of Standards and Technology mengadakan kompetisi internasional untuk mencari algoritma keamanan yang lebih kuat untuk menggantikan algoritma DES.

Pada tahun 2001 terdapat dua kriptografer yang berasal dari Belgia mengikuti kompetisi yang diselenggarakan oleh pihak National Institute of Standards. dua kriptografer ini bernama Vincent Rijmen dan Joan Daemen, dua kriptografer ini melakukan pengajuan sebuah algoritma bernama Rijndael dalam kompetisi internasional tersebut. Nama algoritma Rijndael ini diambil dari nama dua kriptografer tersebut. Pada tahun yang sama, pihak dari National Institute of Standards menyatakan bahwa algoritma Rijndael karya dari Vincent Rijmen dan Joan Daemen sebagai pemenang dalam kompetisi internasional ini, sehingga pihak penyelenggara mengadopsi algoritma Rijndael tersebut dan merubah namanya menjadi Advanced Encryption Standard atau dikenal sebagai algoritma AES yang bertujuan untuk mengganti algoritma DES tersebut.

Advanced Encryption Standard atau disingkat AES merupakan sebuah jenis algoritma simetris dikarenakan hanya menggunakan satu kunci yang bersifat privat dalam proses enkripsi dan dekripsinya.

Algoritma AES ini memiliki tiga jenis panjang kunci yang digunakan dalam proses enkripsi dan dekripsinya. Setiap jenis panjang kunci tersebut memiliki jumlah putaran yang berbeda dalam prosesnya. Nama dan jumlah kunci pada AES bisa dilihat di tabel 2.1 dibawah ini.

Tabel 2. 1 Putaran Kunci Algoritma AES (Hulu dkk.,2020)

AES (Bits)	Panjang Kunci (Nk Words)	Ukuran Blok (Nb Word)	Jumlah Putaran (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Pada proses enkripsi dan dekripsi pada algoritma AES memiliki beberapa tahapan dalam prosesnya.

### 2.2.1 Proses Enkripsi

Pada proses enkripsi akan menghasilkan sebuah transformasi, dalam proses transformasi ada empat jenis transformasi yang digunakan dalam prosesnya yaitu:

#### 1. SubBytes

Menurut Saputra Djong dan Siswanto. (2022), SubBytes merupakan transformasi byte yang dilakukan dengan cara



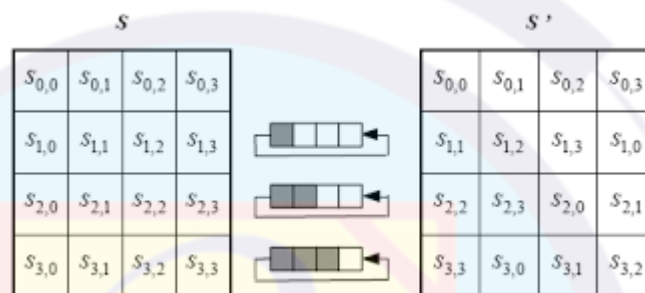
mensubstitusikan atau mengganti setiap byte dari state dengan byte yang berada pada tabel S-Box AES. Setiap nilai byte dalam array state, misalkan  $S[r, c] = xy$  dan  $xy$  adalah digit heksadesimal dari nilai  $S[r, c]$ . Nilai yang menggantikan  $S[r, c]$  dinyatakan dengan  $S'[r, c]$ , yaitu bilangan heksadesimal yang berada pada tabel S-Box AES. Pada tahap SubBytes bisa dilihat dari gambar 2.3 ini.

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Gambar 2. 3 Tabel substitusi S-Box

## 2. ShiftRows

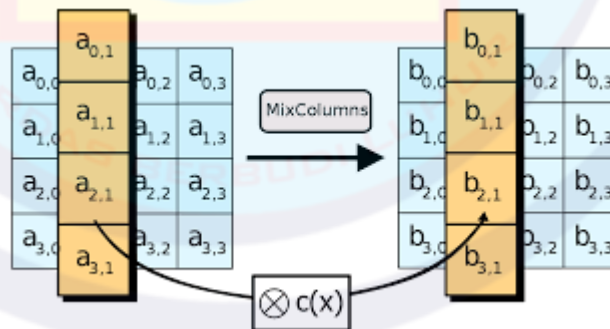
Pada proses tahap shiftrows, menurut Saputra Djong dan Siswanto. (2022), Shiftrows adalah transformasi yang melakukan pergeseran nilai byte pada tiga baris terakhir dari array state. Banyak pergeseran bergantung pada nilai baris  $r$ . Ketentuannya yaitu jika baris  $r$  sama dengan 1 maka pergeseran dilakukan sebanyak satu byte, jika baris  $r$  sama dengan 2 maka pergeseran dilakukan sebanyak dua byte, dan jika baris  $r$  sama dengan 3 maka pergeseran dilakukan sebanyak tiga byte. Baris  $r$  sama dengan 0 maka tidak dilakukan pergeseran sama sekali. Proses kedua ini bisa di lihat dari gambar 2.4.



Gambar 2. 4 proses shiftrows (Prayudha dkk., 2019)

## 3. MixColumns

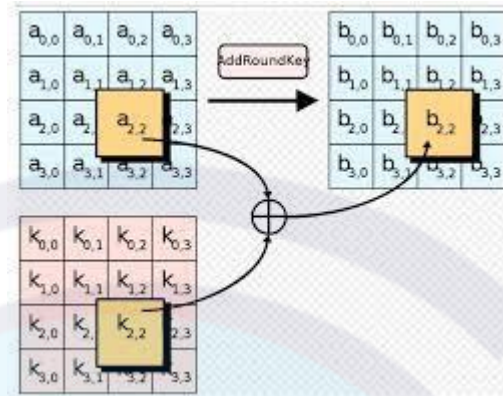
MixColumns mengoperasikan setiap elemen yang berada dalam satu kolom pada state. Secara lebih jelas, transformasi mixcolumns dapat dilihat pada perkalian matriks pada gambar 2.5 berikut ini (Prayudha dkk.,2019).



Gambar 2. 5 proses Mixcolumns (Prayudha dkk.,2019)

#### 4. AddRoundkey

Pada proses addroundkey akan melakukan XOR antara state sekarang dengan round key seperti gambar 2.6 dibawah ini (Prayudha dkk.,2019).



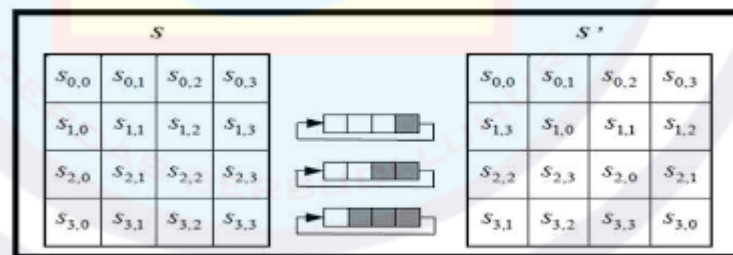
Gambar 2. 6 proses AddRoundKey(Prayudha dkk.,2019)

#### 2.2.2 Proses Deskripsi

Pada proses deskripsi ada empat jenis transformasi bytes yang digunakan dalam proses nya yaitu:

##### 1. InvShiftRows

Pada proses InvShiftRows yang dimana merupakan proses yang diberlawanan dengan proses ShiftRows sehingga byte data sekarang berada di posisi sebelah kanan di pindahkan ke sisi sebelah kiri kembali. Proses InvShiftRows bisa dilihat dari gambar 2.7 dibawah ini.



Gambar 2. 7 InvShiftRows (Prayudha dkk.,2019)

##### 2. InvSubBytes

InvSubBytes juga merupakan transformasi bytes yang berkebalikan dengan transformasi SubBytes. Pada InvSubBytes, tiap elemen pada state dipetakan dengan menggunakan tabel Inverse S-Box (Prayudha dkk.,2019).

##### 3. InvMixColumns

Setiap kolom dalam state dikalikan dengan matrik perkalian dalam AES. Perkalian dalam matrik dapat dilihat seperti contoh gambar 2.8 dibawah ini (Prayudha dkk.,2019):

$$\begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

Gambar 2. 8 InvMixColumns (Prayudha dkk.,2019)

#### 4. AddRoundKey

Transformasi Inverse AddRoundKey tidak berbeda dengan transformasi AddRoundkey karna dalam transformasi ini hanya dilakukan operasi penambahan sederhana dengan operasi bitwise XOR (Prayudha dkk.,2019).

Selain memiliki perbedaan jenis panjang kunci, AES memiliki beberapa jenis mode dalam proses enkripsi dan deskripsi seperti ECB, CBC, CFB, OFB, CTR dan GCM.

#### 2.2.3 AES-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 (Jamaluddin dkk.,2020). pada proses enkripsi dan deskripsi peneliti melakukan pengutipan dari jurnal dengan penulis Almorabea, A. M., & Aslam, M. A. (2015). "Symmetric Key Encryption Using AES-GCM and External Key Derivation for Smart Phones." Nama Jurnal, Volume 3(6).

##### a. Proses enkripsi AES-GCM

Dalam proses enkripsi menurut Almorabea, A. M., & Aslam, M. A. (2015) yang diartikan ke dalam bahasa indonesia oleh penulis, proses enkripsi AES pada mode gcm dengan panjang kunci 256. Proses enkripsi kami menggunakan nonce dengan panjang 16 byte. Berkas input dienkripsi bersama dengan kunci 256 bit yang dihasilkan pada langkah pertama dan AES. Kerjasama antara AES dan nonce memastikan kerahasiaan dan keaslian (integritas) dari berkas

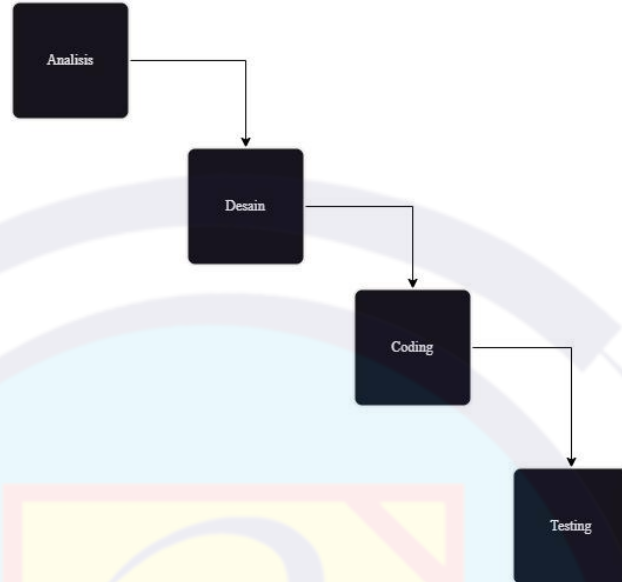
terenkripsi. Fitur menarik dari proses enkripsi kami adalah nilai unik nonce untuk setiap proses enkripsi, yaitu nilai nonce akan berbeda untuk setiap proses enkripsi dan akan unik untuk setiap berkas gambar atau input, serta nonce ini akan berada pada 16 byte pertama dalam berkas input. Proses enkripsi kami memaksimalkan langkah-langkah keamanan dengan menghasilkan hasil yang berbeda untuk gambar input yang sama. Artinya, jika kita mengenkripsi gambar yang sama (gambar asli) dua kali, hasilnya tidak akan sama. Fitur ini meningkatkan integritas informasi dan keamanan dari sumber yang tidak sah, seperti para penyerang. Hal ini dikarenakan jika para penyerang menyadap gambar yang sama dengan dua berkas enkripsi, mereka tidak akan dapat memahami bahwa kedua gambar tersebut identik. Hal ini disebabkan oleh penggunaan nonce yang bersifat acak dan tidak akan mengulangi nilai dua kali. Proses enkripsi mengenkripsi berkas input dan membuatnya siap untuk dibagikan dengan pihak lain. Pada akhir proses ini, berkas input (misalnya, berkas gambar) menjadi tidak dapat dibaca dan tidak dapat dikenali oleh aplikasi terkait sebagai berkas yang valid, kecuali jika didekripsi dan informasi asli dikembalikan. Pada proses enkripsi ini terdapat sebuah nonce dalam prosesnya. Nonce memiliki nama lain yaitu IV atau Initialization Vector

b. Proses deskripsi

Dalam proses deskripsi menurut Almorabea, A. M., & Aslam, M. A. (2015) yang diartikan ke dalam bahasa Indonesia oleh penulis, Proses dekripsi melibatkan beberapa langkah untuk memulihkan informasi asli dari file terenkripsi. Pertama, nonce diekstraksi dari file terenkripsi. Setelah nonce atau IV diekstraksi, kunci disuntikkan ke dalam file untuk memungkinkan fungsi dekripsi mendekripsi file masukan. Jika kunci masukan benar, file akan berhasil didekripsi. Namun, jika ada pemalsuan data, bahkan satu byte saja, fungsi dekripsi akan mendeteksinya dan tidak akan mendekripsi file masukan.

### 2.3 Metodologi Waterfall

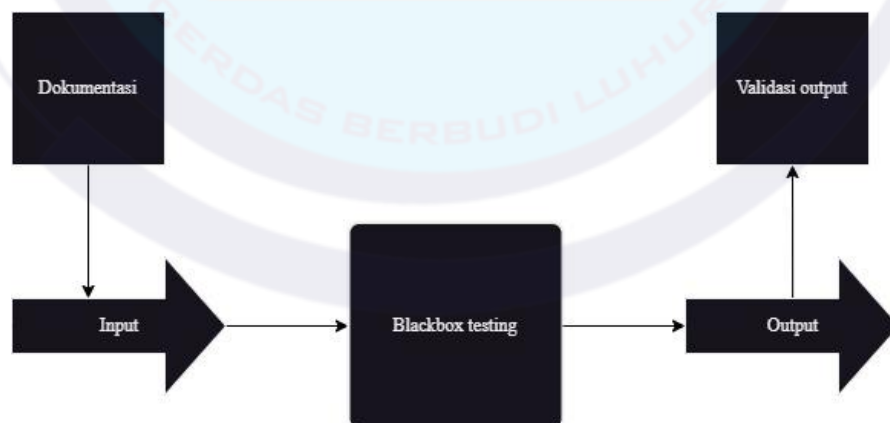
Merupakan sebuah metode pengembangan perangkat lunak dengan meliputi proses analisis, desain, coding dan pengujian pada sebuah perangkat lunak. Proses Metodologi *waterfall* yang digunakan dalam penelitian ini bisa dilihat dari gambar 2.9 dibawah ini:



Gambar 2. 9 metodologi waterfall

### 2.4 BlackBox Testing

Merupakan sebuah metode pengujian pada perangkat lunak untuk mengetahui apakah sebuah perangkat lunak tersebut berfungsi sesuai dengan tujuan pembuatan perangkat lunak yang merupakan sebuah website. Proses dalam penggunaan *blackbox testing* ini hanya meliputi dari input dan output dari perangkat lunak yang berupa sebuah website. Proses *blackbox testing* bisa dilihat di gambar 2.10 bawah ini:

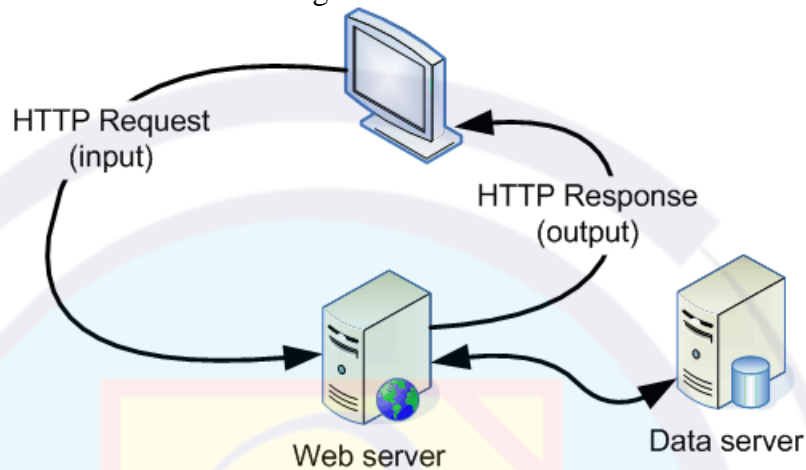


Gambar 2. 10 blackbox testing



## 2.5 WEB SERVER

Menurut Ihsan dkk (2020), web server adalah software yang memberikan layanan data yang mempunyai fungsi untuk menerima permintaan HTTP (HyperText Transfer Protocol) atau HTTPS (Hypertext Transfer Protocol Secure) yang dikirim oleh klien melalui web browser dan mengirimkan kembali hasilnya dalam bentuk halaman web yang umumnya berbentuk dokumen HTML (HyperText Markup Language). Proses kerja pada web server bisa dilihat dari gambar 2.11 dibawah ini:



Gambar 2. 11 web server (Ihsan dkk.,2023)

## 2.6 Data Rekam Medis

Data rekam medis adalah dokumen yang berisikan data identitas pasien, pemeriksaan, pengobatan, tindakan dan pelayanan lain yang telah diberikan kepada pasien (Rahmawati dkk.,2020). Ada sebuah peraturan yang di keluarkan oleh menteri kesehatan indonesia yang dicantumkan pada peraturan Menteri Kesehatan Republik Indonesia Nomor 46 Tahun 2022 tentang Rekam Medis. Detail pasal yang terkait akan disajikan dalam lampiran. Umumnya data rekam medis mencakup informasi seperti nama, umur, karakteristik fisik seperti tinggi, berat, golongan darah, riwayat penyakit, pengobatan yang pernah diberikan dan tindakan yang pernah dilakukan oleh pihak penyedia layanan kesehatan.

## 2.7 Studi Literatur

Dalam studi literatur ini ada beberapa referensi yang digunakan oleh penulis diantaranya:

**Tabel 2. 2 Studi liter**

Judul	:	Algoritme AES-256 Untuk Keamanan Basis Data Penilaian Pegawai Pada Pt. Buana Jaya Korindo
Penulis	:	Anggi Dwi Saputra, Mohammad Syafrullah
Tahun	:	2022
Jurnal	:	Seminar Nasional Mahasiswa Fakultas Teknologi Informasi
ISSN	:	2962-8628
Deskripsi	:	Dalam penelitian ini berfokus terhadap penggunaan algoritma kriptografi AES dengan panjang kunci 256 untuk memberikan keamanan lebih terhadap data – data yang ada dari Pt. Buana Jaya Korindo.
Link	:	<a href="http://senafiti.budiluhur.ac.id/index.php/senafiti/article/view/237#">http://senafiti.budiluhur.ac.id/index.php/senafiti/article/view/237#</a>
Judul	:	Implementasi Advanced Encryption Standard Pada Enkripsi Dan Dekripsi Dokumen Rahasia Diintelkam Polda DIY
Penulis	:	Berita Estu Widodo, A. Sidiq Purnomo
Tahun	:	2020
Jurnal	:	Jurnal Teknik Informatika
e-ISSN	:	2723-3871
Deskripsi	:	Dalam penelitian ini hanya berfokus terhadap proses pemberian keamanan lebih terhadap file dokumen dari Polda DIY dengan menggunakan algoritma AES dengan panjang kunci 256 bit. selain memberikan keamanan lebih ada aspek lain yang di teliti yaitu kecepatan proses enkripsi dan proses deskripsi tersebut.
Link	:	<a href="http://www.jutif.if.unsoed.ac.id/index.php/jurnal/article/view/21">http://www.jutif.if.unsoed.ac.id/index.php/jurnal/article/view/21</a>
Judul	:	Implementasi Algoritma Advanced Encryption Standard dalam Pengamanan Data Penjualan Ramayana Department Store.
Penulis	:	Sunil Setti , Indra Gunawan, Bahrudi Efendi Damanik, Sumarno, Ika Okta Kirana.
Tahun	:	2020
Jurnal	:	Jurnal Riset Komputer
e-ISSN	:	2715-7393
Deskripsi	:	Pada penelitian ini terfokus terhadap mengamankan data penjualan dari Ramayana department store berupa sebuah file dengan ekstensi berupa .doc, .xls, .ppt, .pdf. hasil dari proses enkripsi dan deskripsi ini akan berpengaruh terhadap ukuran file dan kecepatan dalam prosesnya. Dalam penelitian ini hanya

		menggunakan sebuah algoritma tunggal yaitu algoritma AES tanpa menggunakan sebuah mode AES dan dengan panjang kunci yaitu 128. Hasil dari penelitian ini berupa sebuah website
Link	:	<a href="http://www.ejurnal.stmik-budidarma.ac.id/index.php/jurikom/article/view/1960">http://www.ejurnal.stmik-budidarma.ac.id/index.php/jurikom/article/view/1960</a>
Judul	:	Implementasi Algoritma AES (Advance Encryption Standard) Rijndael Pada Aplikasi Keamanan Data.
Penulis	:	Agung Prajuhana Putra, Herfina, Sufiatul Maryana, Andrian Setiawan.
Tahun	:	2020
Jurnal	:	Jurnal Ilmiah Penelitian Teknologi Informasi & Komputer
ISSN	:	2722-953X
Deskripsi	:	Pada penelitian ini berfokus terhadap file digital dengan menerapkan sebuah algoritma tunggal yaitu algoritma AES dengan panjang kunci AES yaitu 128 bit. dalam proses penelitian ini terfokus terhadap kecepatan waktu dan perubahan ukuran dalam proses enkripsi dan deskripsinya. Hasil dari penelitian ini berupa sebuah aplikasi untuk android.
Link	:	<a href="https://journal.upgris.ac.id/index.php/jipetik/article/view/KAI">https://journal.upgris.ac.id/index.php/jipetik/article/view/KAI</a>
Judul	:	Implementasi Algoritma AES-128 Dan SHA-256 Dalam Perancangan Aplikasi Pengamanan File Dokumen.
Penulis	:	Herman, Robby Wijaya, Kenner Farandi, Satriya Miharja, Wilson.
Tahun	:	2021
Jurnal	:	Jurnal Times Technology Informatics & Computer System
e-ISSN	:	2549 – 015X
Deskripsi	:	Dalam penelitian ini berfokus terhadap pengamanan terhadap sebuah file dengan menghasilkan sebuah aplikasi yang dimana dalam proses nya tersebut melibatkan dua algoritma yaitu algoritma AES dengan panjang kunci 128bit dan algoritma SHA dengan panjang kunci 256 bit.
Link	:	<a href="https://ejournal.stmik-time.ac.id/index.php/jurnalTIMES/article/view/666">https://ejournal.stmik-time.ac.id/index.php/jurnalTIMES/article/view/666</a>
Judul	:	Implementasi Algoritma AES 256 Bit Dan Lsb Untuk Pengamanan Dan Penyisipan Pesan Teks Pada File Audio.
Penulis	:	Ricaro Laia
Tahun	:	2020
Jurnal	:	Jurnal Pelita Informatika
ISSN	:	2301-9425
Deskripsi	:	Dalam penelitian ini berfokus terhadap mengamankan sebuah file audio dengan menghasilkan sebuah software yang berbasis gui

		dengan menerapkan sebuah algoritma AES dengan panjang kunci yaitu 256 dan menggunakan sebuah metode stegonagrafik yaitu LSB
Link	:	<a href="https://ejurnal.stmik-budidarma.ac.id/index.php/pelita/article/view/2445/1721">https://ejurnal.stmik-budidarma.ac.id/index.php/pelita/article/view/2445/1721</a>
Judul	:	Implementasi Algoritma AES 256 CBC, BASE 64, Dan SHA 256 Dalam Pengamanan Dan Validasi Data Ujian Online
Penulis	:	Ferzha Putra Utama , Gusman Wijaya , Ruvita Faurina , Arie Vatesia
Tahun	:	2023
Jurnal	:	Jurnal Teknologi Informasi dan Ilmu Komputer
e-ISSN	:	2528-6579
Deskripsi	:	Dalam penelitian ini berfokus untuk melindungi data asli dari ujian online berbasis website, dengan menggunakan gabungan dari beberapa algoritma yaitu AES 256 dengan mode CBC, BASE 64, Dan SHA 256.
Link	:	<a href="https://jtiik.ub.ac.id/index.php/jtiik/article/view/6558">https://jtiik.ub.ac.id/index.php/jtiik/article/view/6558</a>
Judul	:	Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSUD Imelda Medan.
Penulis	:	Delisman Hulu, Berto Nadeak, Soeb Aripin
Tahun	:	2020
Jurnal	:	Konferensi Nasional Teknologi Informasi dan Komputer
e-ISSN	:	2597-4645
Deskripsi	:	Dalam penelitian berfokus terhadap keamanan file hasil radiologi di RSUD imelda Medan dengan menggunakan sebuah algoritma AES dengan panjang kunci 128bit dan jenis file yang di amankan berupa jenis gambar. Dalam penelitian ini akan menghasilkan sebuah website.
Link	:	<a href="https://ejurnal.stmik-budidarma.ac.id/index.php/komik/article/view/2645">https://ejurnal.stmik-budidarma.ac.id/index.php/komik/article/view/2645</a>
Judul	:	Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES).
Penulis	:	Jaka Prayudha, Saniman, Ishak
Tahun	:	2019
Jurnal	:	Sains dan Komputer
e-ISSN	:	2615-3475
Deskripsi	:	Dalam penelitian ini berfokus untuk mengamankan data gaji pada karyawan dengan menggunakan sebuah algoritma tunggal yaitu AES dengan panjang kunci 128 bit. dalam penelitian ini akan menghasilkan sebuah software desktop.

Link	:	<a href="http://ojs.trigunadharma.ac.id/index.php/jis/article/viewFile/150/100">http://ojs.trigunadharma.ac.id/index.php/jis/article/viewFile/150/100</a>
Judul	:	Implementasi Kriptografi AES-128 Untuk Mengamankan url (UNIFORM RESOURCE LOCATOR) Dari Sql Injection.
Penulis	:	Hamid Wijaya
Tahun	:	2020
Jurnal	:	JURNAL AKADEMIKA
e-ISSN	:	2548-4184
Deskripsi	:	Dalam penelitian ini berfokus terhadap pengamanan terhadap URL supaya terlindungi dari serangan sql injection dengan menerapkan sebuah algoritma AES dengan panjang kunci yaitu 128 bit. dalam proses uji coba pada penelitian ini menggunakan sqlmap untuk mengetahui apakah berhasil menerapkan atau tidak.
Link	:	<a href="https://www.ejournal.lppmunidayan.ac.id/index.php/akd/article/view/129/20">https://www.ejournal.lppmunidayan.ac.id/index.php/akd/article/view/129/20</a>
Judul	:	Rancang Bangun Sistem Informasi Rekam Medik Studi Kasus: UPTD Puskesmas Padamara Kabupaten Purbalingga.
Penulis	:	Eka Rahmawati, Saifudin, Chandra Kesuma, Amin Nur Rais
Tahun	:	2020
Jurnal	:	Indonesian Journal on Software Engineering
e-ISSN	:	2714-9935
Deskripsi	:	Pada penelitian ini berfokus terhadap pembangunan sebuah sistem informasi rekam medik yang bertujuan untuk mempermudah penyimpanan data, melakukan pencarian data dan hanya beberapa user yang bisa mengaksesnya yang mendapatkan ijin atau yang berwenang dari pihak rumah.
Link	:	<a href="https://www.neliti.com/id/publications/490685/rancang-bangun-sistem-informasi-rekam-medik-studi-kasus-uptd-puskesmas-padamara">https://www.neliti.com/id/publications/490685/rancang-bangun-sistem-informasi-rekam-medik-studi-kasus-uptd-puskesmas-padamara</a>

## BAB III METODOLOGI PENELITIAN

### 3.1 Data Penelitian

Dalam penelitian ini data yang digunakan atau didapatkan berasal dari klinik mulya berupa sebuah file hasil scanner 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.

### 3.2 Metode pembandingan

Pada metode pembandingan ini peneliti melakukan pembandingan antara 2 penelitian yang lain dengan penelitian yang peneliti lakukan. Pada proses metode pembandingan ini bisa dilihat dari tabel di bawah ini:

**Tabel 3. 1 Metode pembandingan**

NO	JUDUL	Karakteristik Metode		Perbandingan metode yang digunakan peneliti
		kelebihan	kekurangan	
1	Implementasi Algoritma AES (Advance Encryption Standard) Rijndael Pada Aplikasi Keamanan Data.	Pada penelitian ini berhasil melakukan proses enkripsi dan deskripsi pada sistem nya.	Hanya menggunakan satu jenis algoritma kriptografi dalam proses penelitian tersebut	dalam hal perbandingan metode yang digunakan oleh peneliti terletak pada jumlah algoritma dan panjang kuncinya. Pada penelitian ini, peneliti menggunakan 2 algoritma yaitu AES dan AES-GCM. Untuk panjang kunci yang digunakan yaitu untuk kedua algoritma sebesar 256 bit. selain jumlah dan panjang kunci, penelitian ini akan menggunakan 2 kunci privat dan 2 kunci tambahan dalam proses enkripsi AES-GCM



2	Implementasi Advanced Encryption Standard Pada Enkripsi Dan Dekripsi Dokumen Rahasia Diintelkam Polda DIY	Kelebihan dari penelitian ini berupa proses enkripsi dan dekripsi berjalan sesuai dengan fungsionalnya dan mengetahui jumlah waktu yang dihabis melakukan proses enkripsi.	Hanya menggunakan satu jenis algoritma kriptografi dalam proses penelitian tersebut	Dalam hal perbandingan metode dengan penelitian sebelumnya terletak pada jumlah algoritma yang digunakan dalam penelitian tersebut. Dalam penelitian yang dilakukan oleh penulis, penulis menggunakan dua algoritma dalam proses penelitian ini. Selain perbedaan jumlah algoritmanya, kunci yang digunakan dalam proses enkripsi akan menggunakan 2 kunci private dan akan menghasilkan 2 kunci tambahan dalam proses enkripsinya.
---	---	--	---	---

### 3.3 Penerapan metode

Pada penerapan metode penelitian ini, ada beberapa proses yang akan dilakukan oleh penulis. Proses penerapan metode penelitian ini menggunakan beberapa tahapan yang akan di lalui seperti:

#### 3.3.1 Pengumpulan Data

Dalam proses pengumpulan data ini, peneliti menggunakan sebuah metode kualitatif yang dimana proses pengumpulan data tersebut akan menggunakan tiga cara yaitu:

##### 1. Wawancara

Merupakan sebuah metode yang melakukan pengajuan sebuah pertanyaan kepada narasumber yang mengetahui sumber data yang di perlukan dalam penelitian.

##### 2. 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 mulia. Proses observasi dalam penelitian ini akan

melingkupi cara penyimpanan, keamanan dan hak akses terhadap dokumen yang berisikan data rekam medis dengan cara menggunakan algoritma AES-256 dan AES-GCM.

3. Studi Pustaka

Pada proses ini dilakukan dengan cara mencari informasi atau referensi dari jurnal online, kumpulan skripsi 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 medik supaya berkaitan dengan penelitian ini.

### 3.3.2 Analisis Kebutuhan

Ada beberapa proses yang akan dilakukan dalam analisis kebutuhan diantaranya:

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 implementasi ini akan dilaksanakan ketika 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.

### 3.3.3 Penerapan algoritma AES

1. Algoritma AES-256

Ada beberapa tahapan yang akan dilakukan penerapan algoritma AES-256 ini diantaranya:

a. Panjang Kunci

Dalam tahapan ini panjang kunci yang digunakan adalah 256-bit yang dimana akan menghasilkan 14 putaran dalam proses enkripsi dan deskripsi tersebut.

b. Proses Enkripsi

Dalam proses ini objek yang dijadikan target akan berubah menjadi sebuah plaintext dengan menggunakan panjang kunci sekitar 256-bit.

c. Proses Deskripsi

Dalam proses ini objek yang telah berubah menjadi plaintext akan diubah menjadi bentuk semulanya atau dikenal sebagai cipher text dengan menggunakan panjang kunci yaitu 256-bit.

2. Algoritma AES-GCM

Ada beberapa tahapan yang akan dilakukan penerapan algoritma AES-GCM ini diantaranya:

a. Panjang Kunci

Dalam proses ini akan menggunakan jumlah panjang kunci sekitar 256-bit seperti pada AES pada proses pertama.

b. Inisialisasi Vektor

Dalam proses ini panjang dari Inisialisasi Vektor (IV) ini disarankan menggunakan panjang sekitar 96bit atau 12 byte. IV merupakan sebuah nilai acak yang digunakan bersama dengan key dalam proses enkripsi dan deskripsi, selain sebagai nilai acak IV berfungsi sebagai pengecekan pesan yang sama dan kunci yang sama menghasilkan teks pesan yang berbeda sehingga tidak ada hasil yang sama jika isi pesan dan kunci yang sama digunakan dan memberikan keamanan yang lebih.

c. Autentikasi Tag

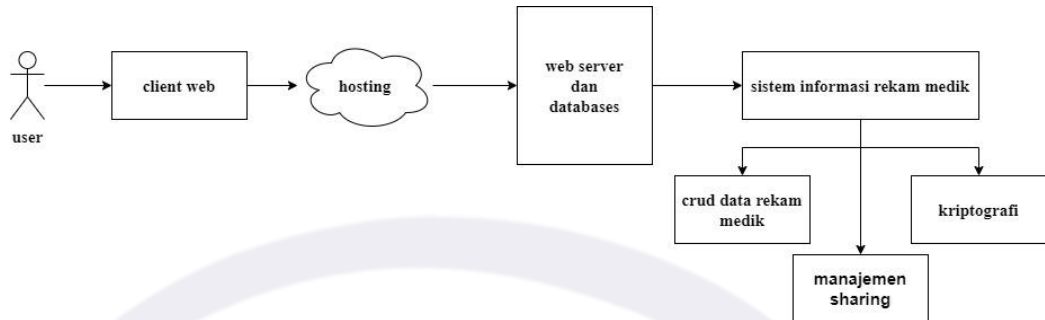
Dalam proses akan terjadi ketika proses enkripsi sudah dijalankan dan berhasil dalam proses enkripsi dan untuk memastikan keotentikan dan integritas pesan yang dienkripsi.

d. Enkripsi Dan Deskripsi

Dalam proses ini terdapat dua proses, pertama proses enkripsi yang dimana bertujuan untuk mengubah isi asli objek menjadi sebuah ciphertext dan proses kedua merupakan proses deskripsi yang dimana isi objek yang berubah menjadi ciphertext berubah menjadi bentuk isi aslinya atau menjadi plaintext.

### 3.4 Arsitektur Sistem

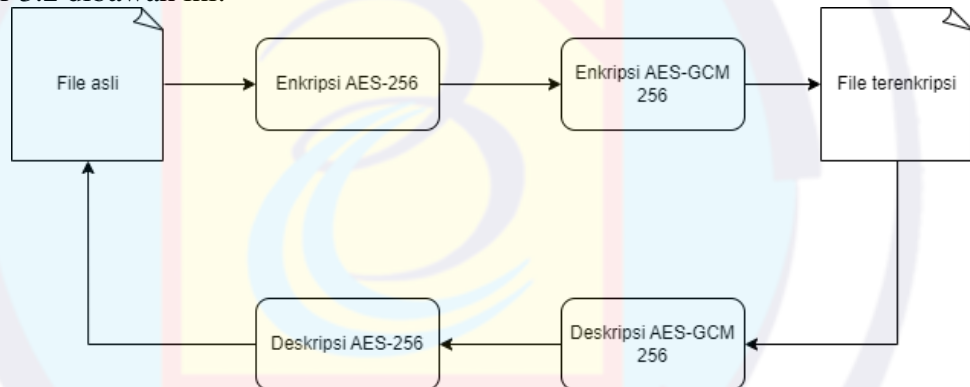
Arsitektur sistem merupakan sebuah skema atau gambaran proses kerja sebuah sistem. Arsitektur sistem dalam penelitian ini bisa dilihat di gambar 3.1 dibawah ini:



Gambar 3. 1 arsitektur sistem

### 3.5 Diagram Arsitektur Proses Enkripsi Dan Deskripsi

Pada proses diagram arsitektur proses enkripsi dan deskripsi pada penelitian ini, peneliti pada proses diagram ini akan menampilkan proses enkripsi dan deskripsi pada file. Pada diagram developer bisa dilihat dari gambar 3.2 dibawah ini:



Gambar 3. 2 Diagram arsitektur proses enkripsi dan deskripsi

### 3.6 Rancangan pengujian

Dalam proses rancangan pengujian ini, penelitian akan menggunakan sebuah metode *blackbox testing* dalam melakukan pengujiannya. Ada beberapa tahapan yang akan dilakukan dalam rancangan pengujian dalam penelitian ini yang akan dijabarkan dalam sebuah tabel 3.1 dibawah ini:

Tabel 3. 2 Rancangan pengujian

No	Pengujian	Hasil yang diinginkan
1	Login	Setelah berhasil melakukan login maka user bisa langsung masuk kedalam halaman dashboard
2	Manajemen user	Dalam tahapan ini admin bisa melakukan penambahan dan

		perubahan data user dalam semua jenis kategori user
3	Pemberian akses	Dalam tahapan ini ketika terjadinya permintaan oleh user lain untuk mendapatkan akses rekam medis maka admin akan memberikan akses rekam medis tersebut
4	Add dokumen rekam medis	Melakukan penambahan dokumen rekam medis kedalam sistem yang berbasis website dan terjadinya proses enkripsi pada dokumen tersebut
5	Upgrade dokumen rekam medis	Sebuah pembaharuan terhadap dokumen rekam medis yang berisikan sebuah hasil diagnosa terbaru dan proses terjadinya enkripsi pada dokumen rekam medis
6	Unduh dokumen rekam medis	Proses terjadinya deskripsi pada dokumen dan proses pengunduhan atau pengambilan salinan pada dokumen yang di simpan pada server
7	Fungsi enkripsi dokumen	Dokumen yang dimasukan ke dalam sistem terenkripsikan
8	Fungsi deskripsi dokumen	Dokumen yang dimasukan ke dalam sistem terdeskripsikan

### 3.7 Rancangan Basis data

#### 3.7.1 Spesifikasi Basis Data

Ada beberapa spesifikasi basis data yang akan digunakan dalam penelitian ini dan akan ditampilkan dengan sebuah tabel dibawah ini:

##### 1. Tabel user

Fungsi: untuk data login user

Primary key: id\_user

Spesifikasi basis data bisa dilihat di tabel 3.2 bawah ini:

**Tabel 3. 3 Tabel user**

No	Nama field	Tipe	Panjang
1	Id_user	Char	18
2	Username	Varchar	100
3	Password	Varchar	12
4	Last_login	Date	
5	Categori_user	Char	13

2. Tabel patient

Fungsi: data patient

Primary key: patientID

Foreign Key: useID, useAddID

Spesifikasi basis data bisa dilihat di tabel 3.3 bawah ini:

**Tabel 3. 4 Tabel pasien**

No	Nama field	Tipe	Panjang
1	patientID	Char	18
2	useID	Char	18
3	Datebirth	Date	
4	Nik	Int	20
5	No_bpjs	Int	20
6	Blood_type	Char	2
7	Phone number	Varchar	15
8	Address	Varchar	200
9	useAddID	Char	18
10	namePatient	varchar	100

3. Tabel medical record

Fungsi: penyimpanan data rekam medis

Primary key: RMID

Foreign Key: patientID dan userIdUP

Spesifikasi basis data bisa dilihat di tabel 3.4 bawah ini:

**Tabel 3. 5 Tabel rekam medis**

No	Nama field	Tipe	Panjang
1	RMID	Int	18
2	patientID	Char	18
3	userIdUP	Char	18
4	consultationDate	Date	
5	Consultation	Varchar	200
6	NameFile	Varchar	100



7	UploadDate	date	
8	consultationConten	varchar	200
9	Tag	varchar	200
10	Iv	varchar	200

4. Tabel access

Fungsi: untuk akses terkonfirmasi

Primary key: AccessID

Foreign Key: patientID dan id\_useAccessID

Spesifikasi basis data bisa dilihat di tabel 3.5 bawah ini:

**Tabel 3. 6 Tabel akses**

No	Nama field	Tipe	Panjang
1	AccessID	Int	18
2	UserAccessID	Char	18
3	patientID	Char	18
4	userCreatorID	Char	18
6	accessCreationDATE	Date	
7	checkupStartDate	Date	
8	ChekupEndDate	Date	
9	shareStartDate	Date	
10	ShareEndDate	Date	
11	nameUserAddAkses	varchar	100
12	nameShareto	varchar	100

### 3.7.2 Rancangan kode

Dalam rancangan kode ini membahas tentang untuk memberitaukan tentang kode jenis yang digunakan dalam tabel user yang berfungsi untuk membedakan kategori user dalam sistem yang berbentuk website ini. Rancangan kode ini bisa dilihat dari tabel 3.6 kategori user dibawah ini:

**Tabel 3. 7 Tabel kategori user**

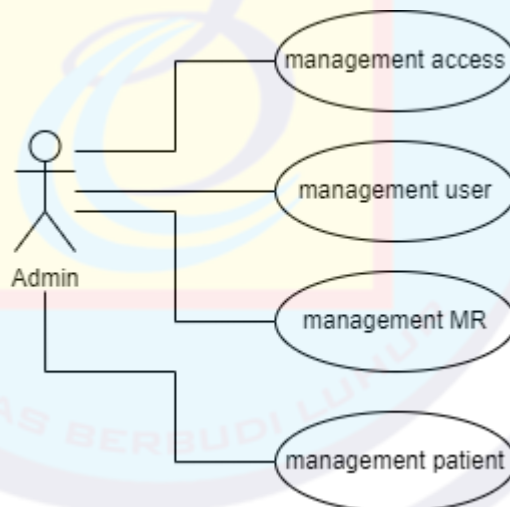
Kategori user	Bentuk awal id user
Admin	Ad
Nakes	Na
Dinkes	Di
Pasien	Pa

### 3.7.3 Use Case Diagram

Use case diagram merupakan sebuah gambaran interaksi antara satu aktor dengan aktor lain dalam sebuah sistem. Proses use case diagram dalam penelitian ini bisa dilihat dari gambar dibawah ini:

#### 1. Use case diagram admin

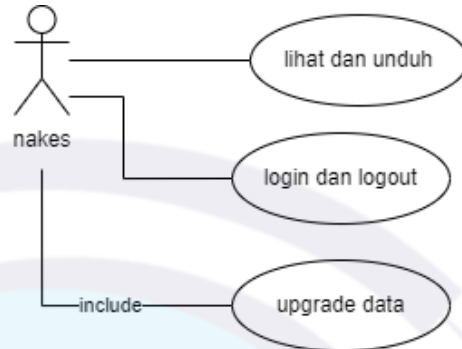
Admin berfungsi sebagai suatu user yang bisa melakukan manajemen user, manajemen medical record, manajemen patient dan manajemen akses. Gambar use case diagram untuk admin bisa dilihat di gambar 3.3 dibawah ini:



**Gambar 3. 3 Use case admin**

2. Use case diagram tenaga kesehatan

Tenaga kesehatan atau singkat nakes dalam sistem ini bisa melakukan update, melihat dan mengunduh medical record pasien. Gambar use case diagram untuk tenaga kesehatan bisa dilihat di gambar 3.4 dibawah ini:



Gambar 3. 4 Use case diagram nakes

3. Use case diagram external parties

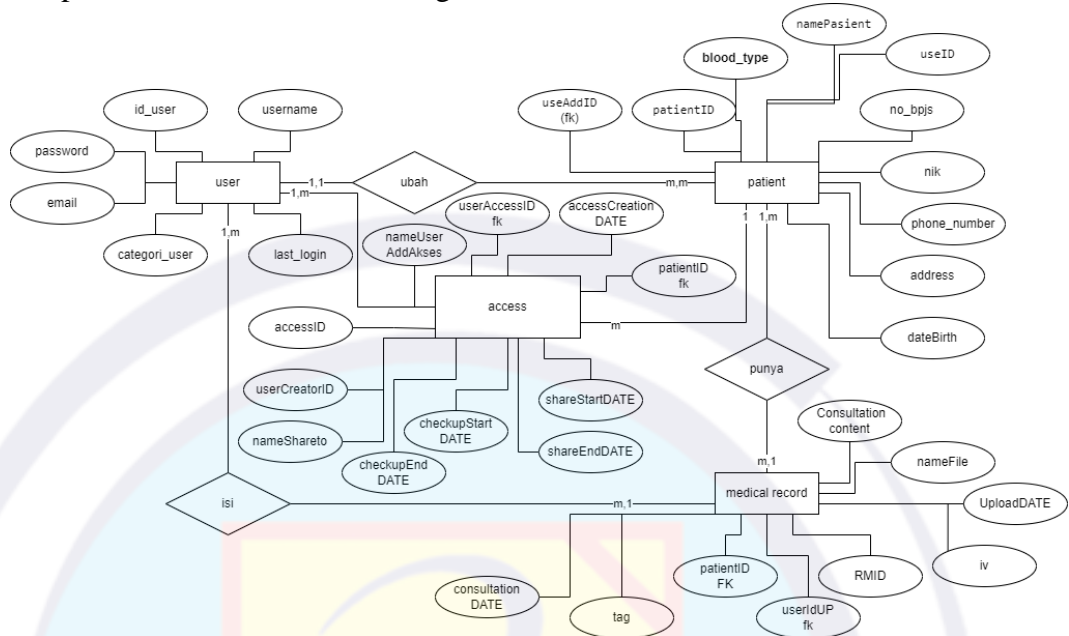
Pada user yang bersifat pihak luar (External parties) seperti dinas kesehatan atau disingkat dinkes dan pasien hanya bisa melakukan permintaan akses kepada admin, melihat dan mengunduh file rekam medis. Gambar use case diagram untuk pihak luar bisa dilihat di gambar 3.5 dibawah ini:



Gambar 3. 5 Use case diagram pihak luar

### 3.7.4 Entity Relationship Diagram (ERD)

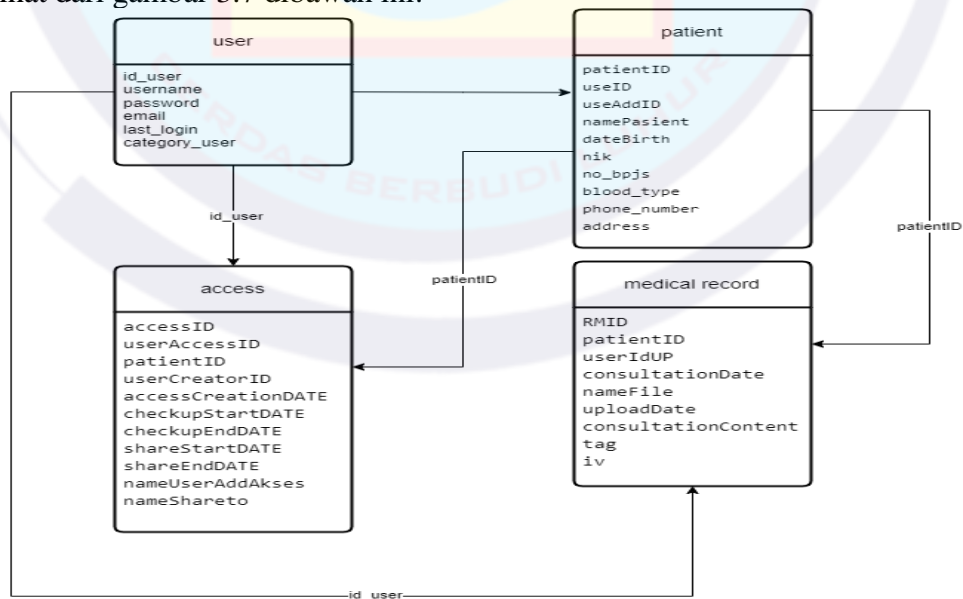
Entity relationship diagram atau disebut sebagai ERD berfungsi untuk menggambarkan hubungan antara entitas dan atribut dengan basis data. ERD dalam penelitian ini bisa dilihat dari gambar 3.6 dibawah ini:



Gambar 3. 6 Entity relationship diagram

### 3.7.5 Logical Record Structure (LRS)

Logical Record Structure atau disebut sebagai LRS, LRS memiliki sebuah fungsi untuk membantu mengatur dan menghubungkan data dalam basis data untuk pengelolaan yang optimal. LRS dalam penelitian ini bisa dilihat dari gambar 3.7 dibawah ini:



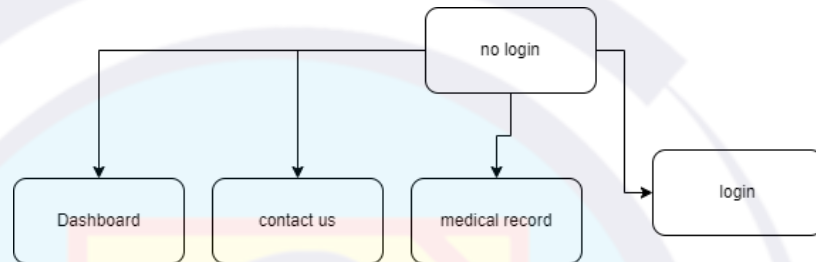
Gambar 3. 7 Logical record structure

### 3.8 Rancangan Menu

Rancangan menu akan dibagi menjadi 5 rancangan menu meliputi rancangan menu sebelum login, rancangan menu setelah login sebagai admin, rancangan menu setelah login sebagai nakes, rancangan menu setelah login sebagai pihak luar (external parties) dan rancangan menu setelah mendapat akses data rekam medis pasien. Rancangan menu pada website bisa dilihat dibawah ini:

1. Rancangan menu sebelum login

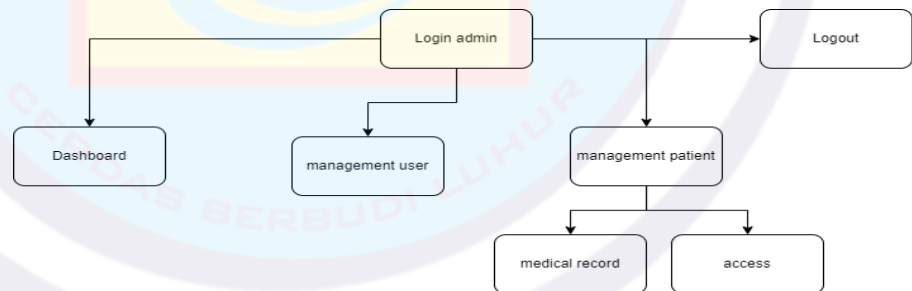
Dalam rancangan menu ini akan meliputi menu dashboard, contact, medical record dan login. Untuk gambar dalam proses rancangan menu ini bisa dilihat melalui gambar 3.8 dibawah ini:



Gambar 3. 8 Rancangan menu sebelum login

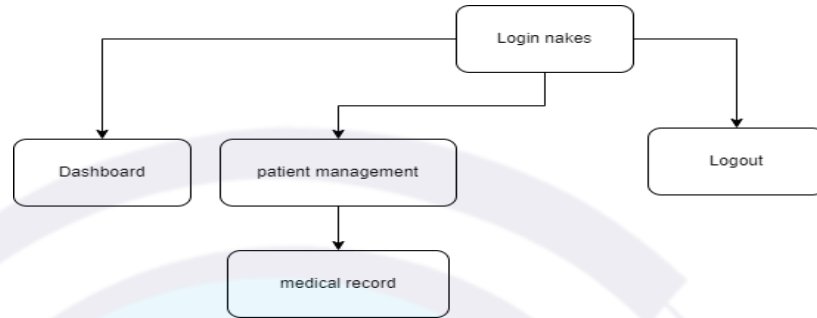
2. Rancangan menu setelah login sebagai admin

Dalam rancangan menu ini akan meliputi menu dashboard, management user, management patient dan logout. Untuk gambar dalam proses rancangan menu ini bisa dilihat melalui gambar 3.9 dibawah ini:



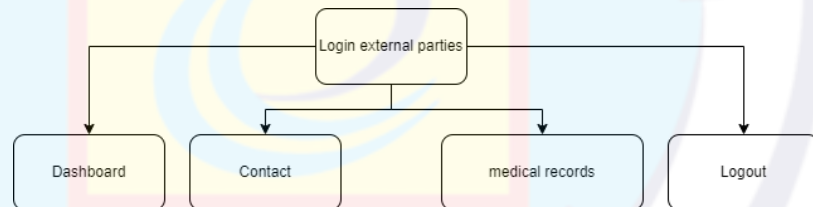
Gambar 3. 9 Rancangan menu setelah login sebagai admin

3. Rancangan menu setelah login sebagai nakes  
Dalam rancangan menu ini akan meliputi menu dashboard, management patient dan logout. Untuk gambar dalam proses rancangan menu ini bisa dilihat melalui gambar 3.10 dibawah ini:



**Gambar 3. 10 Rancangan menu setelah login sebagai nakes**

4. Rancangan menu setelah login sebagai pihak luar (external parties)  
Dalam rancangan menu ini akan meliputi menu dashboard, contact, medical record dan login. Untuk gambar dalam proses rancangan menu ini bisa dilihat melalui gambar 3.11 dibawah ini:



**Gambar 3. 11 Rancangan menu setelah login sebagai pihak luar**



### 3.9 Rancangan Layar

Dalam proses rancangan layar ini akan menggambarkan sketsa bentuk fisik dari sebuah sistem yang berbasis website yang akan digunakan dalam penelitian ini. Dalam rancangan layar ini ada beberapa bagian yang akan dibedakan berdasarkan jenis kategori user dan dua rancangan layar untuk proses masuk dan pendaftaran user. Rancangan layar ini bisa dilihat dibawah ini.

#### 3.9.1 Racangan halaman awal

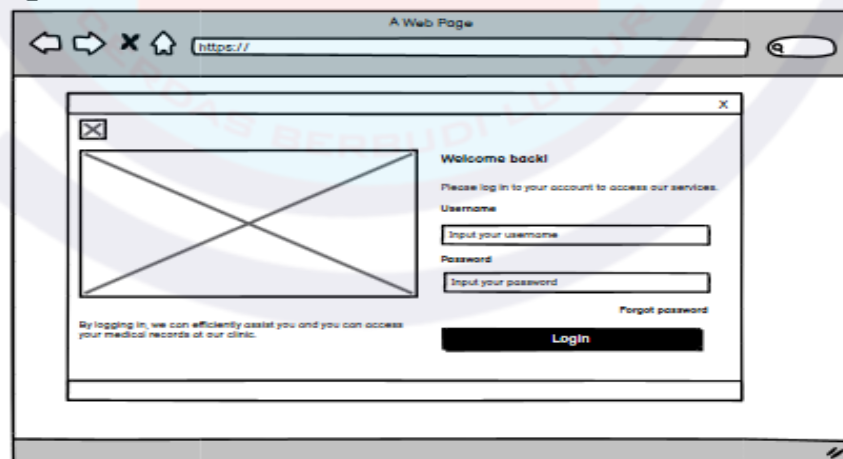
Pada racangan halaman menu awal bisa dilihat dari gambar 3.12 dibawah ini:



Gambar 3. 12 Rancangan tampilan awal

#### 3.9.2 Rancangan layar login

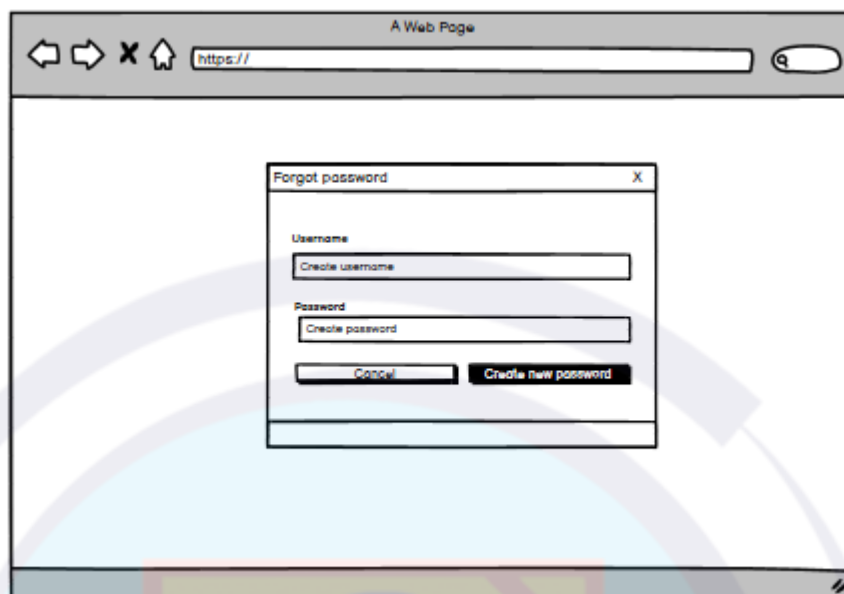
Proses rancangan layar login bisa dilihat pada gambar 3.13 dibawah ini:



Gambar 3. 13 Rancangan layar login

### 3.9.3 Rancangan layar forgot password

Pada proses forgot password bisa dilihat dari gambar 3.14 dibawah ini:

A screenshot of a web browser window titled 'A Web Page'. The address bar shows 'https://'. A modal dialog box titled 'Forgot password' is centered on the screen. It contains two input fields: 'Username' with a placeholder 'Create username' and 'Password' with a placeholder 'Create password'. Below these fields are two buttons: 'Cancel' and 'Create new password'.

Gambar 3. 14 Rancangan layar forgot password

### 3.9.4 Rancangan layar Admin dashboard

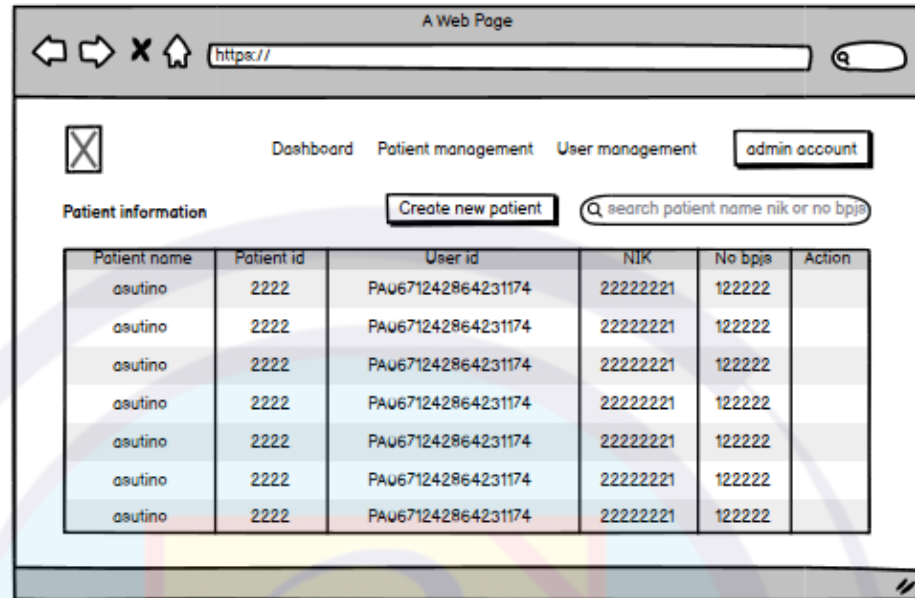
Pada rancangan layar admin dashboard bisa dilihat pada gambar 3.15 dibawah ini:

A screenshot of a web browser window titled 'A Web Page'. The address bar shows 'https://'. The dashboard layout includes a top navigation bar with a logo (a square with an 'X'), and links for 'Dashboard', 'Patient management', 'User management', and 'admin account'. The main content area features a section titled 'Medical Records' with the text 'We provide the fastest and safest route to your health information through medical records data.' To the right of this text is a large rectangular placeholder with a diagonal 'X' across it.

Gambar 3. 15 Rancangan layar admin dashboard

### 3.9.5 Rancangan layar admin pada menu patient management

Pada rancangan layar admin menu patient management bisa dilihat dari gambar 3.16 dibawah ini:



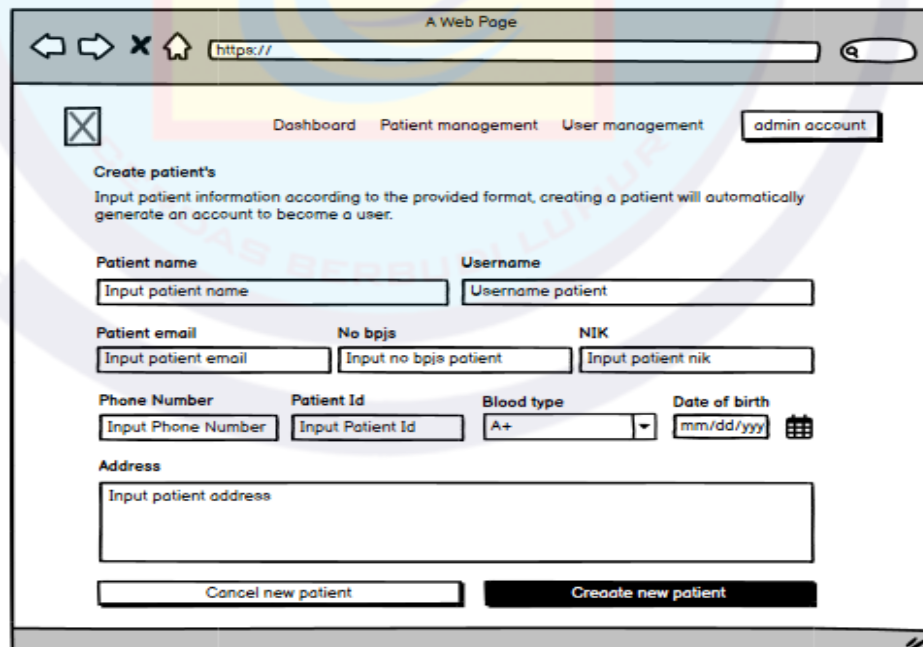
The screenshot shows a web browser window titled "A Web Page" with a URL bar containing "https://". The page has a navigation bar with links for "Dashboard", "Patient management", and "User management", along with a button for "admin account". Below the navigation bar, there is a "Patient information" section with a "Create new patient" button and a search bar labeled "search patient name nik or no bpjs". The main content area displays a table with patient data.

Patient name	Patient id	User id	NIK	No bpjs	Action
asutino	2222	PAU671242864231174	22222221	122222	
asutino	2222	PAU671242864231174	22222221	122222	
asutino	2222	PAU671242864231174	22222221	122222	
asutino	2222	PAU671242864231174	22222221	122222	
asutino	2222	PAU671242864231174	22222221	122222	
asutino	2222	PAU671242864231174	22222221	122222	
asutino	2222	PAU671242864231174	22222221	122222	

Gambar 3. 16 Rancangan layar admin pada menu patient management

### 3.9.6 Rancangan layar menu create patient pada admin

Pada rancangan layar admin menu create patient bisa dilihat dari gambar dibawah ini:

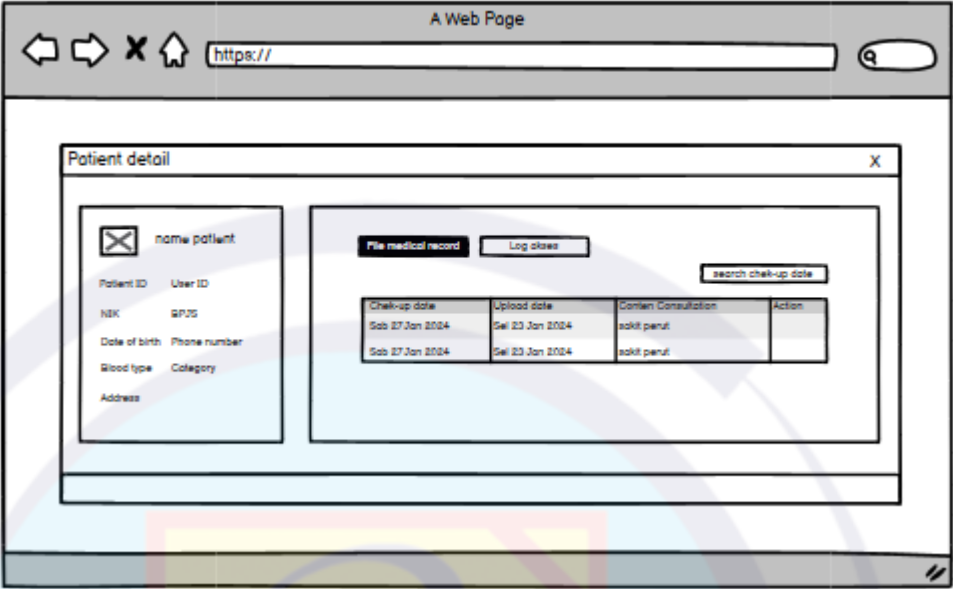


The screenshot shows a web browser window titled "A Web Page" with a URL bar containing "https://". The page has a navigation bar with links for "Dashboard", "Patient management", and "User management", along with a button for "admin account". Below the navigation bar, there is a "Create patient's" section with instructions: "Input patient information according to the provided format, creating a patient will automatically generate an account to become a user." The form contains several input fields: "Patient name" (with a sub-label "Username" and "Username patient"), "Patient email", "No bpjs" (with a sub-label "Input no bpjs patient"), "NIK" (with a sub-label "Input patient nik"), "Phone Number" (with a sub-label "Input Phone Number"), "Patient Id" (with a sub-label "Input Patient Id"), "Blood type" (with a dropdown menu showing "A+" and a sub-label "mm/dd/yyyy"), and "Date of birth" (with a calendar icon). There is also a large "Address" input field. At the bottom, there are two buttons: "Cancel new patient" and "Create new patient".

Gambar 3. 17 Rancangan layar menu create patient pada admin

3.9.7 Rancangan layar menu detail pasien pada admin

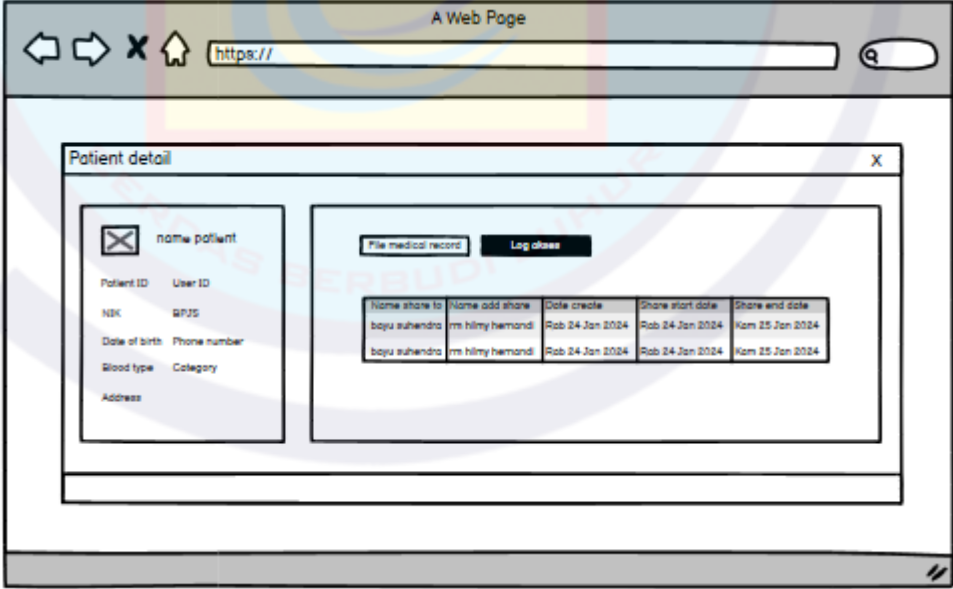
Pada rancangan layar admin menu detail patient bisa dilihat dari gambar 3.18 dibawah ini:



Gambar 3. 18 Rancangan layar menu detail pasien pada admin

3.9.8 Rancangan layar menu log akses pada admin

Pada rancangan layar admin menu log akses bisa dilihat dari gambar 3.19 dibawah ini:



Gambar 3. 19 Rancangan layar menu log akses pada admin

### 3.9.9 Rancangan layar menu medical pada admin dan nakes

Pada rancangan layar admin dan nakes menu medical bisa dilihat dari gambar 3.20 dibawah ini:

The screenshot shows a web browser window titled 'A Web Page' with a URL bar containing 'https://'. The main content area displays a form titled 'Medical record upload' with a close button (X) in the top right corner. The form is divided into two main sections. The left section contains an 'Upload file' button with a document icon, followed by input fields for 'Patient ID' and 'Administrator ID'. Below these are date pickers for 'Consultation date' and 'Upload date', both showing the format 'mm/dd/yyyy'. The right section is a large text area labeled 'Input the results of the patient consultation'. At the bottom of the form are two buttons: 'Cancel upload' and 'Upload'.

Gambar 3. 20 Rancangan layar menu medical pada admin dan nakes

### 3.9.10 Rancangan layar menu akses pada admin

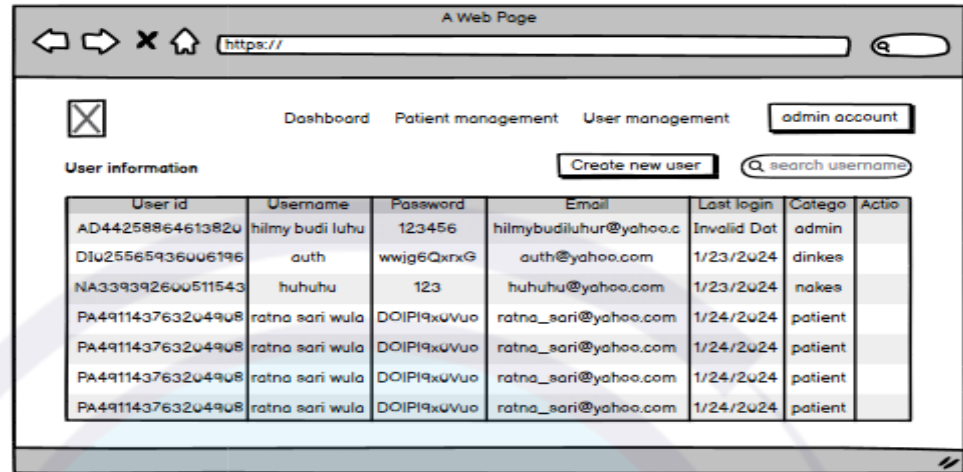
Pada rancangan layar admin menu akses bisa dilihat dari gambar 3.21 dibawah ini:

The screenshot shows a web browser window titled 'A Web Page' with a URL bar containing 'https://'. The main content area displays a form titled 'Medical record access' with a close button (X) in the top right corner. The form is divided into two main sections. The left section, titled 'Document collection', contains a table with two columns: 'Check-up date' and 'Upinad Date'. Both columns have two rows of data, each showing 'Rob 24 Jan 2424'. The right section, titled 'From creating new access', contains a sub-header and a paragraph: 'If you want to create access, please select or click on the combo box in the field and fill in the form above.' Below this are input fields for 'Patient ID' (with a dropdown menu showing 'Auto') and 'Share access to' (with a dropdown menu showing 'Enter username external or patie'). There are also date pickers for 'Check-up start date', 'Check-up end date', 'Access create date', 'Share start date', and 'Share end date', all showing the format 'mm /dd /yyyy'. At the bottom of the form are two buttons: 'Cancel upload' and 'Upload'.

Gambar 3. 21 Rancangan layar menu akses pada admin

### 3.9.11 Rancangan layar menu user managment admin

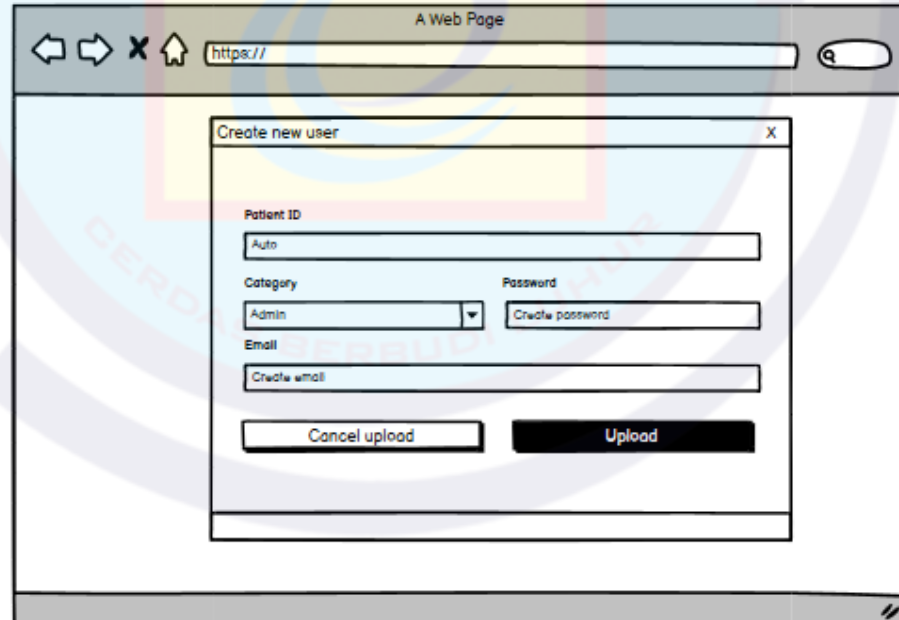
Pada rancangan layar menu user managment pada admin bisa dilihat dari gambar 3.22 dibawah ini:



Gambar 3. 22 Rancangan layar menu user managment admin

### 3.9.12 Rancangan layar menu create user admin

Pada rancangan layar menu create user pada admin bisa dilihat dari gambar 3.23 dibawah ini:




Gambar 3. 23 Rancangan layar menu create user admin



### 3.9.13 Rancangan layar menu edit user pada admin

Pada rancangan layar menu edit user pada admin bisa dilihat dari gambar 3.24 dibawah ini:



The image shows a web browser window titled 'A Web Page' with a URL bar containing 'https://'. Inside the browser, there is a form titled 'Edit user' with a close button 'X' in the top right corner. The form contains four input fields: 'User id' with the value 'Auto', 'Username' with the placeholder 'Create username', 'Email' with the placeholder 'Create email', and 'Password' with the placeholder 'Create password'. At the bottom of the form, there are two buttons: 'Cancel upload' and 'Upload'.

Gambar 3. 24 Rancangan layar menu edit user pada admin

### 3.9.14 Rancangan layar menu dashboard pada nakes

Pada rancangan layar menu dashboard pada nakes bisa dilihat dari gambar 3.25 dibawah ini:



The image shows a web browser window titled 'A Web Page' with a URL bar containing 'https://'. Inside the browser, there is a dashboard for 'Medical Records'. At the top, there are three tabs: 'Dashboard' (selected), 'Patient management', and 'Nakes account'. Below the tabs, there is a large heading 'Medical Records' and a subheading 'We provide the fastest and safest route to your health information through medical records data.' To the right of the text, there is a large empty box with a diagonal cross, indicating a missing image or a placeholder for a chart.

Gambar 3. 25 Rancangan layar menu dashboard pada nakes

### 3.9.15 Rancangan layar menu dashboard pada pasien dan dinkes

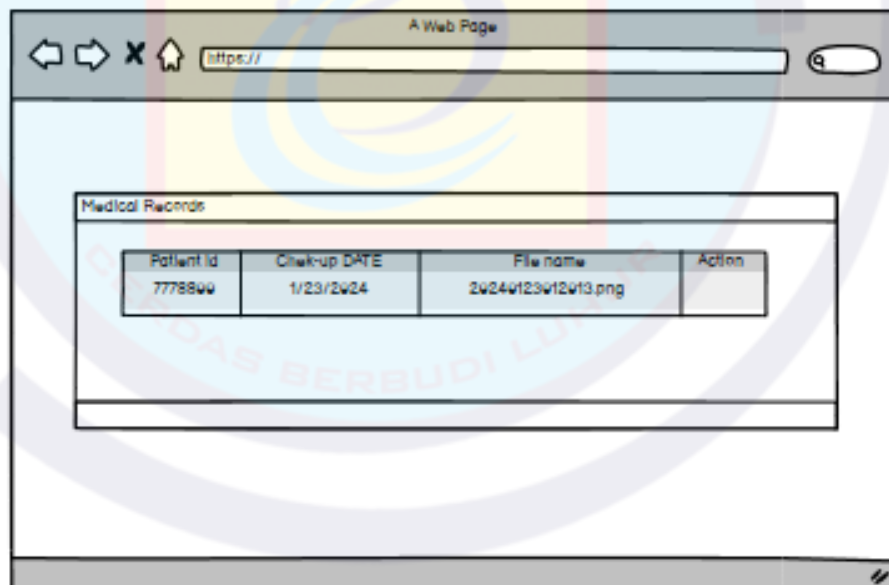
Pada rancangan layar menu dashboard pada pasien pada pihak luar atau dinkes bisa dilihat dari gambar 3.26 dibawah ini:



Gambar 3. 26 Rancangan layar menu dashboard pada pasien dan pihak luar

### 3.9.16 Rancangan layar menu medical record pada pasien dan dinkes

Pada rancangan layar menu medical record pada pasien pada pihak luar bisa atau dinkes dilihat dari gambar 3.27 dibawah ini:



Gambar 3. 27 Rancangan layar menu medical record pada pasien dan dinkes

## **BAB IV HASIL DAN PEMBAHASAN**

### **4. 1 Lingkungan Percobaan**

Pada lingkungan percobaan ini, perangkat keras dan perangkat lunak yang digunakan pada penelitian ini sebagai pendukung dalam proses perancangan aplikasi yang menghasilkan sebuah website dan proses penelitian ini. Dalam lingkungan percobaan ini, peneliti menggunakan beberapa perangkat keras dan lunak yang akan di jabarkan dibawah ini:

#### **4.1.1 Spesifikasi Perangkat Keras**

Dibawah ini peneliti akan memberikan menjabarkan spesifikasi perangkat keras yang peneliti digunakan dalam proses peneltian ini:

- a. Prosesor yang digunakan Intel(R) Core(TM) i5-4300M CPU @ 2.60GHz 2.59 GHz
- b. Kapasitas RAM 8gb
- c. Hardisk 500gb dan ssd 250gb

#### **4.1.2 Spesifikasi Perangkat Lunak**

Dibawah ini peneliti akan memberikan menjabarkan spesifikasi perangkat lunak yang peneliti digunakan dalam proses peneltian ini:

- a. Visual studio code
- b. Mysql di xampp
- c. Node.js sebagai localhost
- d. Google chrome dan firefox

### **4. 2 Implementasi Metode**

Dalam proses implentasi metode ini peneliti menggunakan sebuah algoritma AES dengan panjang kunci 256 tanpa mode dan algoritma AES dengan mode GCM dengan panjang kunci 256 yang telah di cantumkan pada bab sebelumnya. Dalam implementasi metode yang di gunakan oleh peneliti akan di jelaskan dibawah ini:

- a. Proses enkripsi AES dan enkripsi AES-GCM

Dalam proses enkripsi pada sebuah file rekam medis pasien seorang admin atau pun dokter harus masuk ke halaman patient management setelah itu akan tampil halaman tersebut lalu masuk ke halaman medical untuk menambahkan file rekam medis milik pasien. Dalam proses menambahkan file tersebut proses enkripsi akan berjalan. Proses enkripsi pertama kali akan menggunakan algoritma AES dengan panjang kunci 256 tanpa mode setelah itu akan di lanjutkan menggunakan algoritma AES dengan metode GCM menggunakan panjang kunci 256. Proses penambahan file rekam medis bisa dilihat dari gambar.

b. Proses deskripsi AES-GCM dan AES

Dalam proses deskripsi ini merupakan proses yang berlawanan dengan enkripsi dikarenakan algoritma terakhir yang digunakan dalam proses terjadinya enkripsi pada sistem yang dimana AES-GCM adalah algoritma terakhir sehingga proses deskripsinya akan di mulai dengan algoritma AES-GCM lalu algoritma AES. Proses deskripsi terjadi ketika pasien dan dinas kesehatan mengklik tombol medical record lalu tampil sebuah popup yang berisikan rekam medis pasien berupa file dan proses dekripsi akan berjalan ketika pasien dan dinas kesehatan mengklik tombol unduh pada proses ini dapat dilihat pada gambar. Untuk admin dan dokter atau tenaga kesehatan untuk terjadi deskripsi itu ketika memasuki halaman patient management lalu mengklik button detail pada tabel yang berisikan informasi pasien. setelah masuk ke halaman detail di sana terdapat sebuah informasi pasien berupa biodata, kumpulan file rekam medis dan log akses. Untuk bisa melakukan deskripsi admin dan dokter atau tenaga kesehatan harus mengklik unduh pada tabel rekam medis yang bisa dilihat pada gambar.

c. Request library

Dalam proses pembuatan sistem yang berbasis website ini, peneliti menggunakan sebuah library yang berfungsi untuk melakukan proses enkripsi dan deskripsi. Library yang peneliti gunakan ini bernama crypto.

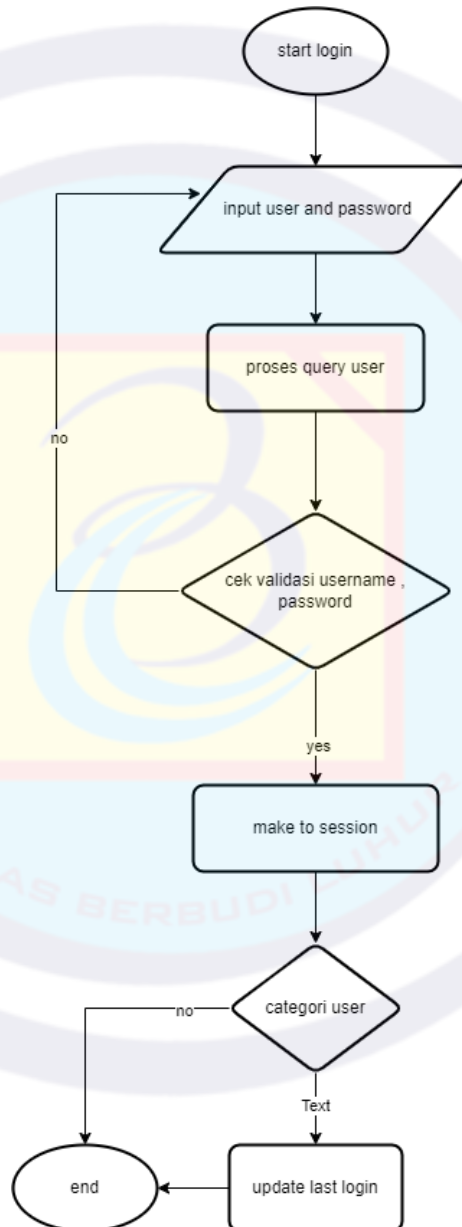
Library crypto ini termasuk kedalam sebuah library yang open source yang bisa digunakan pada bahasa pemrograman JS dengan bantuan node.js sebagai alat instalasi.

### 4.3 Flowchart

Pada pembangunan sistem ini flowchart berfungsi sebagai alat untuk menjelaskan proses pada setiap fitur yang terdapat pada sistem yang berbentuk website ini.

#### 4.3.1 Flowchart login

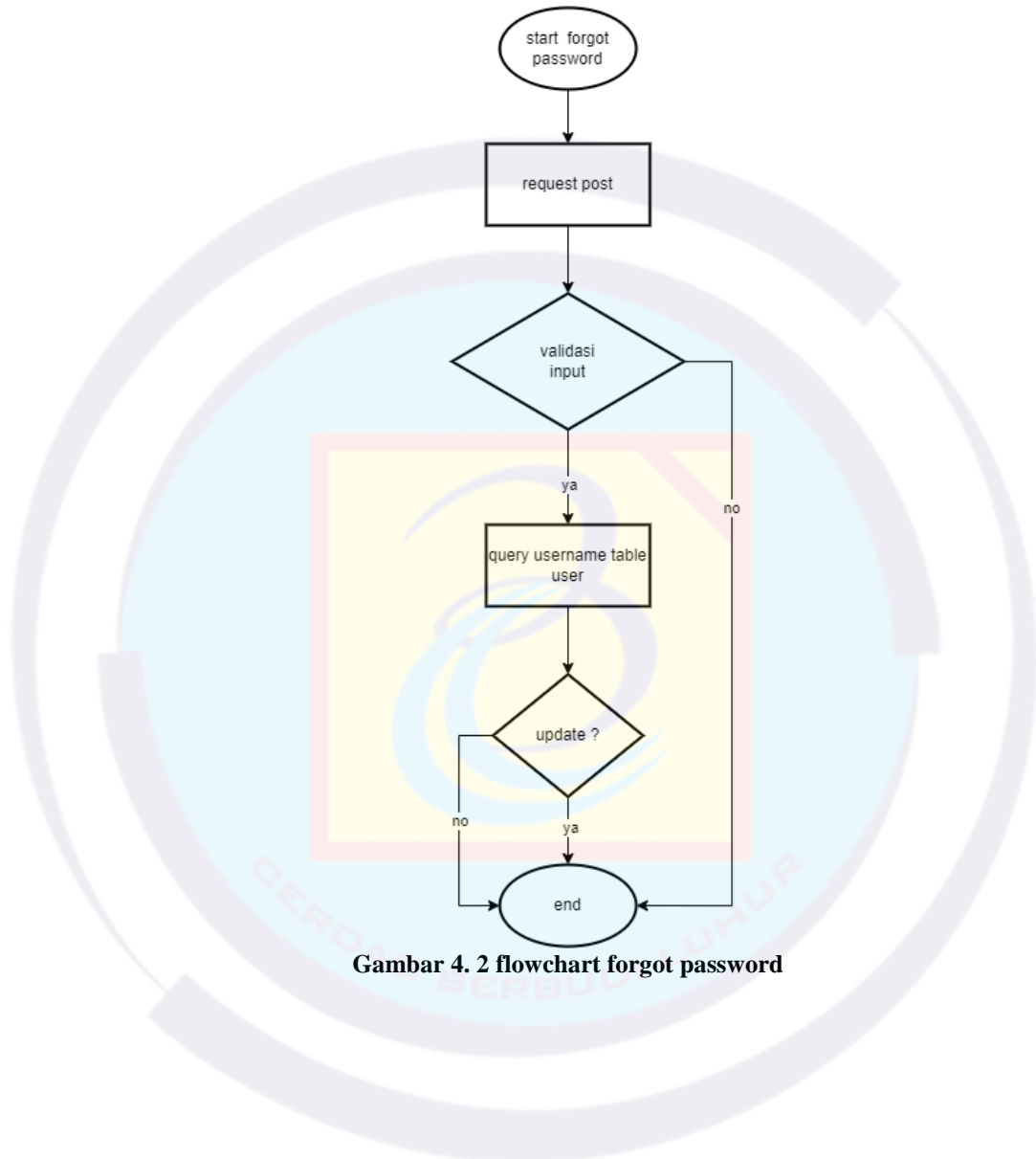
Pada proses login ini, user harus memasukkan username dan password supaya sistem bisa mengetahui jenis user berdasarkan kategori user. Dalam proses login ini bisa dilihat pada gambar 4.1 dibawah ini:



Gambar 4. 1 flowchart login

#### 4.3.2 Flowchart forgot password

Pada proses forgot password terjadi ketika user lupa dengan password yang dimiliki sebelumnya. Dalam proses ini user hanya memasuki username dan password terbarunya. Proses ini bisa dilihat dari gambar 4.2 dibawah ini:

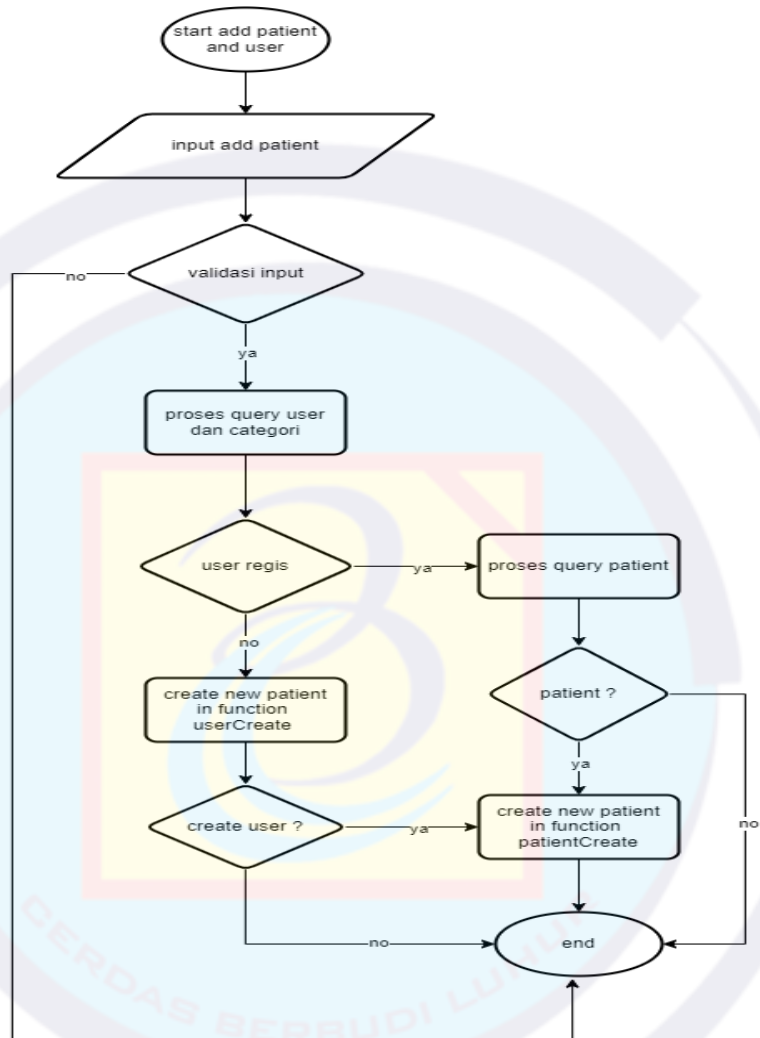


Gambar 4. 2 flowchart forgot password



#### 4.3.3 Flowchart add pasien dan add user

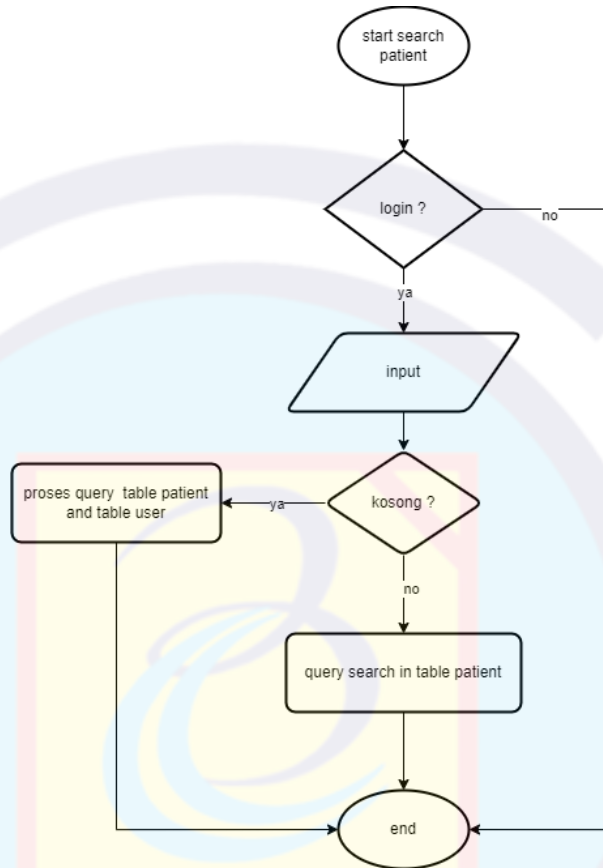
Pada proses add pasien dan add user ini hanya berfungsi pada user berkategori sebagai admin. Dalam proses ini hanya memasukan informasi biodata patient berserta nomer rekam medis patient. Proses add pasien dan add user bisa dilihat melalui gambar 4.3 dibawah ini:



Gambar 4. 3 Flowchart add pasien dan add user

#### 4.3.4 Flowchart search pasien

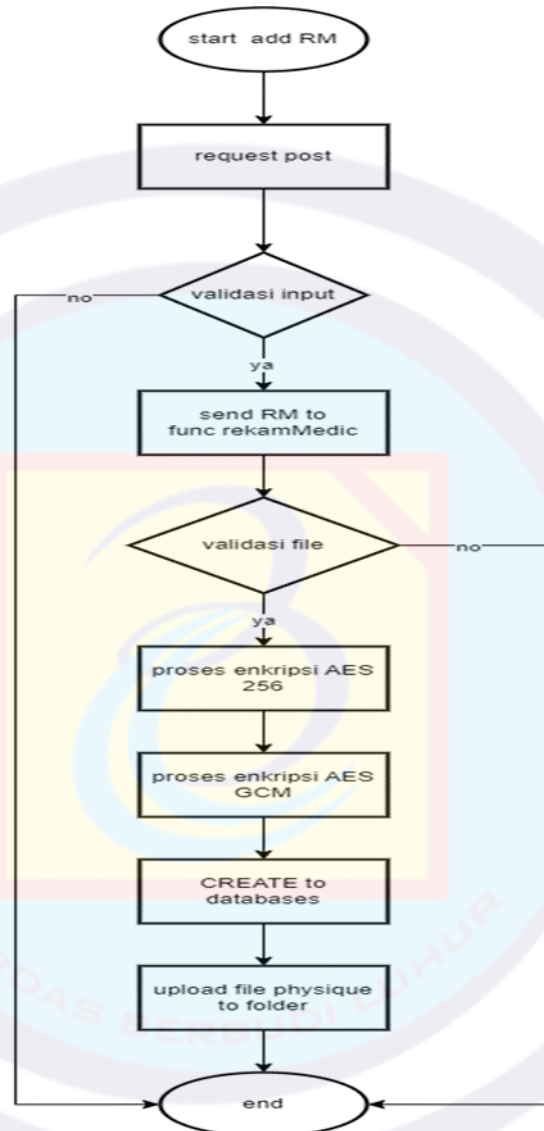
Dalam proses search pasien hanya bisa dilakukan oleh admin dan dokter atau tenaga kesehatan untuk mencari nama pasien di halaman patient management. Prosesnya search pasien bisa dilihat pada gambar 4.4 dibawah ini:



Gambar 4. 4 Flowchart search pasien

#### 4.3.5 Flowchart add rekam medis

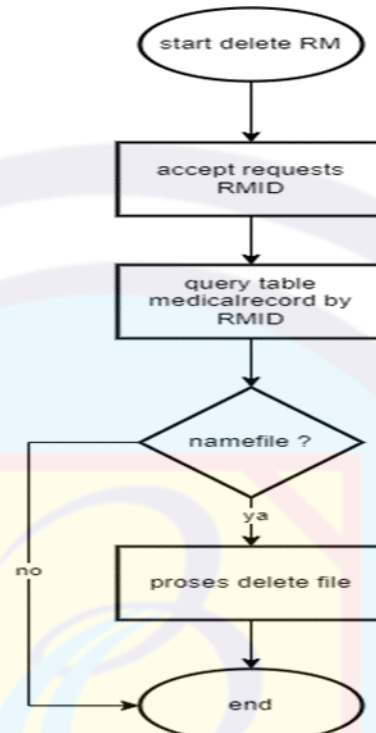
Pada proses add rekam medis pasien ini hanya bisa dilakukan oleh admin dan dokter atau tenaga kesehatan. Dalam proses ini akan terjadi proses enkripsi pada file yang diawali dengan algoritma AES dan AES-GCM. proses tersebut bisa dilihat dari gambar 4.5 dibawah ini:



Gambar 4. 5 Flowchart add rekam medis

#### 4.3.6 Flowchart delete rekam medis

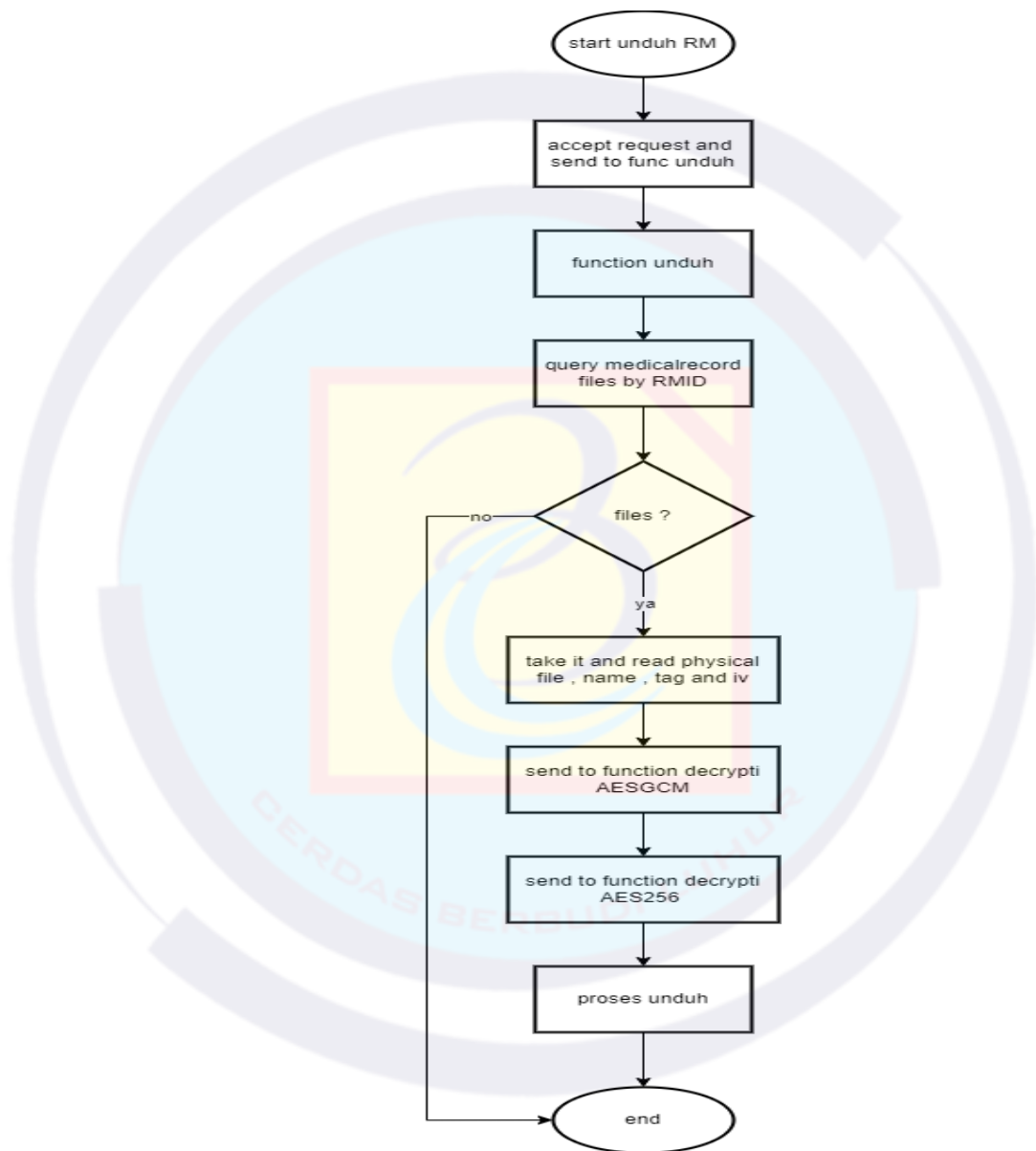
Pada proses delete rekam medis hanya bisa dilakukan oleh admin dan dokter atau tenaga kesehatan dengan melakukan mengklik button berlogo tempat sampah di halaman detail. Proses delete rekam medis tersebut dapat dilihat dari gambar 4.6 dibawah ini:



**Gambar 4. 6 Flowchart delete rekam medis**

#### 4.3.7 Flowchart unduh file rekam medis

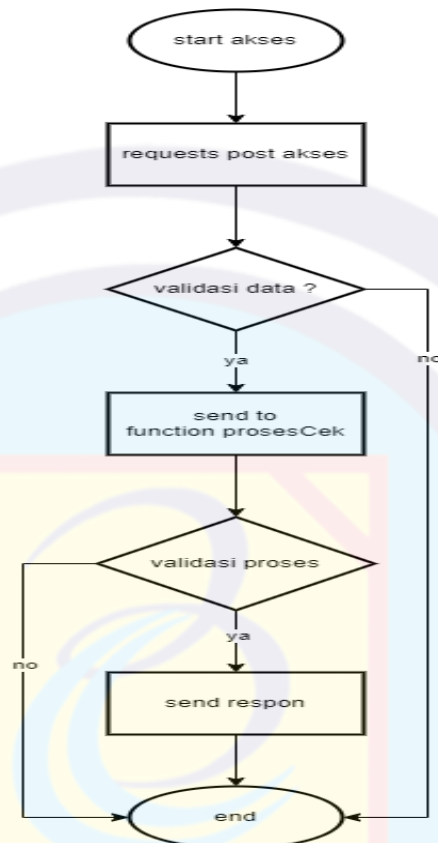
Proses unduh file rekam medis bisa dilakukan oleh admin, dokter atau tenaga kesehatan, pasien dan dinas kesehatan. Untuk pasien dan dinas kesehatan hanya bisa mengunduh file rekam medis tersebut ketika telah diberikan akses oleh admin. Dalam proses unduh tersebut akan terjadi proses dekripsi yang mana akan di awalin oleh algoritma AES-GCM lalu algoritma AES. Proses unduh bisa dilihat pada gambar 4.7 di bawah ini:



Gambar 4. 7 Flowchart unduh file rekam medis

#### 4.3.8 Flowchart add akses rekem medis

Pada proses add akses rekam medis ini hanya bisa dilakukan oleh admin kepada pasien atau dinas kesehatan jika mereka meminta data dengan batas tanggal tertentu. Proses add akses tersebut dapat dilihat dari gambar 4.8 dibawah ini:

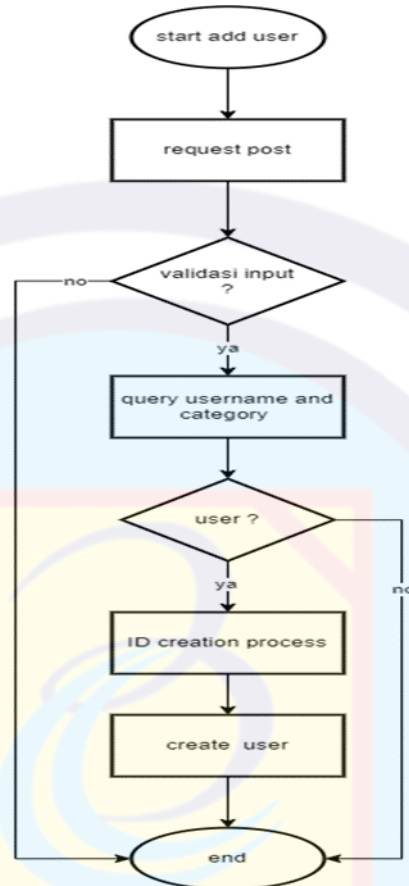


Gambar 4. 8 Flowchart add akses rekem medis



#### 4.3.9 Flowchart add user

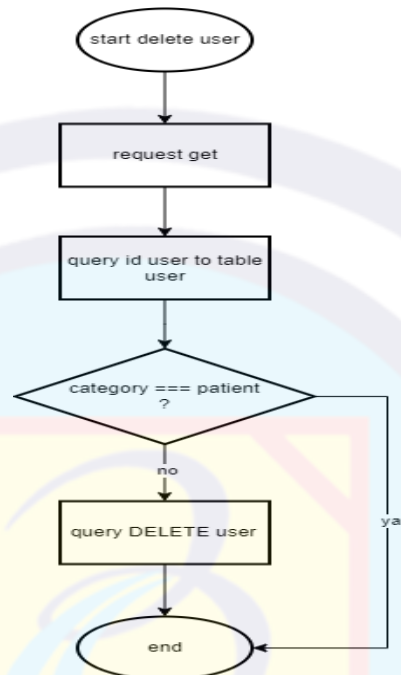
Pada proses add user ini hanya bisa dilakukan oleh admin pada halaman user management yang dimana akan memasukan biodata singkat milik pasien. Proses add user bisa dilihat dari gambar 4.9 dibawah ini:



Gambar 4. 9 Flowchart add user

#### 4.3.10 Flowchart delete user

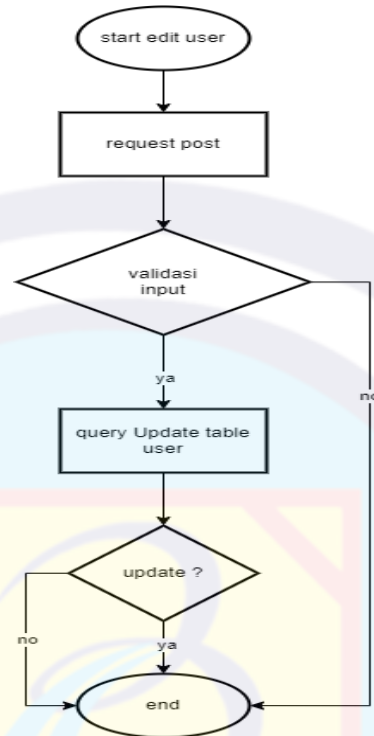
Pada proses delete user ini hanya bisa dilakukan oleh admin pada halaman user management yang dimana prosesnya hanya mengklik tombol dengan ikon tempat sampah, tetapi hanya selain user yang berkategori sebagai patient tidak akan bisa dihapus karena terikat oleh rekam medis itu sendiri. Proses delete user bisa dilihat dari gambar 4.10 dibawah ini:



Gambar 4. 10 Flowchart delete user

#### 4.3.11 Flowchart edit user

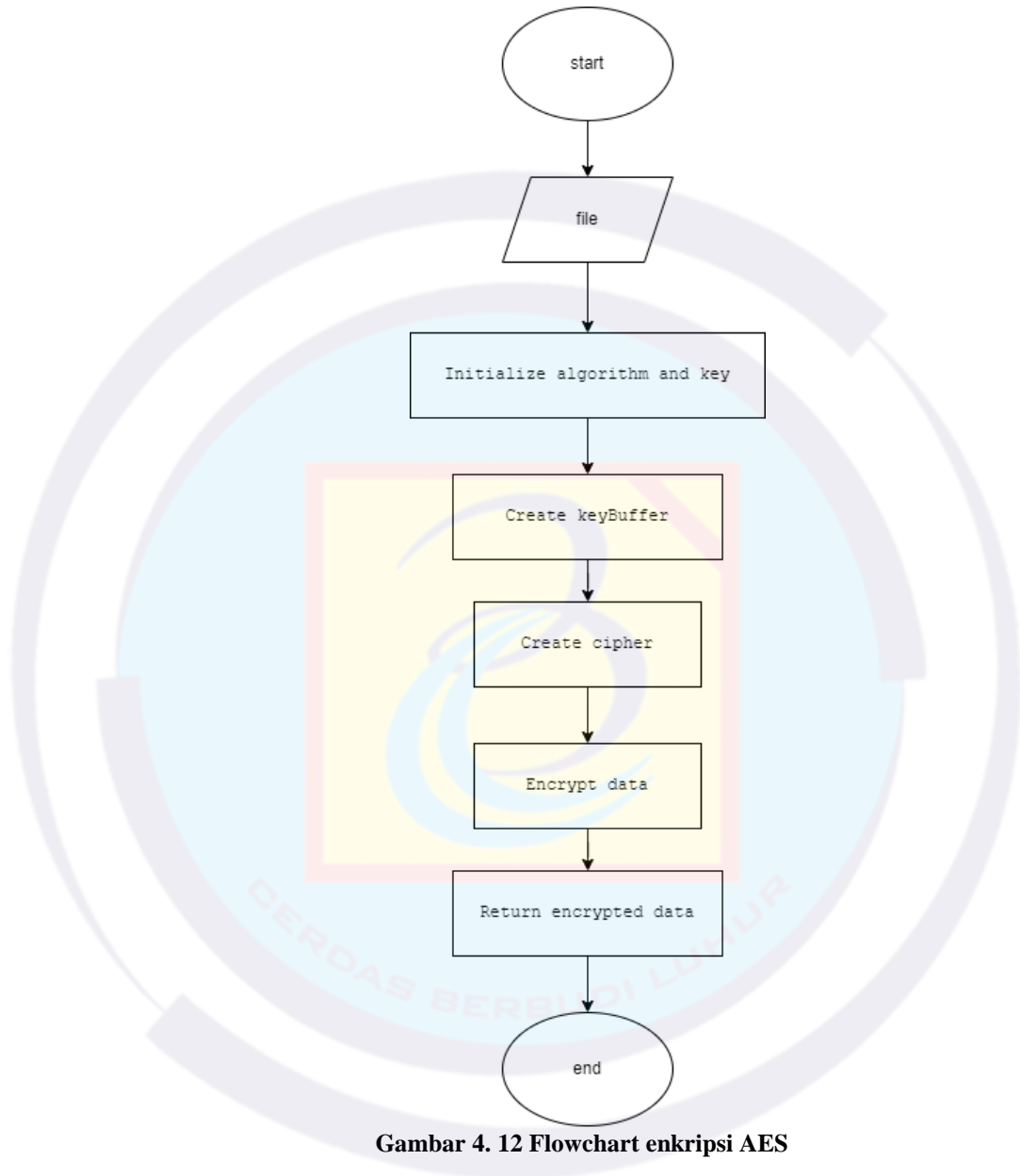
Pada proses edit user hanya bisa dilakukan oleh admin pada halaman user management yang dimana prosesnya hanya mengubah username, password dan email. Proses ini bisa dilihat melalui gambar 4.11 dibawah ini:



Gambar 4. 11 Flowchart edit user

#### 4.3.12 Flowchart enkripsi AES

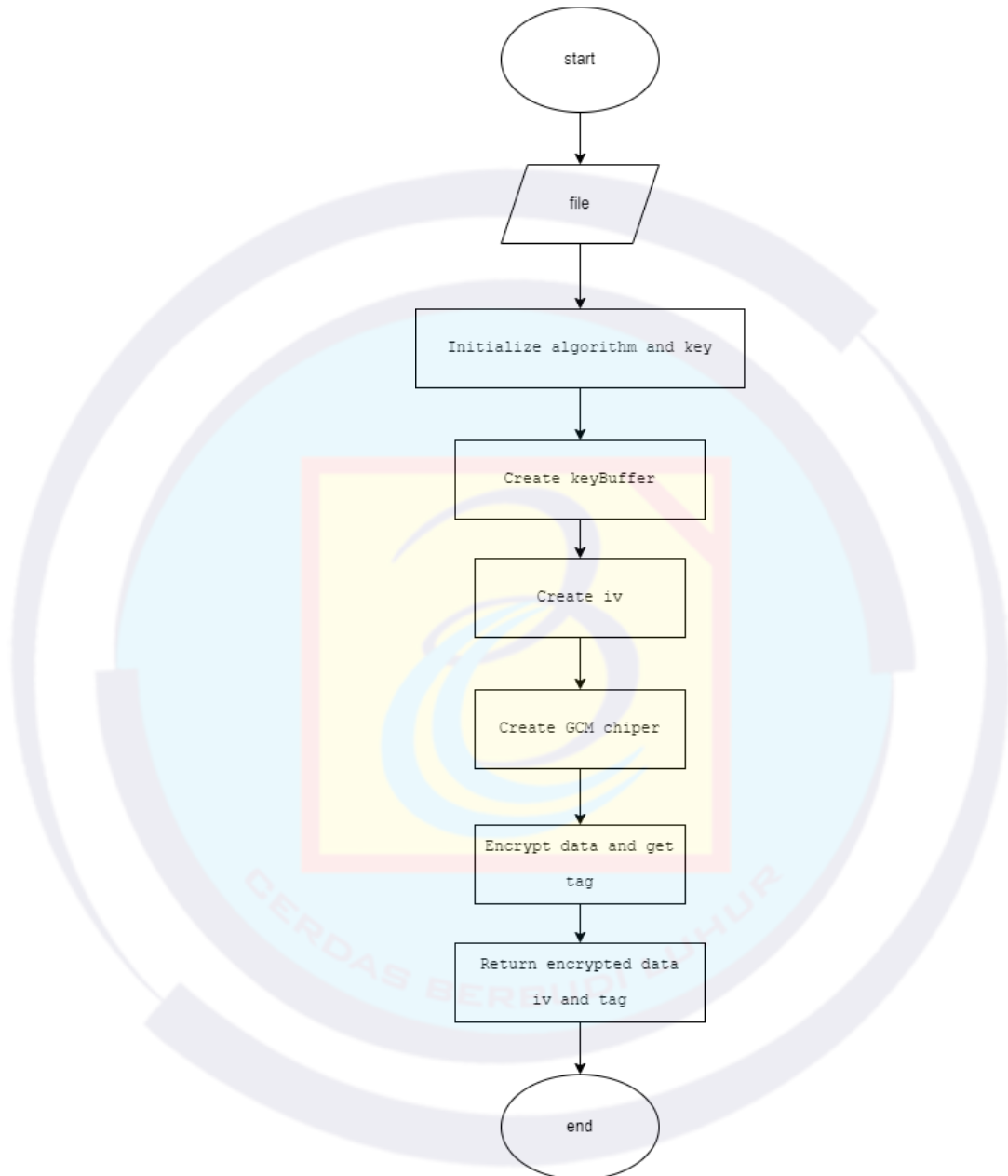
Pada proses enkripsi AES-256 pada penelitian ini, peneliti menggunakan sebuah library dari node.js yang bernama crypto. Tahap – tahapan enkripsi AES-256 bisa dilihat melalui gambar 4.12 dibawah ini:



Gambar 4. 12 Flowchart enkripsi AES

#### 4.3.13 Flowchart enkripsi AES-GCM

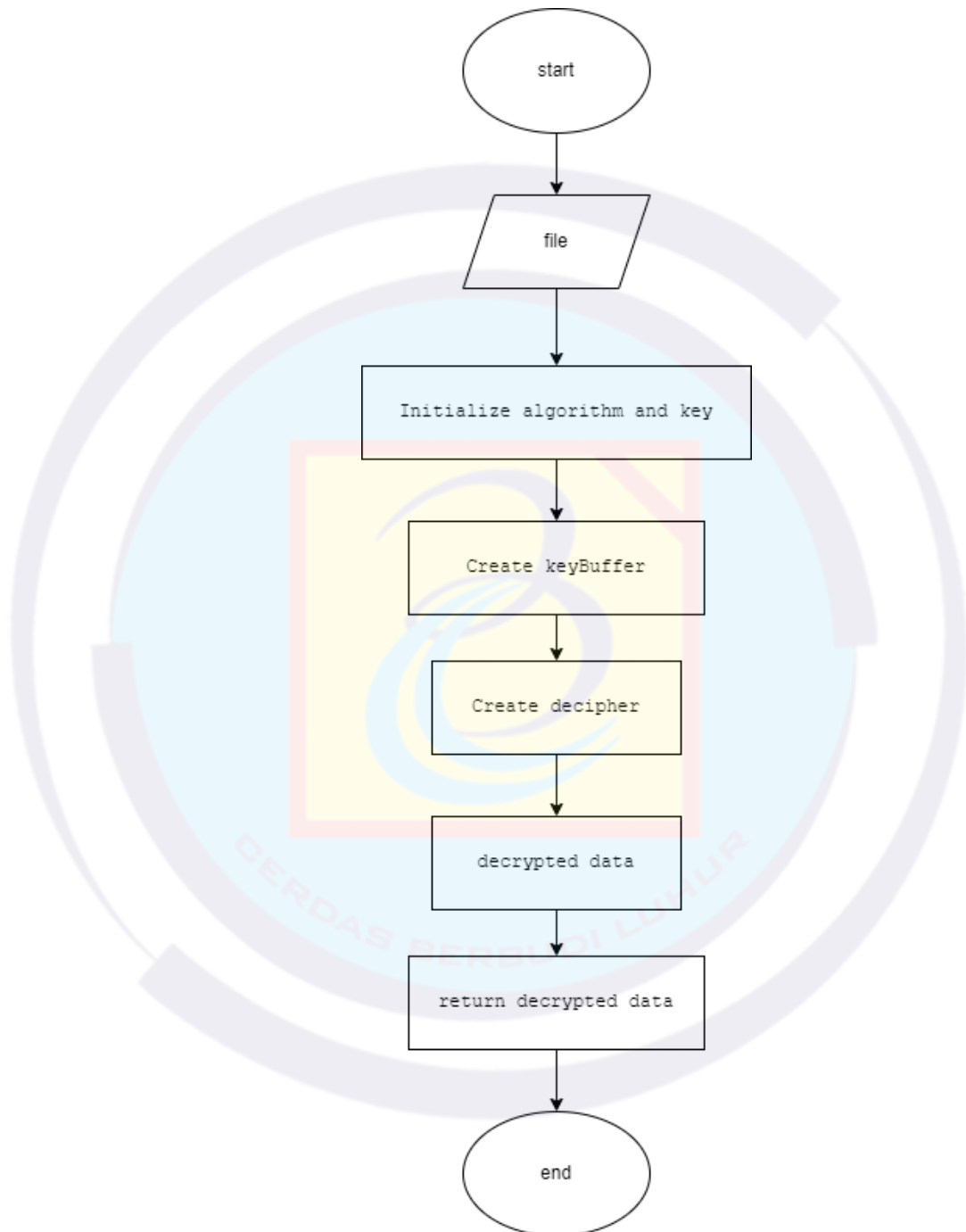
Pada proses enkripsi AES-GCM pada penelitian ini, peneliti menggunakan sebuah library dari node.js yang bernama crypto. Tahap – tahapan enkripsi AES-GCM bisa dilihat melalui gambar 4.13 dibawah ini:



Gambar 4. 13 Flowchart enkripsi AES-GCM

#### 4.3.14 Flowchart deskripsi AES

Pada proses deskripsi AES pada penelitian ini, peneliti menggunakan sebuah library dari node.js yang bernama crypto. Tahap – tahapan deskripsi AES bisa dilihat melalui gambar 4.14 dibawah ini:

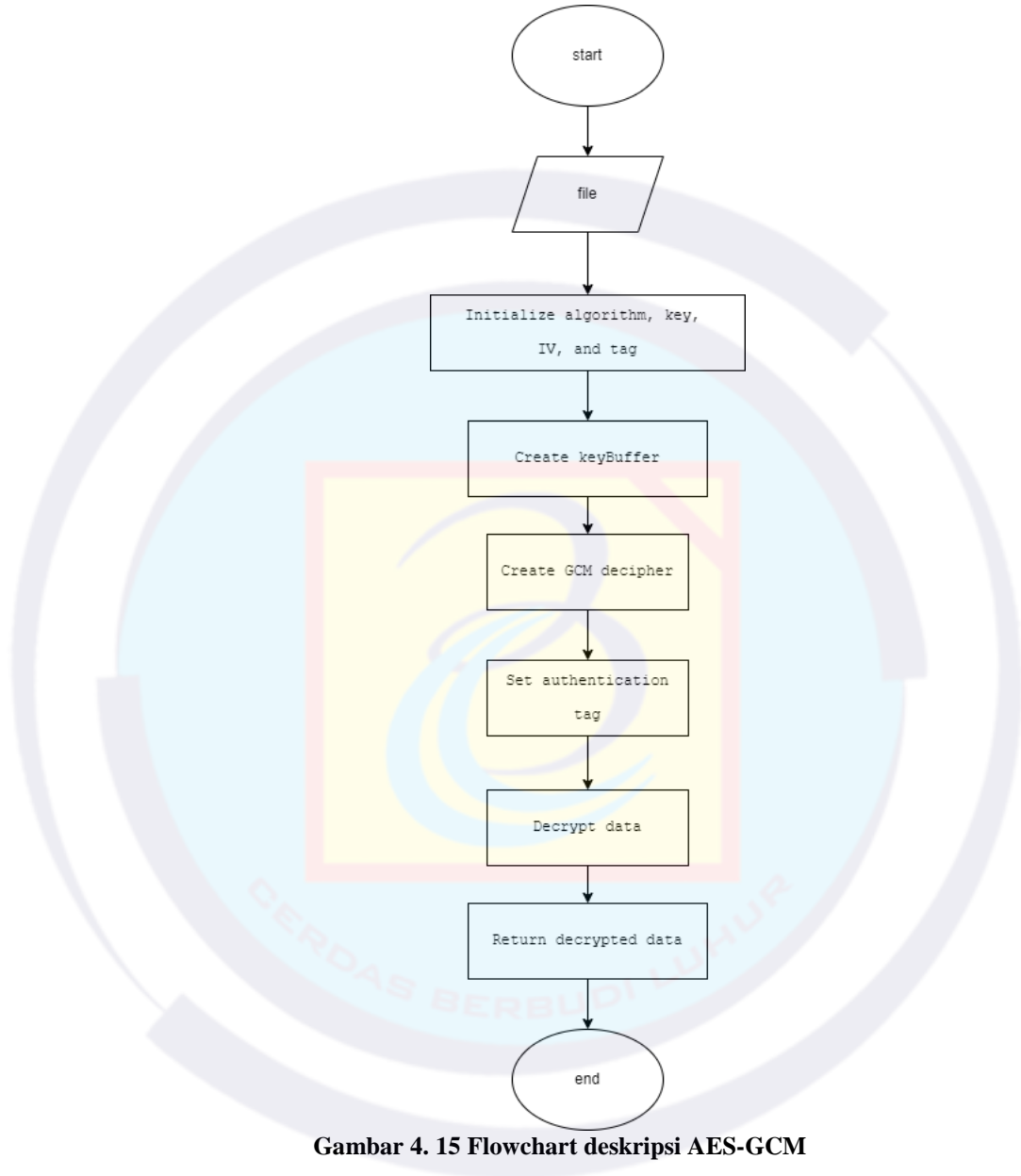


Gambar 4. 14 Flowchart deskripsi AES



#### 4.3.15 Flowchart deskripsi AES-GCM

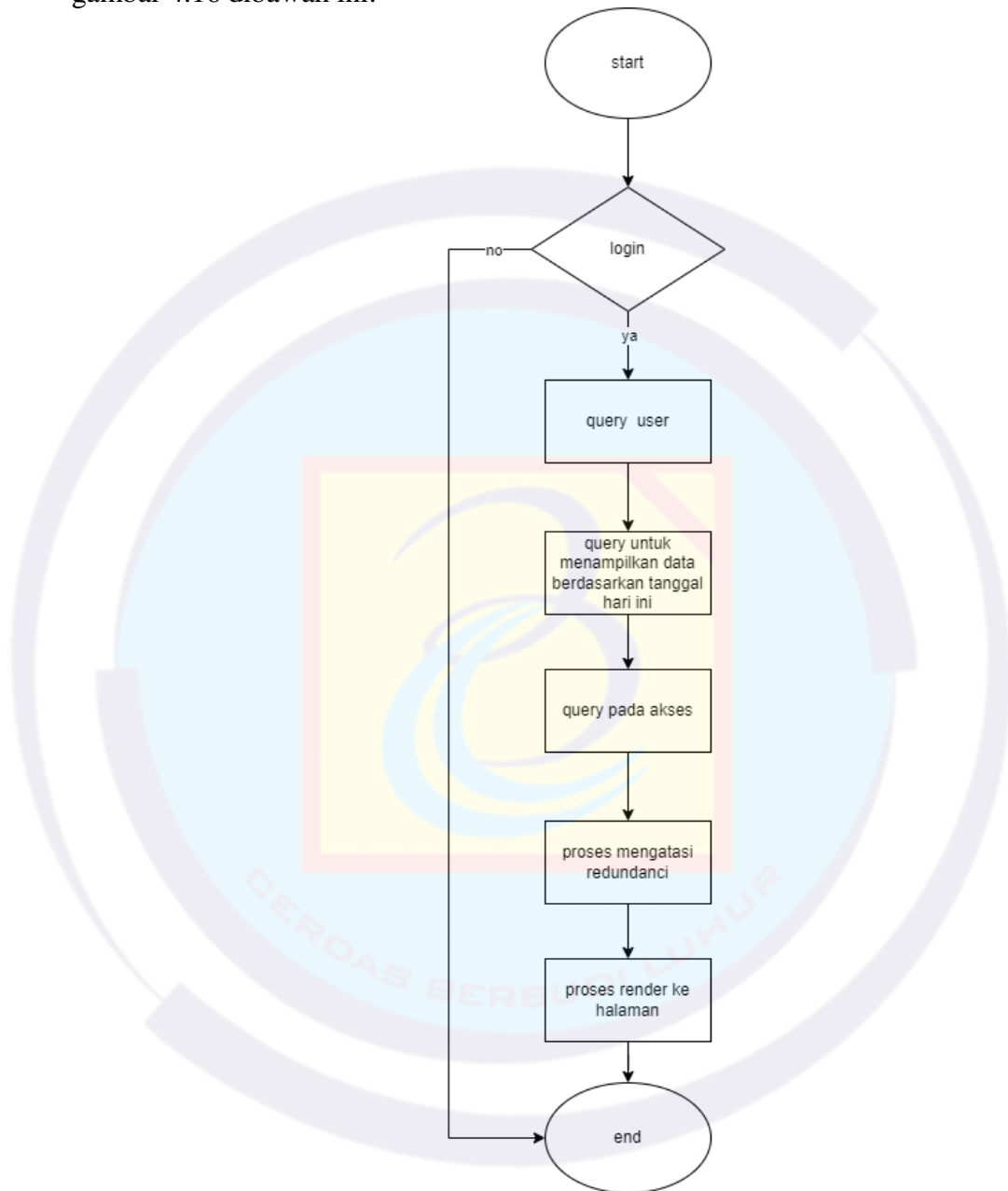
Pada proses deskripsi AES-GCM pada penelitian ini, peneliti menggunakan sebuah library dari node.js yang bernama crypto. Tahap – tahapan deskripsi AES-GCM bisa dilihat melalui gambar 4.15 dibawah ini:



Gambar 4. 15 Flowchart deskripsi AES-GCM

#### 4.3.16 Flowchart untuk mengatasi redundansi pada halaman medical record

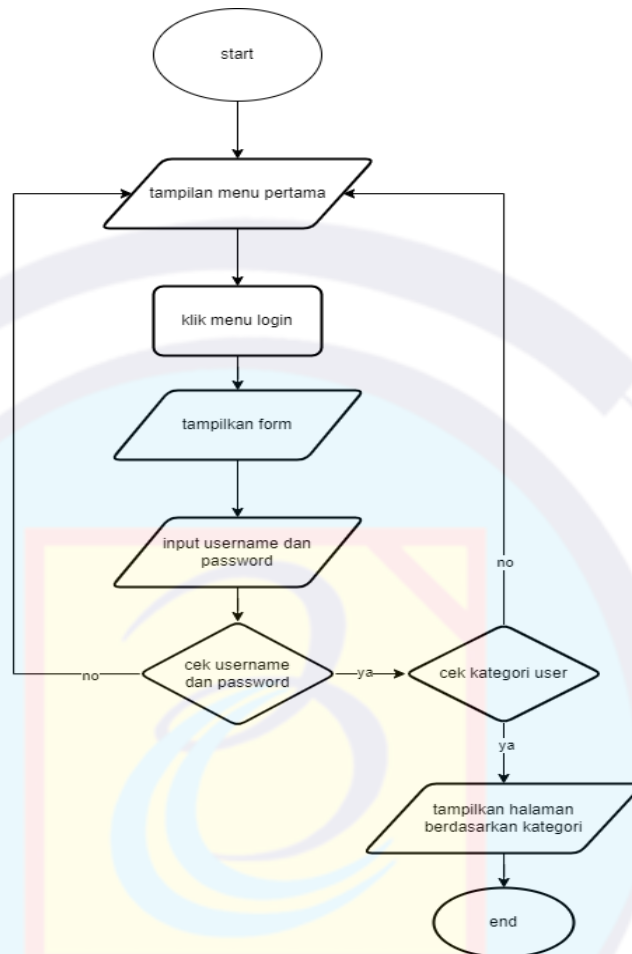
Pada proses mengatasi redundansi pada saat menampilkan file medical record pada halaman medical record pada pasien dan dinkes, bisa dilihat pada gambar 4.16 dibawah ini:



Gambar 4. 16 Flowchart untuk mengatasi redundansi pada halaman medical record

#### 4.3.17 Flowchart halaman login

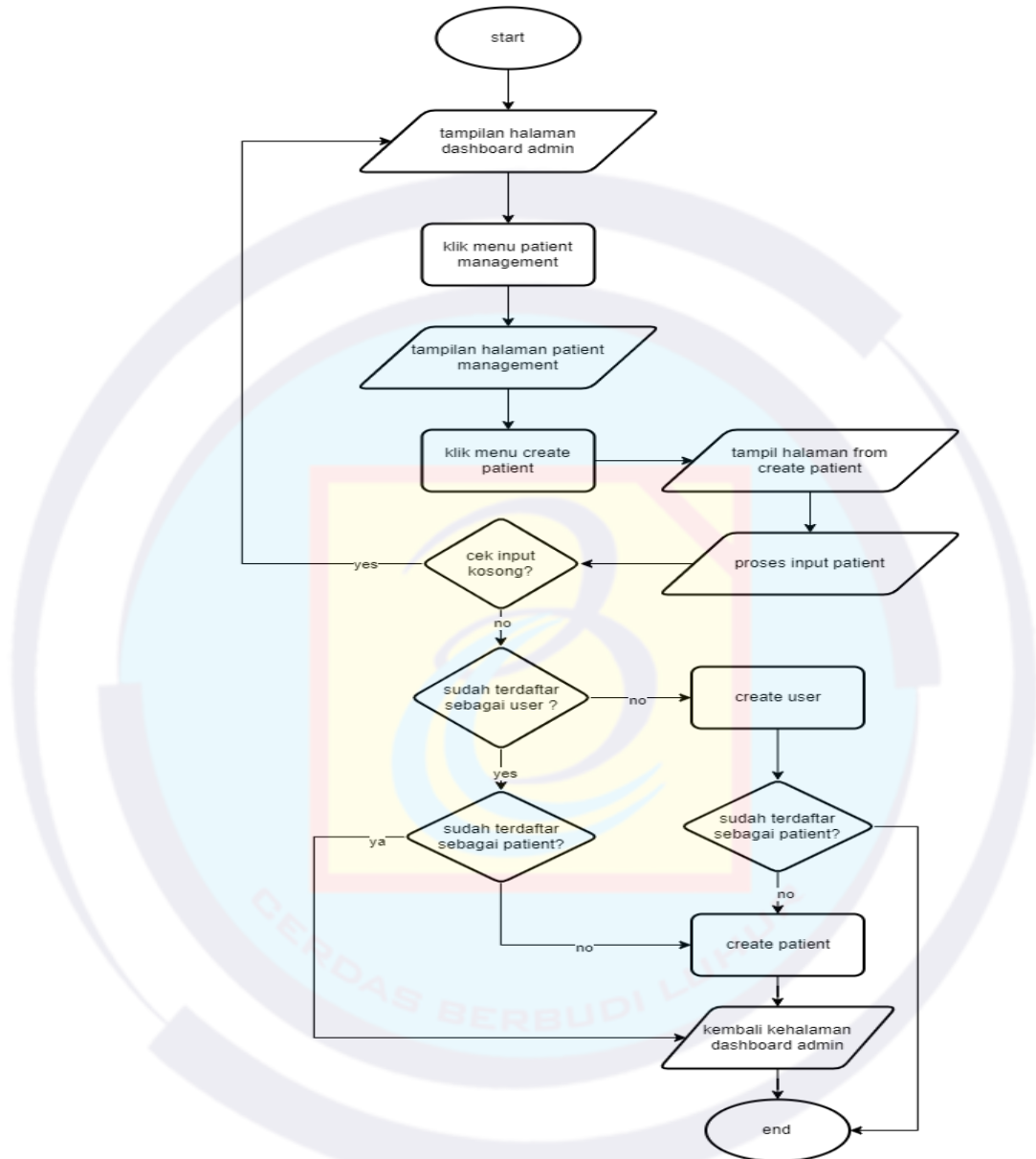
Pada flowchart halaman login bisa dilihat dari gambar 4.17 dibawah ini:



Gambar 4. 17 Flowchart halaman login

#### 4.3.18 Flowchart halaman create pateint dari halaman patient management

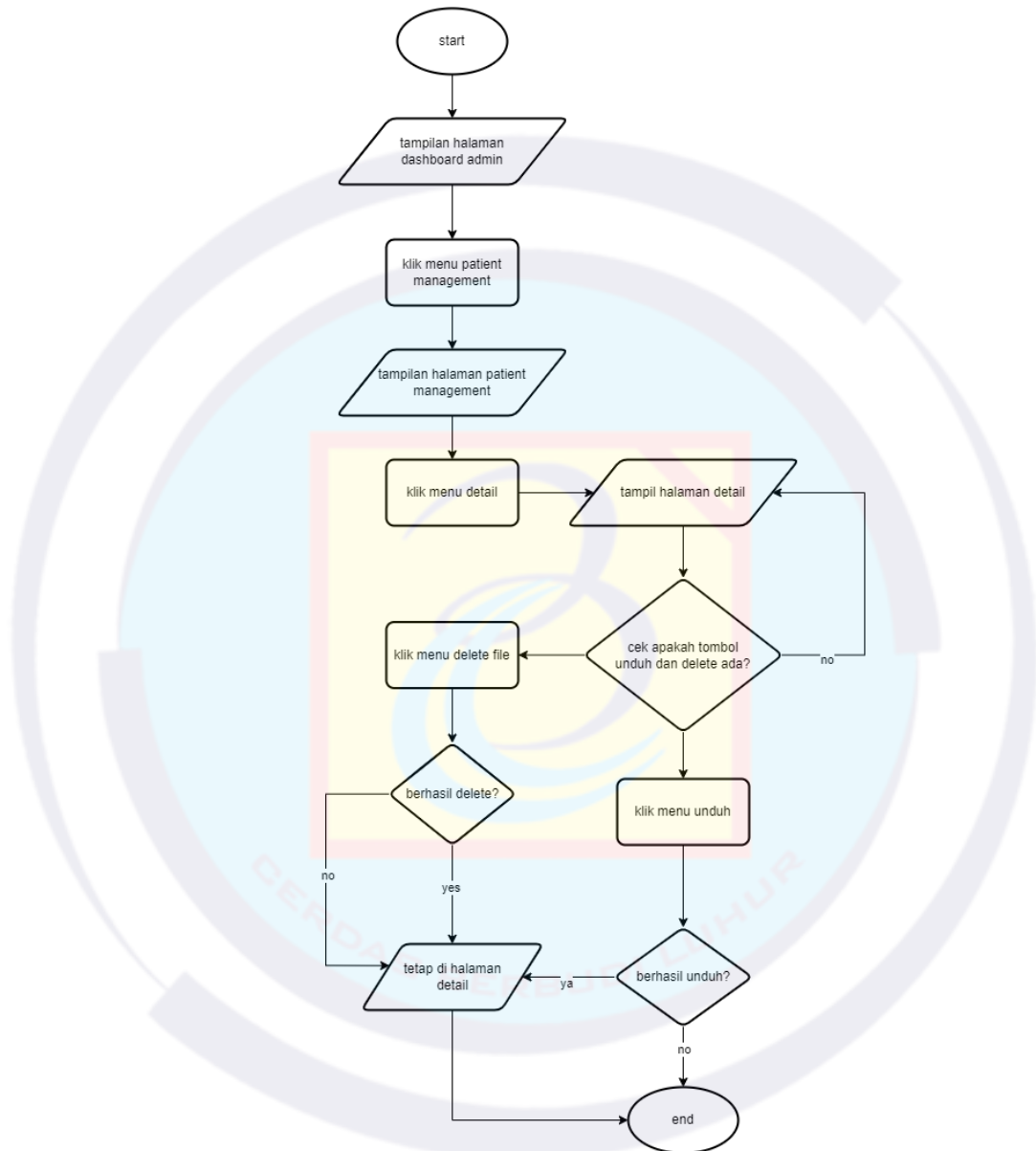
Pada flowchart halaman create patient pada halaman patient management pada admin bisa dilihat dari gambar 4.18 dibawah ini:



Gambar 4. 18 Flowchart halaman create pateint dari halaman patient management

#### 4.3.19 Flowchart halaman detail pasien dan proses unduh dan delete file

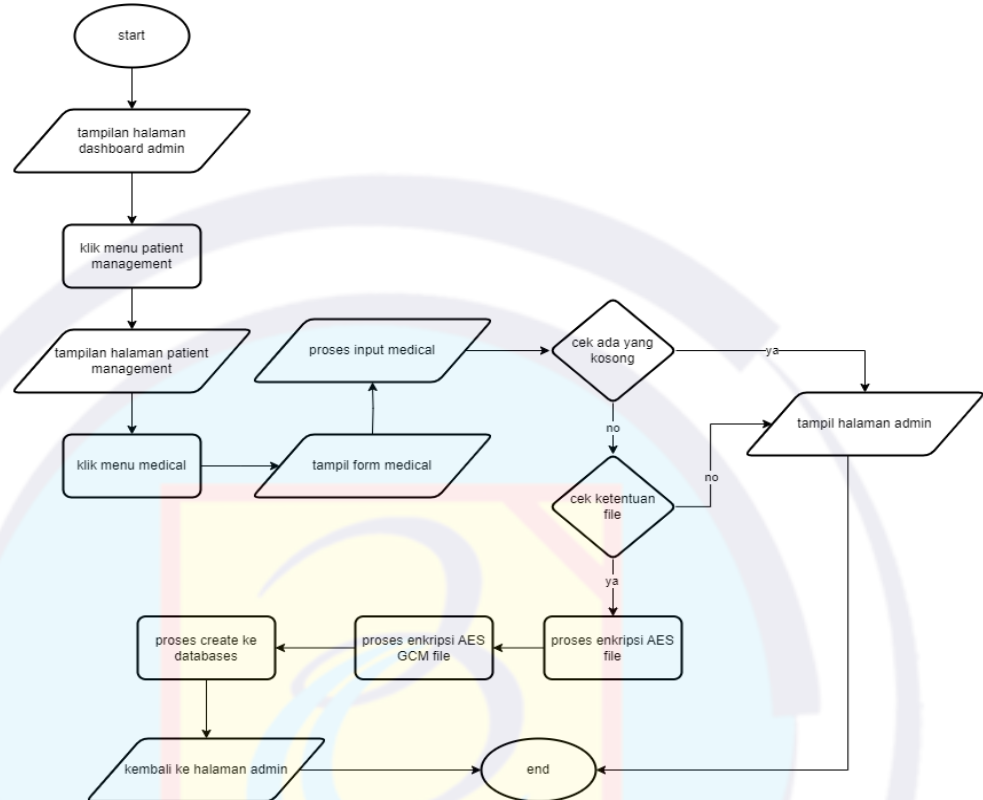
Pada flowchart halaman detail pada halaman patient management dalam proses unduh dan delete file pada admin bisa dilihat dari gambar 4.19 dibawah ini:



Gambar 4. 19 Flowchart halaman detail pasien dan proses unduh dan delete file

#### 4.3.20 Flowchart halaman medical pada menu patient management admin

Pada flowchart halaman medical pada halaman patient management pada admin bisa dilihat dari gambar 4.20 dibawah ini:

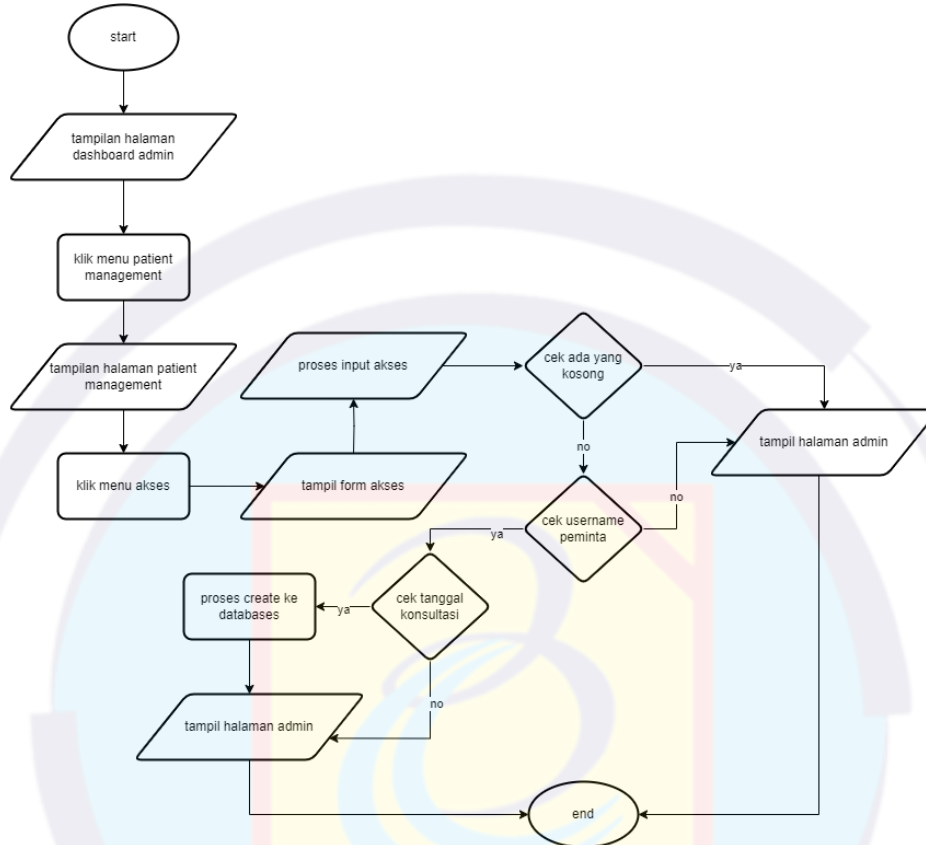


Gambar 4. 20 Flowchart halaman medical pada menu patient management admin



#### 4.3.21 Flowchart halaman akses pada menu patient management admin

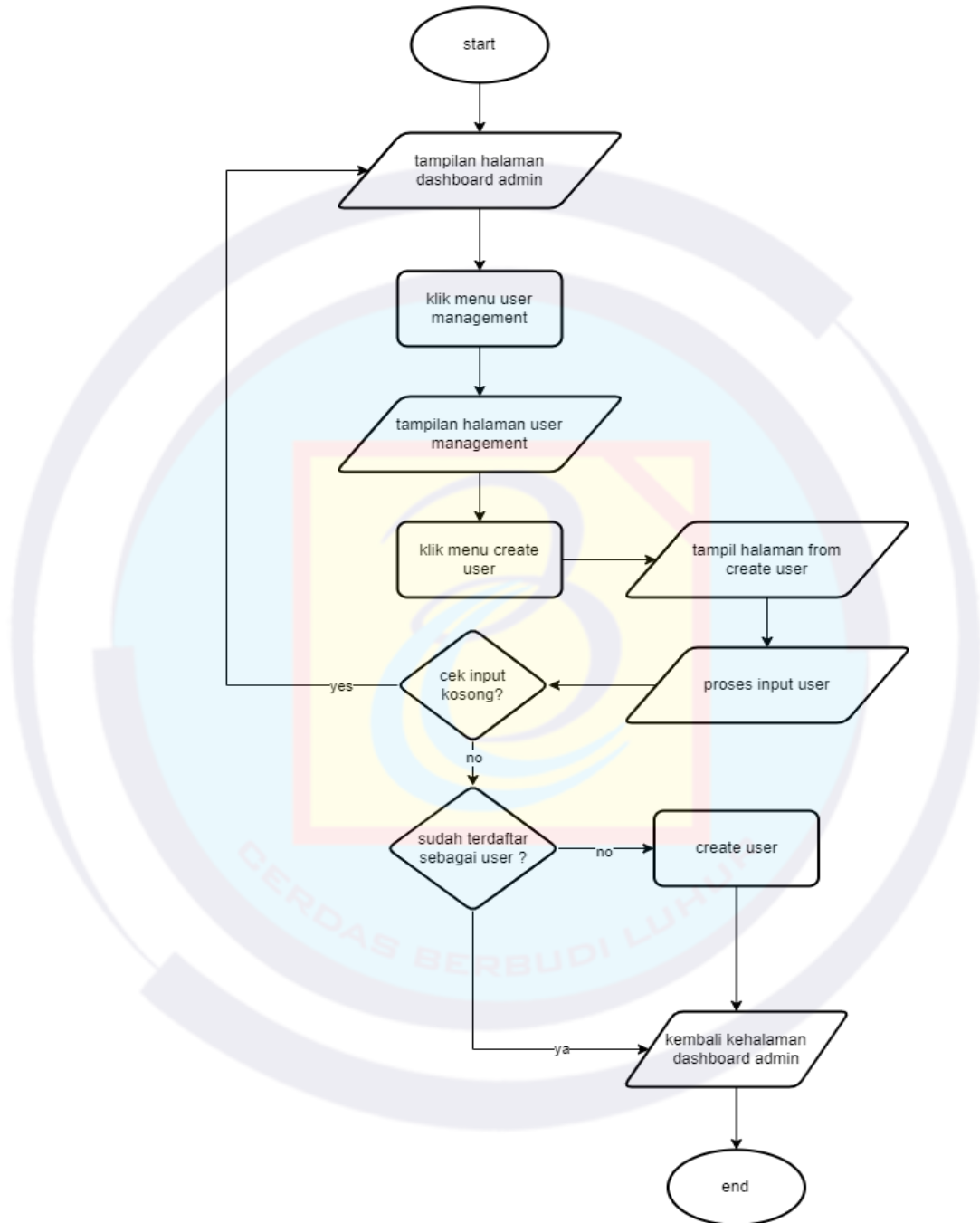
Pada flowchart halaman akses pada halaman patient management pada admin bisa dilihat dari gambar dibawah 4.21 ini:



Gambar 4. 21 Flowchart halaman akses pada menu patient management admin

#### 4.3.22 Flowchart halaman create user pada menu user management admin

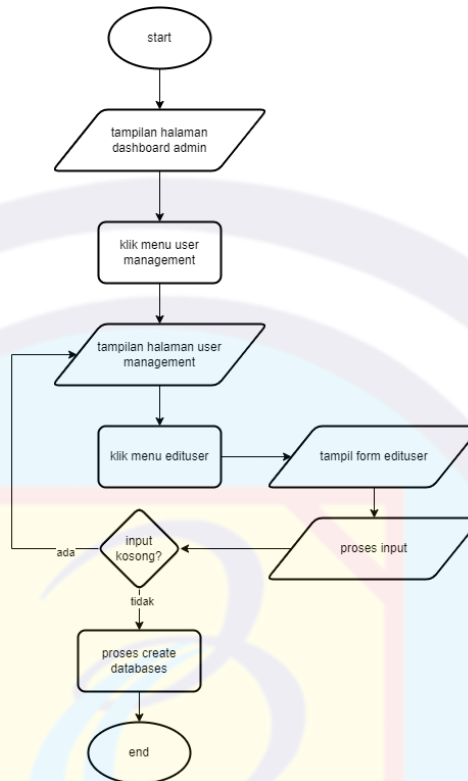
Pada flowchart halaman create user pada halaman user management pada admin bisa dilihat dari gambar 4.22 dibawah ini:



Gambar 4. 22 Flowchart halaman create user pada menu user management admin

#### 4.3.23 Flowchart halaman edit user pada menu user management admin

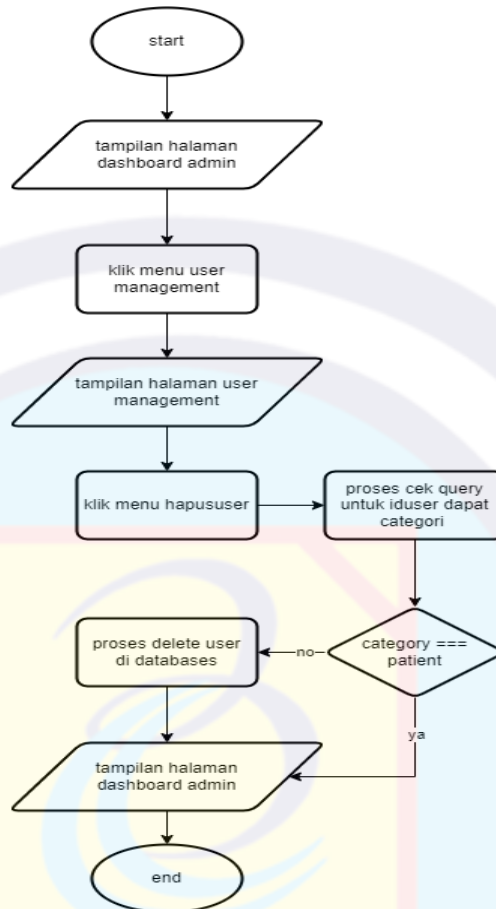
Pada flowchart halaman edit user pada halaman user management pada admin bisa dilihat dari gambar 4.23 dibawah ini:



Gambar 4. 23 Flowchart halaman edit user pada menu user management admin

#### 4.3.24 Flowchart menu hapus user pada menu user management admin

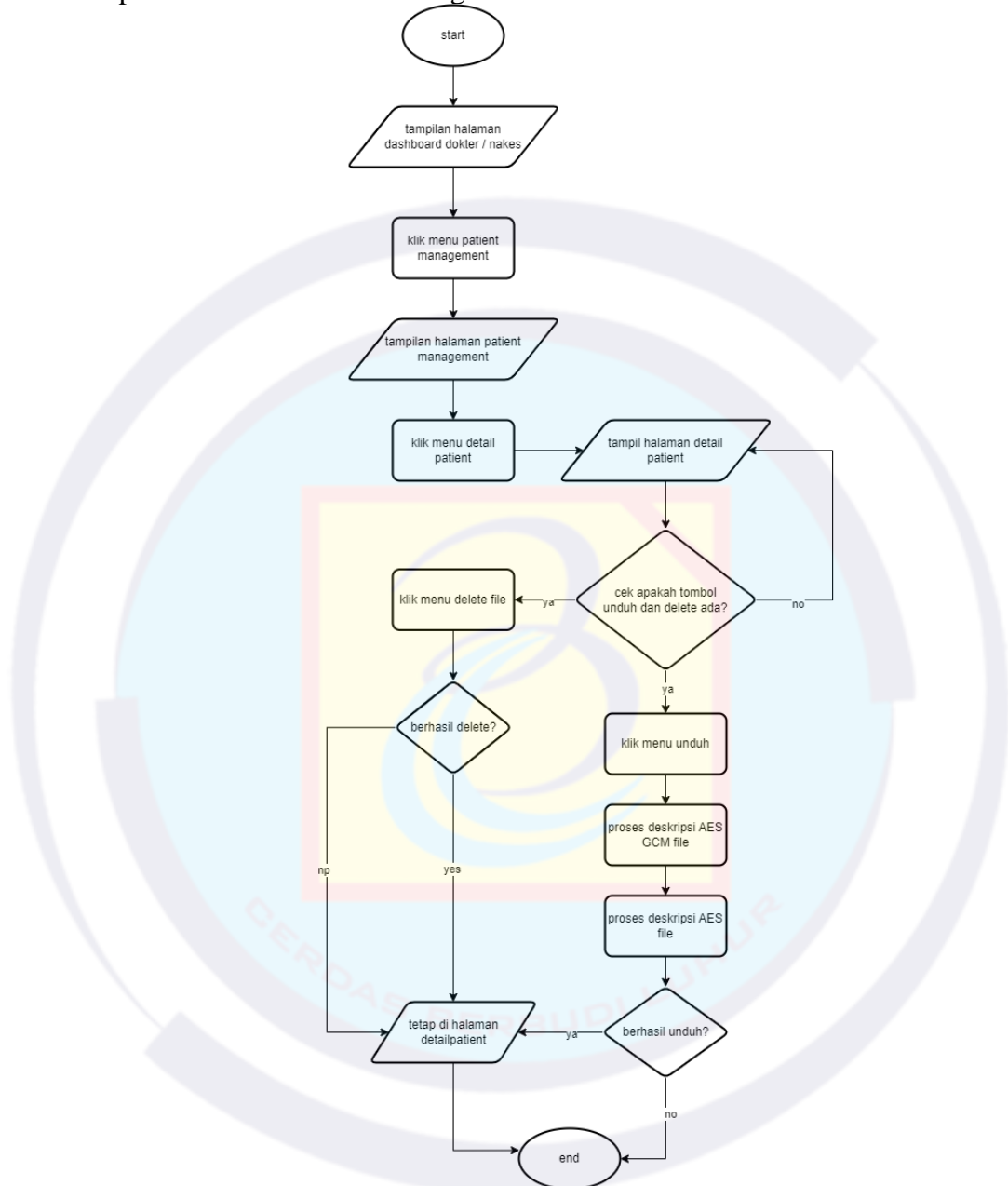
Pada flowchart menu hapus user pada halaman user management pada admin bisa dilihat dari gambar 4.24 dibawah ini:



Gambar 4. 24 Flowchart menu hapus user pada menu user management admin

#### 4.3.25 Flowchart halaman detail pasien dan proses unduh dan delete file

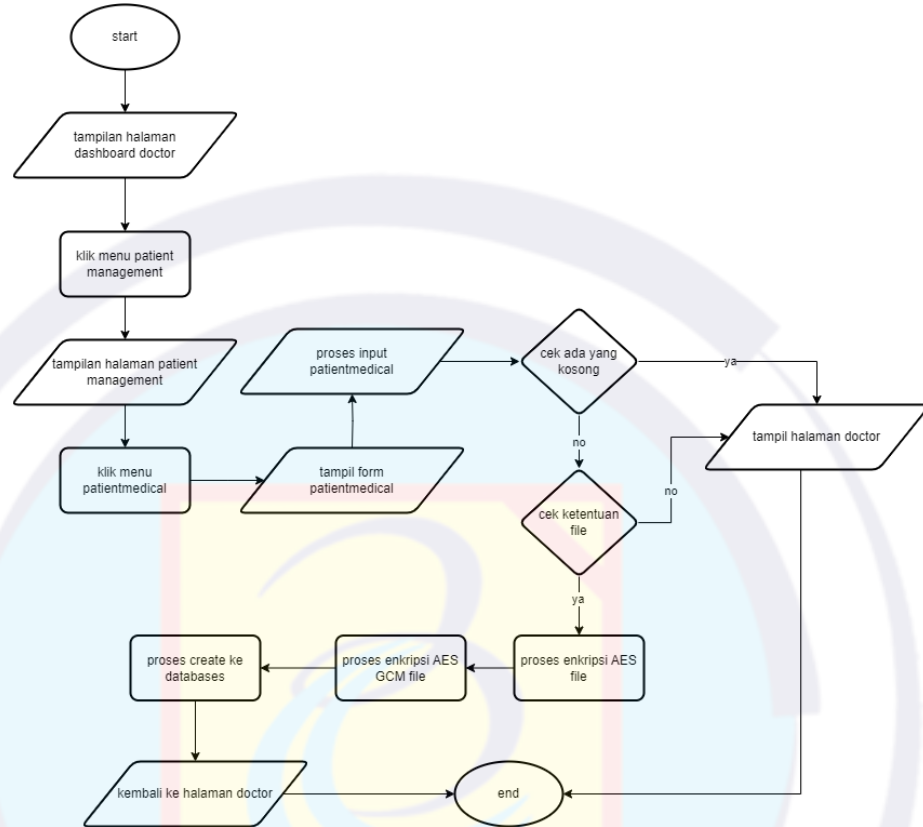
Pada flowchart halaman detail pasien dalam proses unduh dan delete file pada nakes bisa dilihat dari gambar 4.25 dibawah ini:



Gambar 4. 25 Flowchart halaman detail pasien dan proses unduh dan delete file

#### 4.3.26 Flowchart halaman medical pada menu patient management nakes

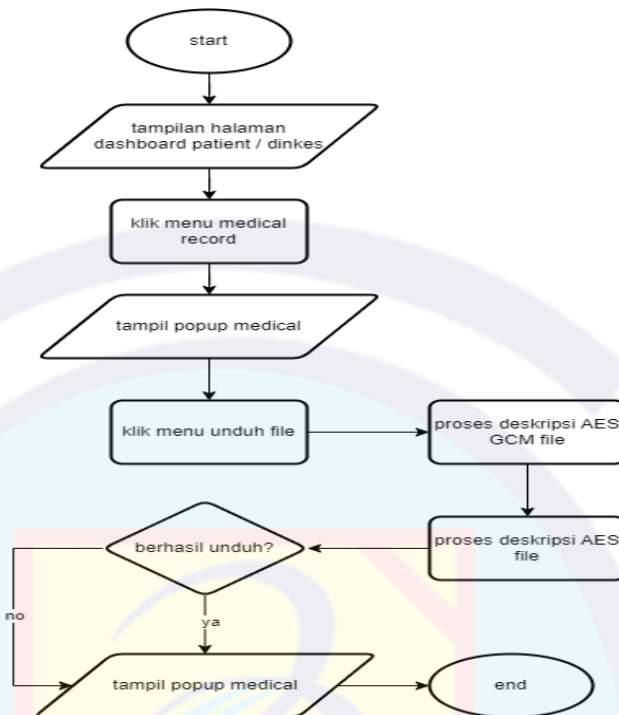
Pada flowchart halaman medical pada nakes bisa dilihat dari gambar 4.26 dibawah ini:



Gambar 4. 26 Flowchart halaman medical pada menu patient management nakes

#### 4.3.27 Flowchart popup medical record pada pasien dan dinkes

Pada flowchart popup medical record pada pasien dan dinkes bisa dilihat dari gambar 4.27 dibawah ini:



Gambar 4. 27 Flowchart popup medical record pada pasien dan dinkes



#### **4. 4 Algoritma**

Pada proses algoritma pada sistem yang berbasis website yang peneliti buat bisa dilihat di bawah ini:

##### **4.4.1 Algoritma login**

Pada algoritma login akan di tampilkan dibawah ini:

**Tabel 4. 1 Algoritma login**

1. Start
2. Input username dan password
3. Proses query user
4. If cek validasi username dan password
5. Make to session
6. If kategori user
7. Update last login
8. Else kategori user
9. Else validasi username dan password
10. End

##### **4.4.2 Algoritma forgot password**

Pada algoritma forgot password akan di tampilkan dibawah ini:

**Tabel 4. 2 Algoritma forgot password**

1. Start
2. Request post
3. If validasi input
4. Query username pada table user
5. If update
6. Else update
7. end

#### 4.4.3 Algoritma add patient dan add user pada admin

Pada algoritma add patient dan add user akan di tampilkan dibawah ini:

**Tabel 4. 3 Algoritma add patient dan add user pada admin**

1. Start
2. Input add patient
3. If validasi input
4. Proses query user dan kategori
5. If user regis
6. Proses query patient
7. If patient
8. Create new patient in function patientCreate
9. Else patient (end)
10. Else user regis
11. Create patient baru ke function userCreate
12. If create user
13. Create patient baru ke function patientCreate
14. Else create user (end)
15. Else validasi input (end)
16. End

#### 4.4.4 Algoritma search patient

Pada algoritma search patient akan di tampilkan dibawah ini:

**Tabel 4. 4 Algoritma search patient**

1. Start
2. If login
3. Input
4. If kosong
5. Proses query table patient dan table user
6. Else kosong
7. Query search di table patient
8. Else login
9. End

#### 4.4.5 Algoritma add rekam medis

Pada algoritma add rekam medis akan di tampilkan dibawah ini:

**Tabel 4. 5 Algoritma add rekam medis**

1. Start
2. Request post
3. If validasi input
4. Kirim RM ke function rekamMedic
5. If validasi file
6. Proses enkripsi AES256
7. Proses enkripsi AES-GCM
8. Create ke databases
9. Upload file fisik ke folder
10. Else validasi file (end)
11. Else validasi input (end)
12. end

#### 4.4.6 Algoritma delete rekam medis

Pada algoritma delete rekam medis akan di tampilkan dibawah ini:

**Tabel 4. 6 Algoritma delete rekam medis**

1. Start
2. Mendapatkan request RMID
3. Query table medicalrecord by RMID
4. If namefile
5. Proses delete file
6. Else namefile (end)
7. End

#### 4.4.7 Algoritma unduh file rekam medis

Pada algoritma unduh file rekam medis akan di tampilkan dibawah ini:

**Tabel 4. 7 Algoritma unduh file rekam medis**

1. Start
2. Mendapatkan request dan kirim ke function unduh
3. Function unduh
4. Query medicalrecord file by RMID
5. If file
6. Ambil dan baca nama file, tag dan iv
7. Kirim ke funtion deskripsi AESGCM
8. Kirim ke funtion deskripsi AES256
9. Proses unduh
10. Else file (end)

#### 4.4.8 Algoritma akses rekam medis

Pada algoritma akses rekam medis akan di tampilkan dibawah ini:

**Tabel 4. 8 Algoritma akses rekam medis**

1. Start
2. Request post akses
3. If validasi data
4. Kirim ke function prosesCek
5. If validasi proses
6. Kirim respon
7. Else validasi proses (end)
8. Else validasi data (end)
9. End

#### 4.4.9 Algoritma add user

Pada algoritma create user akan di tampilkan dibawah ini:

**Tabel 4. 9 Algoritma add user**

1. Start
2. Request post
3. If validasi input
4. Query username and kategori
5. If user
6. Proses pembuatan ID
7. Create user
8. Else user (end)
9. Else validasi input (end)
10. End

#### 4.4.10 Algoritma delete user

Pada algoritma delete user akan di tampilkan dibawah ini:

**Tabel 4. 10 Algoritma delete user**

1. Start
2. Request get
3. Query id user ke table user
4. If category === patient (end)
5. Else kategori
6. Query delete user
7. End

#### 4.4.11 Algoritma edit user

Pada algoritma edit user akan di tampilkan dibawah ini:

**Tabel 4. 11 Algoritma edit user**

1. Start
2. Request post
3. If validasi input
4. Query update table user
5. Else validasi input (end)
6. End

#### 4.4.12 Algoritma enkripsi AES-256

Pada algoritma enkripsi AES-256 akan di tampilkan dibawah ini:

**Tabel 4. 12 Algoritma enkripsi 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

#### 4.4.13 algoritma enkripsi AES-GCM

Pada algoritma enkripsi AES-GCM akan di tampilkan dibawah ini:

**Tabel 4. 13 Algoritma enkripsi 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

#### 4.4.14 Algoritma deskripsi AES-256

Pada algoritma deskripsi AES-256 akan di tampilkan dibawah ini:

**Tabel 4. 14 Algoritma 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

#### 4.4.15 Algoritma deskripsi AES-GCM

Pada algoritma deskripsi AES-GCM akan di tampilkan dibawah ini:

**Tabel 4. 15 Algoritma 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

#### 4.4.16 Algoritma redundansi pada halaman medical record

Pada algoritma redundansi pada halaman medical record akan di tampilkan dibawah ini:

**Tabel 4. 16 Algoritma redundansi pada halaman medical record**

1. start
2. If login
3. Query user
4. Query untuk menampilkan data berdasarkan tanggal hari ini
5. Query pada akses
6. Proses mengatasi redundansi
7. Proses render ke halaman
8. Else login (end)
9. end

#### 4.5 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 ditentukan oleh peneliti. Proses penelitian ini bisa dilihat melalui tabel dibawah ini:

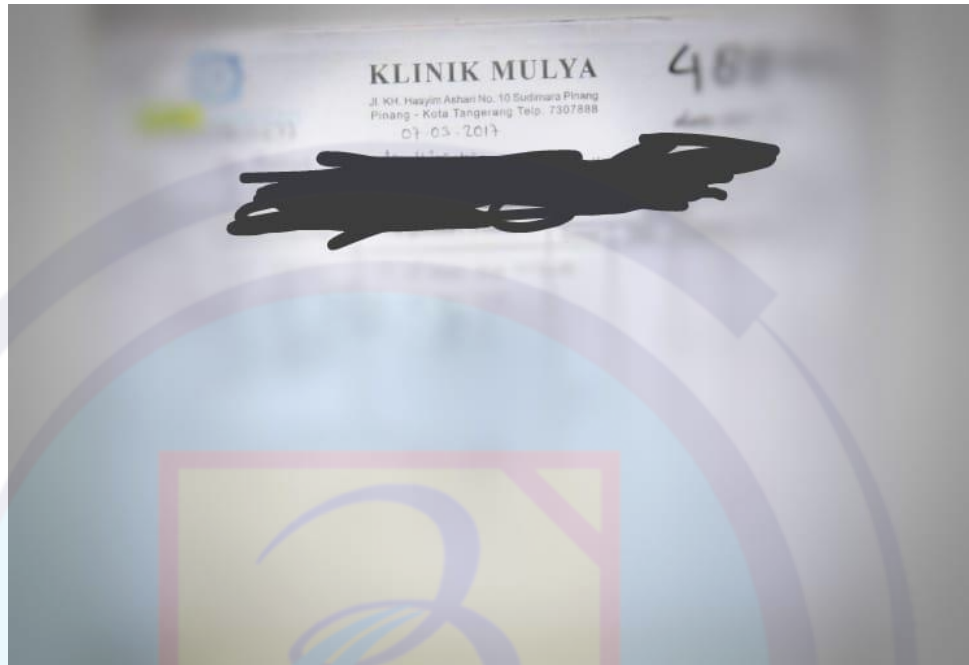
**Tabel 4. 17 Pengujian**

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 pengecekan dari size, ekstensi dan tipe file. Size yang diijinkan sebesar 4mb, ekstensi 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 pengecekan dari size, ekstensi dan tipe file. Size yang diijinkan sebesar 4mb, ekstensi 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 terenripsi 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



#### 4.5.1 Objek dalam pengujian

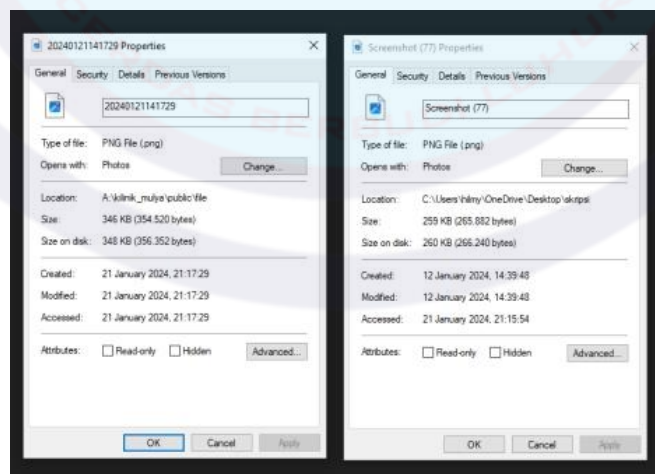
Dibawah ini merupakan objek yang berupa sebuah gambar yang digunakan dalam proses pengujian penelitian ini. Objek ini berupa sebuah foto yang berisikan rekam medis pasien dari klinik mulya. Objek bisa dilihat dibawah ini:



Gambar 4. 28 Objek dalam pengujian

#### 4.5.2 Gambar pengujian enkripsi

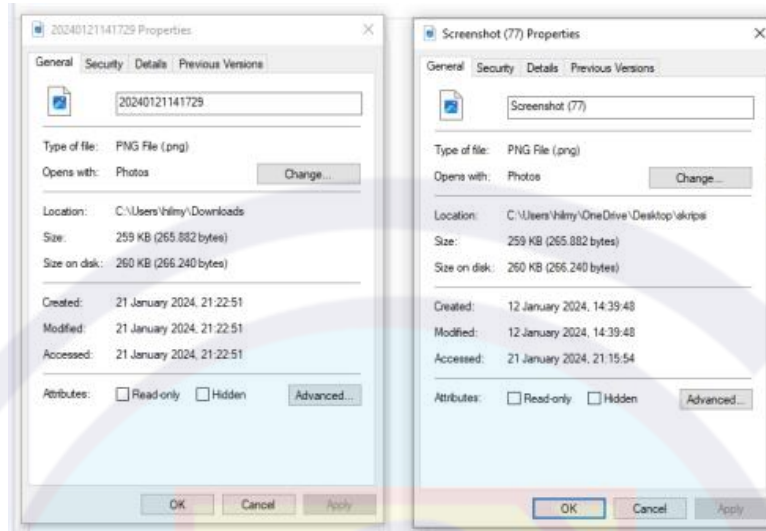
Dibawah ini merupakan gambar hasil dari proses pengujian pada enkripsi AES-256 dengan AES-GCM. Untuk foto sebelah kiri merupakan foto hasil dari enkripsi dan sebelah kanan file asli.



Gambar 4. 29 Gambar pengujian enkripsi

#### 4.5.3 Gambar pengujian deskripsi

Dibawah ini merupakan gambar hasil dari proses pengujian pada deskripsi AES-GCM dengan AES-256. Untuk foto sebelah kiri merupakan foto hasil dari deskripsi dan sebelah kanan file asli.



Gambar 4. 30 Gambar pengujian deskripsi

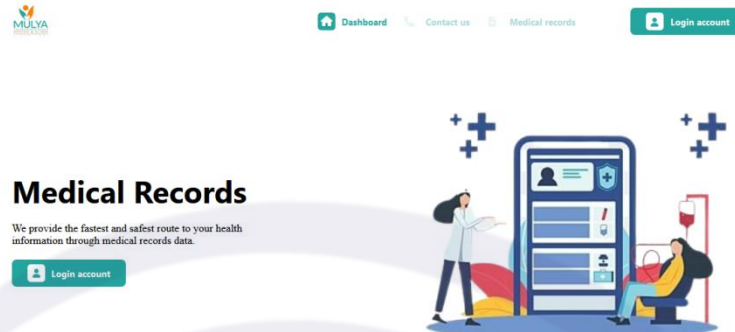
#### 4. 6 Analisa Pengujian

Setelah proses pengujian yang dilakukan oleh peneliti terhadap sistem yang berbasis website ini, peneliti melakukan analisa pengujian terhadap fungsional pada sistem yang peneliti 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 ekstensi 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.

## 4. 7 Tampilan Layar

### 4.7.1 Tampilan layar awal sebelum login

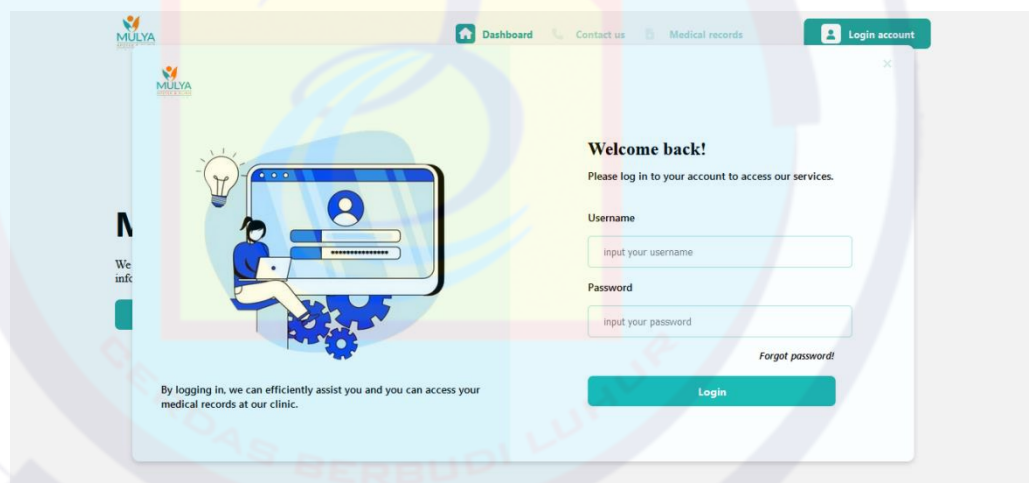
Pada tampilan layar awal sebelum login bisa dilihat dari gambar 4.31 dibawah ini:



Gambar 4. 31 Tampilan layar sebelum login

### 4.7.2 Tampilan layar login

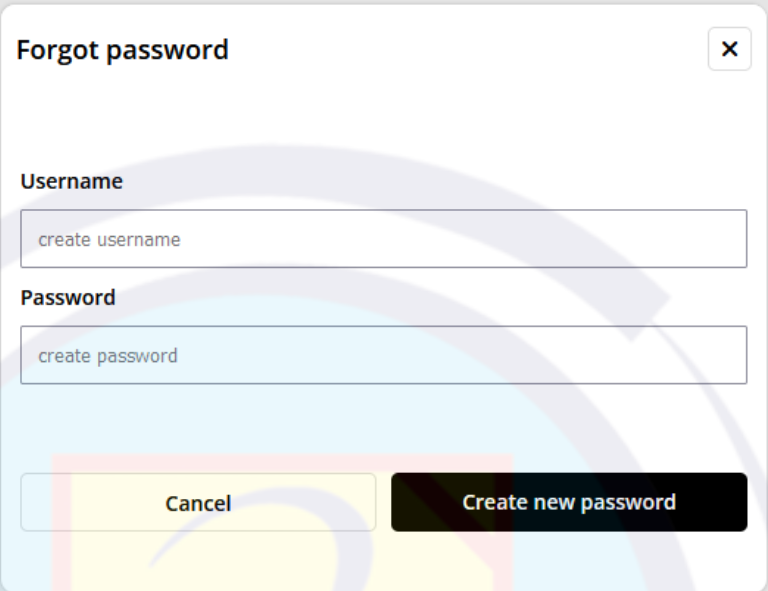
Pada tampilan layar login bisa dilihat dari gambar 4.32 dibawah ini:



Gambar 4. 32 Tampilan layar login

#### 4.7.3 Tampilan layar forgot password

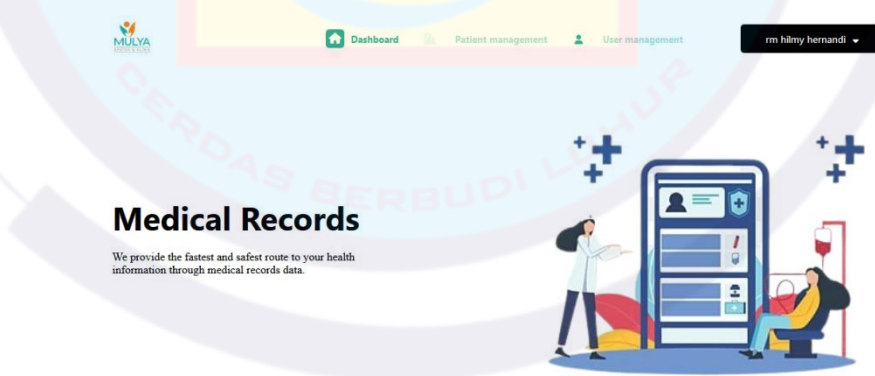
Pada tampilan layar forgot password bisa dilihat dari gambar 4.33 dibawah ini:



Gambar 4. 33 Tampilan layar forgot password

#### 4.7.4 Tampilan layar dashboard sebagai admin

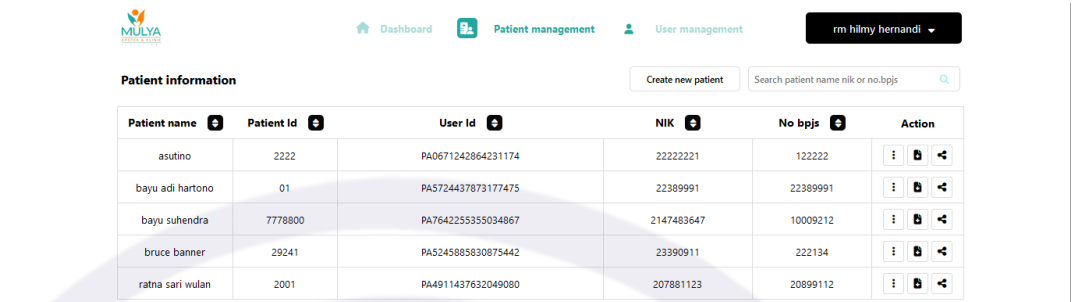
Pada tampilan layar dashboard sebagai admin bisa dilihat dari gambar 4.34 dibawah ini:



Gambar 4. 34 Tampilan layar setelah login sebagai admin

#### 4.7.5 Tampilan layar patient management admin

Pada tampilan layar patient management sebagai admin bisa dilihat dari gambar 4.35 dibawah ini:



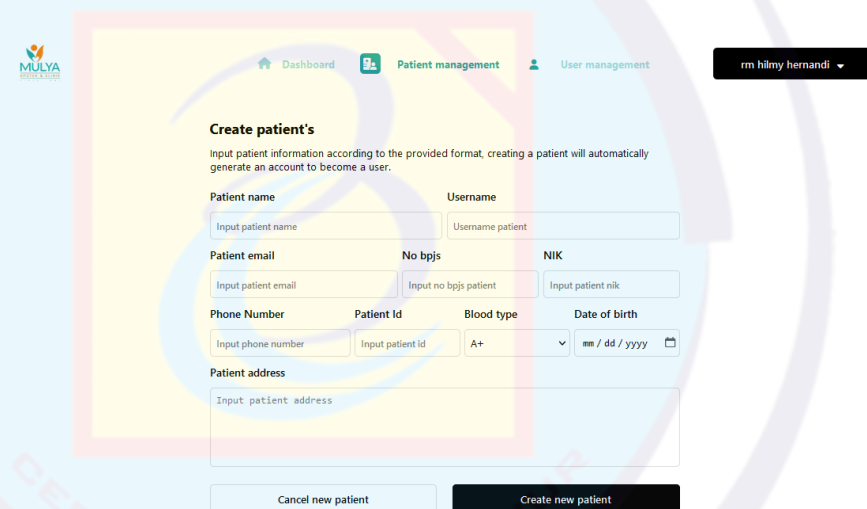
The screenshot shows the 'Patient management' section of the application. At the top, there are navigation links for 'Dashboard', 'Patient management' (active), and 'User management'. A user profile dropdown for 'rm hlmmy hernandi' is visible. Below the navigation, there is a 'Create new patient' button and a search bar labeled 'Search patient name nik or no.bpjs'. The main content is a table titled 'Patient information' with the following data:

Patient name	Patient Id	User Id	NIK	No bpjs	Action
asutino	2222	PA0671242864231174	22222221	122222	[Edit] [Delete] [Add]
bayu adi hartono	01	PA5724437873177475	22389991	22389991	[Edit] [Delete] [Add]
bayu suhendra	7778800	PA764225355034867	2147483647	10009212	[Edit] [Delete] [Add]
bruce banner	29241	PA5245885830875442	23390911	222134	[Edit] [Delete] [Add]
ratna sari wulan	2001	PA4911437632049080	207881123	20899112	[Edit] [Delete] [Add]

Gambar 4. 35 Tampilan layar patient management admin

#### 4.7.6 Tampilan layar create patient admin

Pada tampilan layar create patient sebagai admin bisa dilihat dari gambar 4.36 dibawah ini:



The screenshot shows the 'Create patient's' form. It includes a header with navigation links and a user profile dropdown. The form itself is titled 'Create patient's' and contains the following fields:

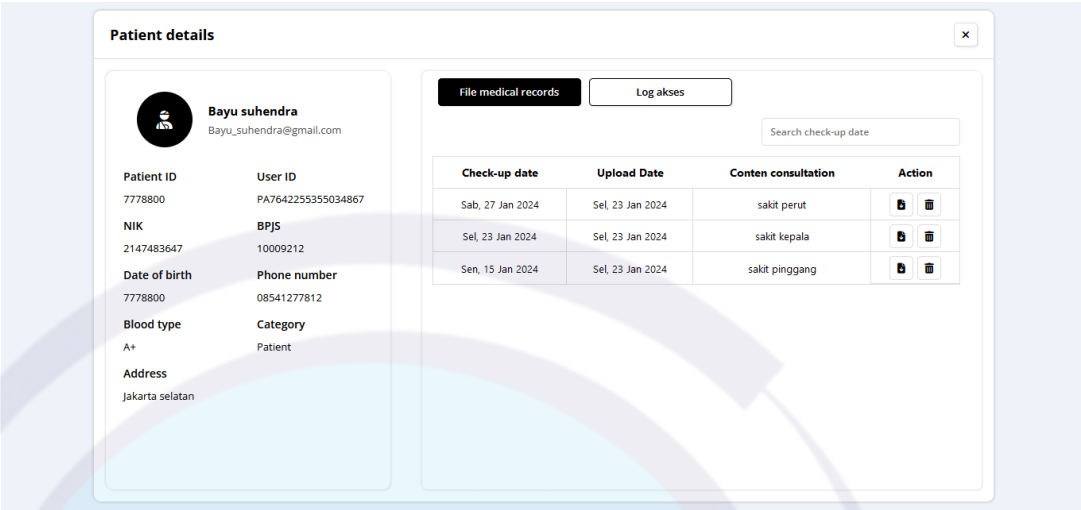
- Patient name** and **Username** (both with input fields)
- Patient email** (input field)
- No bpjs** (input field)
- NIK** (input field)
- Phone Number** (input field)
- Patient Id** (input field)
- Blood type** (dropdown menu, currently showing 'A+')
- Date of birth** (calendar icon)
- Patient address** (text area)

At the bottom of the form, there are two buttons: 'Cancel new patient' and 'Create new patient'.

Gambar 4. 36 Tampilan layar create patient admin

4.7.7 Tampilan layar detail patient admin

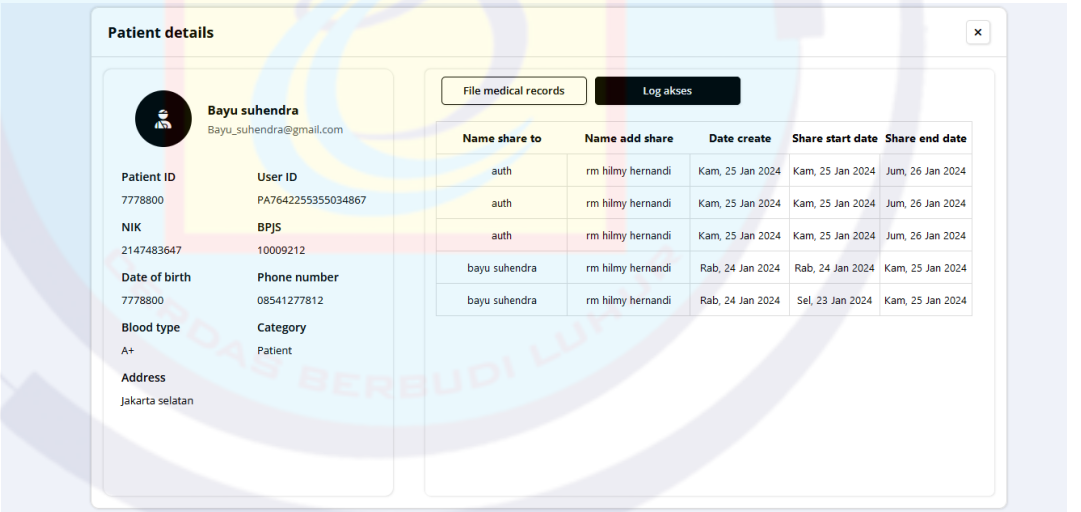
Pada tampilan layar detail patient sebagai admin bisa dilihat dari gambar 4.37 dibawah ini:



Gambar 4. 37 Tampilan layar detail patient admin

4.7.8 Tampilan layar log akses di menu detail pada admin

Pada tampilan layar log akses di menu detail sebagai admin bisa dilihat dari gambar 4.38 dibawah ini:



Gambar 4. 38 Tampilan layar log akses di menu detail pada admin

4.7.9 Tampilan layar add rekam medis pada admin dan nakes

Pada tampilan layar add rekam medis sebagai admin bisa dilihat dari gambar 4.39 dibawah ini:

Medical record upload

Upload File

Input the results of the patient consultation

Patient ID: 7778800

Administrator ID: ad9211233419021045

Consultation date: mm / dd / yyyy

Upload date: 01 / 28 / 2024

Buttons: Cancel upload, Upload

Gambar 4. 39 Tampilan layar add rekam medis pada admin dan nakes

4.7.10 Tampilan layar add akses rekam medis

Pada tampilan layar add akses rekam medis sebagai admin bisa dilihat dari gambar 4.40 dibawah ini:

Medical record access

Document collection

Document checklist to determine the files and access dates.

Check-up date	Upload Date
Sab, 27 Jan 2024	Sel, 23 Jan 2024
Sel, 23 Jan 2024	Sel, 23 Jan 2024
Sen, 15 Jan 2024	Sel, 23 Jan 2024

From creating new access

If you want to create access, please select or click on the combo box in the field and fill in the form above.

Patient ID: 7778800

Share access to: Enter username external or patient

Check-up start date: mm / dd / yyyy

Check-up end date: mm / dd / yyyy

Access create date: 2024-01-28

Share start date: mm / dd / yyyy

Share end date: mm / dd / yyyy

Admin ID: ad9211233419021045

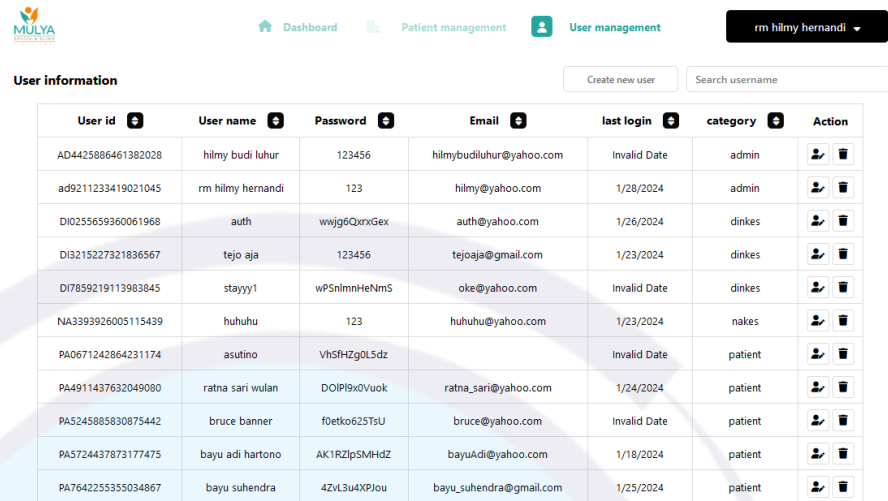
Buttons: Cancel, Create access

Gambar 4. 40 Tampilan layar add akses rekam medis

























#### 4.7.11 Tampilan layar user management pada admin

Pada tampilan layar user management sebagai admin bisa dilihat dari gambar 4.41 dibawah ini:



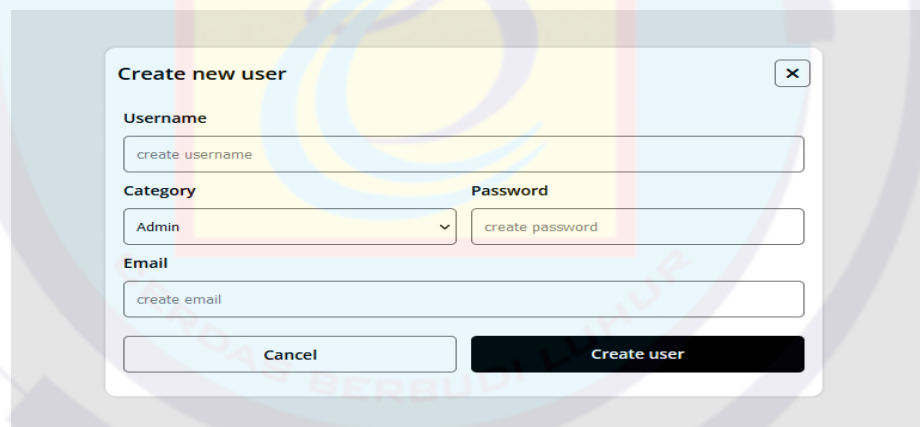
The screenshot shows the 'User management' page. At the top, there are navigation links: 'Dashboard', 'Patient management', and 'User management' (which is active). A user profile dropdown shows 'rm hilmy hernandi'. Below the navigation bar, there's a 'User information' section with a 'Create new user' button and a search bar. The main part of the page is a table listing users.

User id	User name	Password	Email	last login	category	Action
AD4425886461382028	hilmy budi luhur	123456	hilmybudiluhur@yahoo.com	Invalid Date	admin	 
ad9211233419021045	rm hilmy hernandi	123	hilmy@yahoo.com	1/28/2024	admin	 
DI0255659360061968	auth	wwjg6QxrxGex	auth@yahoo.com	1/26/2024	dinkes	 
DI3215227321836567	tejo aja	123456	tejoaja@gmail.com	1/23/2024	dinkes	 
DI7859219113983845	stayyy1	wPSnlmHeNmS	oke@yahoo.com	Invalid Date	dinkes	 
NA3393926005115439	huhuhu	123	huhuhu@yahoo.com	1/23/2024	nakes	 
PA0671242864231174	asutino	VhSfHzg0L5dz		Invalid Date	patient	 
PA4911437632049080	ratna sari wulan	DOLIP9xOVuok	ratna_sari@yahoo.com	1/24/2024	patient	 
PA5245885830875442	bruce banner	f0etko625TsU	bruce@yahoo.com	Invalid Date	patient	 
PA5724437873177475	bayu adi hartono	AK1RZlpSMHdZ	bayuAdi@yahoo.com	1/18/2024	patient	 
PA7642255355034867	bayu suhendra	4ZvL3u4XPJou	bayu_suhendra@gmail.com	1/25/2024	patient	 

Gambar 4. 41 Tampilan layar user management pada admin

#### 4.7.12 Tampilan layar add user pada admin

Pada tampilan layar add user sebagai admin bisa dilihat dari gambar 4.42 dibawah ini:

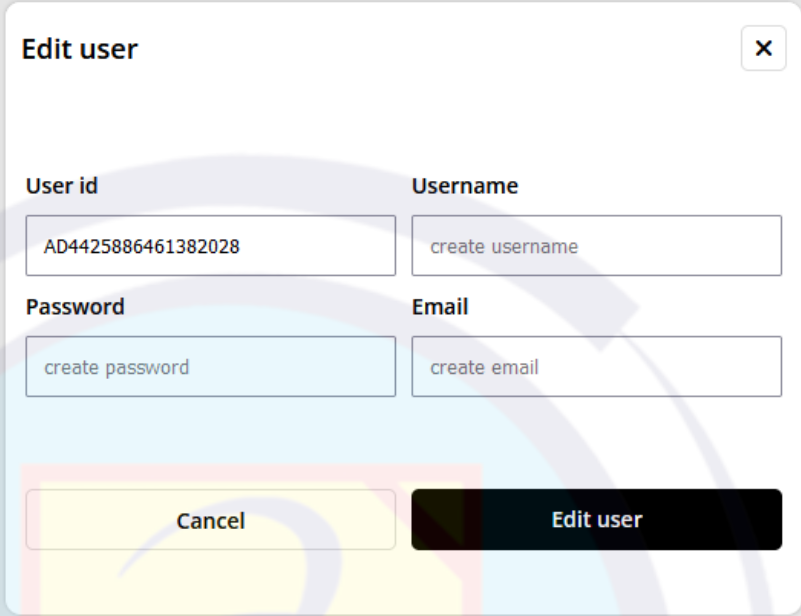


The screenshot shows a 'Create new user' modal form. It has a close button (X) in the top right corner. The form contains the following fields: 'Username' (text input with placeholder 'create username'), 'Category' (dropdown menu with 'Admin' selected), 'Password' (text input with placeholder 'create password'), and 'Email' (text input with placeholder 'create email'). At the bottom, there are two buttons: 'Cancel' and 'Create user'.

Gambar 4. 42 Tampilan layar add user pada admin

#### 4.7.13 Tampilan layar edit user pada admin

Pada tampilan layar edit user sebagai admin bisa dilihat dari gambar 4.43 dibawah ini:



The image shows a modal window titled "Edit user" with a close button (X) in the top right corner. The form contains four input fields arranged in a 2x2 grid. The first row has "User id" with the value "AD4425886461382028" and "Username" with the placeholder "create username". The second row has "Password" with the placeholder "create password" and "Email" with the placeholder "create email". At the bottom of the form are two buttons: a yellow "Cancel" button and a black "Edit user" button.

Gambar 4. 43 Tampilan layar edit user pada admin

#### 4.7.14 Tampilan layar dashboard pada nakes

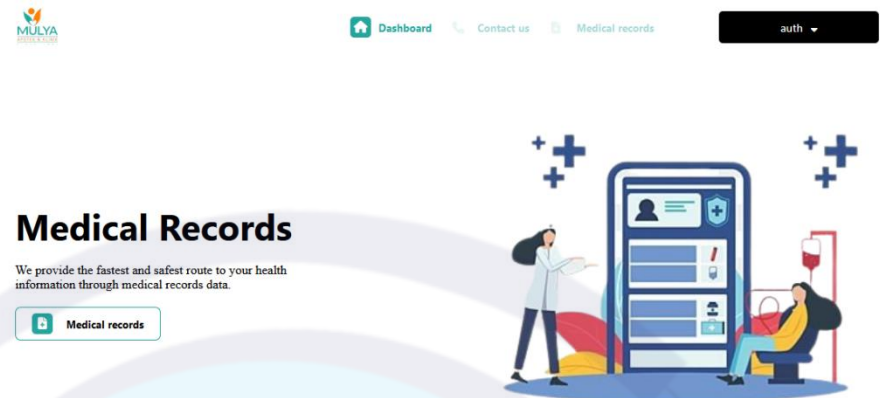
Pada tampilan layar dashboard sebagai nakes bisa dilihat dari gambar 4.44 dibawah ini:



Gambar 4. 44 Tampilan layar dashboard pada nakes

4.7.15 Tampilan layar dashboard pada pasien dan dinkes

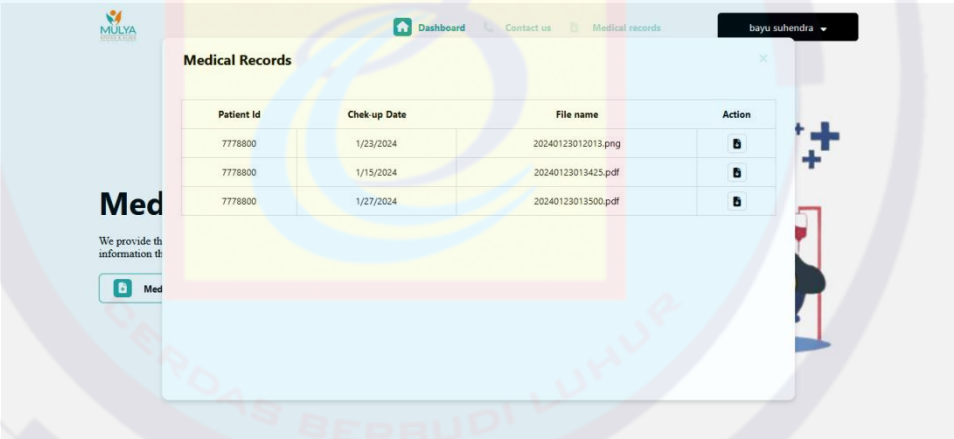
Pada tampilan layar dashboard sebagai pasien dan dinkes bisa dilihat dari gambar 4.45 dibawah ini:



Gambar 4. 45 Tampilan layar dashboard pada pasien dan dinkes

4.7.16 Tampilan layar medical record pada pasien dan dinkes

Pada tampilan layar medical record sebagai pasien dan dinkes bisa dilihat dari gambar 4.46 dibawah ini:



Gambar 4. 46 Tampilan layar medical record pada pasien dan dinkes

## BAB V PENUTUP

Berdasarkan analisa yang telah dilakukan terhadap permasalahan dari sistem ini yang telah dibuat oleh peneliti maka dapat ditarik kesimpulan dan saran yang mungkin diperlukan untuk pengembangan sistem berbasis website ini.

### 5.1 Kesimpulan

Berdasarkan perumusan masalah dari program yang berbasis website ini yang telah dibuat dan di uji coba, maka disimpulkan sebagai berikut:

- a. Website untuk pengaman file dan pengelolaan rekam medis pasien telah berhasil dibuat mengikuti metodologi *waterfall* dan metode pengujian *blackbox testing*.
- b. Dengan adanya sistem ini data rekam medis yang berbentuk file memiliki sistem keamanan yang cukup baik.
- c. Dengan adanya sistem ini peneliti berhasil menerapkan dan melakukan proses enkripsi dan deskripsi dengan algoritma AES-256 dan AES-GCM.

### 5.2 Saran

Selain menarik beberapa kesimpulan, adapun saran yang mungkin diperlukan untuk proses perkembangan pada sistem supaya lebih baik.

- a. Disarankan untuk melakukan perkembangan dalam desain website ini.
- b. Disarankan untuk mengupdate sistem akses.

## DAFTAR PUSTAKA

- Ahmad Mohammed Almorabea, M. A. (2015). *Symmetric Key Encryption Using AES-GCM and External Key Derivation for Smart Phones. International Journal of Computer Networks and Communications Security VOL. 3, NO. 6, JUNE 2015, 3, 264 – 270.*
- Arif Amrulloh, E. (2019). *Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher. Jurnal CoreIT, Vol.5, No.2, Desember 2019, 5, 71-77.*
- Eka Rahmawati, S. ., (2020). *Rancang Bangun Sistem Informasi Rekam Medik Studi Kasus: UPTD Puskesmas Padamara Kabupaten Purbalingga. IJSE – Indonesian Journal on Software Engineering, Vol.6, No. 1, Juni 2020, 6, 133-144.*
- Handrian Saputra Djong, S. 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, 06 September 2022, 149-158.*
- Herman, WijayaRobby, FarandiKenner, MiharjaSatriya, & Wilson. (2020). *Implementasi Algoritma AES-128 Dan SHA-256 Dalam Perancangan Aplikasi Pengamanan File Dokumen. Jurnal Times Technology Informatiics & Computer System.*
- HuluDelisman, NadeakBerto, & AripinSoeb. (2020). *Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSUD Imelda Medan. Konferensi Nasional Teknologi Informasi dan Komputer.*
- Jaka Prayudha, S. I. (2019). *Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES). Sains dan Komputer (SAINTIKOM) Vol.18, No.2, Agustus 2019, 18, 119-129.*
- Jamaluddin, N. F. (2020). *KONSEP PENGAMANAN VIDEO CONFERENCE DENGAN ENKRIPSI AES-GCM PADA APLIKASI ZOOM. METHOMIKA: Jurnal Manajemen Informatika & Komputerisasi Akuntansi Vol. 4 No. 2 (Oktober 2020), 4, 109 -113.*

- LailaRicaró. (2020). Implementasi Algoritma AES 256 Bit Dan Lsb Untuk Pengamanan Dan Penyisipan Pesan Teks Pada File Audio. Jurnal Pelita Informatika.*
- Noviyanti. P, M. (2022). Analisa Algoritma Kriptografi Klasik Caesar Cipher Viginere Cipher dan Hill Cipher. JIFOTECH (JOURNAL OF INFORMATION TECHNOLOGY) Vol. 2, No. 1, Maret 2022, 2, 23-29.*
- PrayudhaJaka, Saniman, & Ishak. (2019). Implementasi Keamanan Data Gaji Karyawan Pada PT. Capella Medan Menggunakan Metode Advanced Encryption Standard (AES). Sains dan Komputer.*
- PutraPrajuhanaAgung , Herfina, MaryanaSufiatul, & Setiawan Andrian. (2020). Implementasi Algoritma AES (Advance Encryption Standard) Rijndael Pada Aplikasi Keamanan Data. Jurnal Ilmiah Penelitian Teknologi Informasi & Komputer.*
- RahmawatiEka, Saifudin , KesumaChandra, & RaisNurAmin. (2020). Rancang Bangun Sistem Informasi Rekam Medik Studi Kasus: UPTD Puskesmas Padamara Kabupaten Purbalingga. Indonesian Journal on Software Engineering.*
- SaputraDwiAnggi , & Syafrulloh Mohamad. (2022). Algoritme AES-256 Untuk Keamanan Basis Data Penilaian Pegawai Pada Pt. Buana Jaya Korindo. Seminar Nasional Mahasiswa Fakultas Teknologi Informasi.*
- SettiSunil, GunawanIndra, DamanikEfendiBahrudin , Sumarno, & Kirana Oktalka . (2020). Implementasi Algoritma Advanced Encryption Standard dalam Pengamanan Data Penjualan Ramayana Department Store. Jurnal Riset Komputer.*
- UtamaPutraFerzha, WijayaGusman, Faurina Ruvita, & VatresiaArie. (2023). Implementasi Algoritma AES 256 CBC, BASE 64, Dan SHA 256*

*Dalam Pengamanan Dan Validasi Data Ujian Online. Jurnal Teknologi Informasi dan Ilmu Komputer.*

*WidodoEstuBerita , & PurnomoSidiqA. (2020). Implementasi Advanced Encryption Standard Pada Enkripsi Dan Dekripsi Dokumen Rahasia Diintelkam Polda DIY. Jurnal Teknik Informatika.*

*WIjayaHamid. (2020). Implementasi Kriptografi AES-128 Untuk Mengamankan url (UNIFORM RESOURCE LOCATOR) Dari Sql Injection. Jurnal Akademika .*





**LAMPIRAN – LAMPIRAN**





**PT. NADIRA FARMASI MULYA**

Jl. KH. Hasyim Ashari No. 10, Sudirman Ploang  
Kota Tangerang, Telp: 021 7307523, 7307688  
www.apotekermulya.com

## SURAT KETERANG RISET

012/KM/SKR/1/2024

Yang bertanda tangan di bawah ini

Nama : Andy Novlandy  
Jabatan : HRD & Adm. Kantor  
Klinik Mulya

Menerangkan bahwa :

Nama : R.M. Hilmy Hermadi  
NIM : 1811501798

Telah melaksanakan riset di Klinik Mulya sejak tanggal 1 September 2023 sampai dengan  
15 Januari 2024 dengan baik

Demikian surat keterangan ini dibuat untuk dapat dipergunakan semestinya

Dibuat di : Tangerang

Tanggal : 19 Januari 2024

Klinik Mulya



Andy Novlandy  
HRD & Adm. Kantor