Jurnal Indonesia : Manajemen Informatika dan Komunikasi
www.journal.amikindonesia.ac.id/jimik/ Vol 4 No 3, September (2023)
E-ISSN: 2723-7079, P-ISSN: 2776-8074

TATA KELOLA REKAM MEDIS BERBASIS TEKNOLOGI INFORMASI DALAM PENANGANAN KERAHASIAAN DAN KEAMANAN DATA PASIEN DENGAN METODE KRIPTOGRAFI

Aellen Sarce Joel [1*], Falaah Abdussalaam [2], Yuyun Yunengsih [3].

[1*,3] Program Studi Manajemen Informasi Kesehatan, Politeknik Piksi Ganesha, Kota Bandung, Provinsi Jawa Barat, Indonesia.
[2] Program Studi Manajemen Informatika, Politeknik Piksi Ganesha, Kota Bandung, Provinsi Jawa Barat, Indonesia.

Corresponding Email: piksi.aellensarce@gmail.com [1*]

Histori Artikel:
Dikirim 20 Mei 2023; *Diterima dalam bentuk revisi* 10 Juni 2023; *Diterima* 1 Juli 2023; *Diterbitkan* 10 September 2023.

Abstrak

Kerahasiaan dan keamanan data pasien di rumah sakit adalah hal yang sangat penting dan wajib adanya perlindungan data-data. Dalam penelitian ini ditemukan permasalahan yaitu belum adanya jaminan perlindugan keamanan dan kerahasiaan data pasien yang memungkinkan data tersebut bisa bocor. Penelitian ini bertujuan untuk merancang sistem tata kelola rekam medis berbasis teknologi informasi untuk menjaga kerahasiaan dan keamanan data pasien. Teknik penelitian menggunakan metodologi kualitatif dengan pendekatan deskriptif dan mengumpulkan data melalui observasi, wawancara dan studi literatur. Sedangkan metode waterfall digunakan untuk mengembangkan sistem melalui tahapan analisis kebutuhan, perancangan, implementasi dan pengujian. Perancangan sistem dilakukan dengan menggunakan Microsoft Visual Studio 2010 yang diimplementasikan dengan menggunakan kriptografi algoritma AES (Advanced Encryption Standard) Rijndael. Hasil dari penelitian yang sudah dilakukan ini didapatkan bahwa dengan adanya tata kelola rekam medis berbasis teknologi informasi dalam penanganan kerahasiaan dan keamanan data pasien menggunakan kriptografi AES dapat meningkatkan kerahasiaan dan keamanan data pasien dalam pengelolaan rekam medis.

Kata Kunci: Advanced Encryption Standard; Kriptografi; Rekam Medis; Teknologi Informasi.

Abstract

Confidentiality and security of patient data in hospitals is very important and data protection is mandatory. In this study, a problem was found, namely that there was no guarantee of protecting the security and confidentiality of patient data which allowed the data to leak. This study aims to design an information technology-based medical record governance system to maintain the confidentiality and security of patient data. The research technique uses a qualitative methodology with a descriptive approach and collects data through observation, interviews and literature studies. While the waterfall method is used to develop the system through the stages of needs analysis, design, implementation and testing. The system design was carried out using Microsoft Visual Studio 2010 which was implemented using the AES (Advanced Encryption Standard) Rijndael cryptography algorithm. The results of the research that has been done are obtained that the existence of information technology-based medical record governance in handling the confidentiality and security of patient data using AES cryptography can increase the confidentiality and security of patient data in medical record management.

Keyword: Advanced Encryption Standard; Cryptography; Medical Records; Information Technology.

1. Pendahuluan

Berkembangnya informasi dan teknologi telah mengubah cara kita hidup dan bekerja dalam segala hal, termasuk dalam bidang kesehatan yang sangat terpengaruh oleh teknologi informasi [1]. Seiring dengan kemajuan teknologi informasi di rumah sakit menjadi suatu kebutuhan dalam pengelolaan data dan informasi pasien. Teknologi informasi dapat mempermudah akses dan penggunaan data pasien secara cepat dengan memanfaatkan Sistem Informasi Manajemen Rumah Sakit (SIMRS) dalam mengelola data pasien salah satunya Rekam Medis [2]. Disamping kemajuan teknologi informasi untuk melakukan komunikasi dan pertukaran informasi. Perkembangan teknologi juga menciptakan tantangan dalam pengelolaan data dan informasi pasien yang sensitive dan bersifat pribadi. Pentingnya untuk memastikan keamanan dan kerahasiaan data pasien dalam penggunaan teknologi kesehatan [3].

Keamanan data adalah suatu proses perlindungan data akses yang tidak aman [4]. Keamanan data melibatkan serangkaian tindakan teknis dan prosedural untuk melindungi informasi dari ancaman keamanan peretasan sistem oleh orang yang tidak berwenang. Jaminan keamanan data pasien meliputi berbagai aspek, seperti keamanan jaringan, keamanan akses, enkripsi data serta manajemen identitas dan akses pengguna. Data rekam medis ini bersifat rahasia sehingga memerlukan pengamanan terhadap data-data penting terkait identitas, hasil pemeriksaan, pengobatan dan juga catatan tentang kondisi pasien.

Kriptografi adalah salah satu teknologi utama dalam sistem yang menjamin keamanan data pasien, memastikan data pasien terenkripsi dan hanya dapat diakses oleh pihak tertentu. Kriptografi ialah teknologi yang mengenkripsi untuk membuatnya tidak dapat dibaca oleh siapapun yang tidak berkepentingan, sehingga menjaga kerahasiaan dan keamanan data [5]. AES *(Advanced Encryption Standard)* ialah algoritma kriptografi simetris yang digunakan untuk mengamankan data dalam sistem komputer. Pada tahun 2001 AES diadopsi pertama kali sebagai standar enkripsi federal oleh *National Intitute of Standards and Technology (NIST)*. AES menggunakan kunci simetris untuk enkripsi dan menjelaskan data berbasis *chipper* blok dengan ukuran kunci dapat bervariasi dari 128, 192, hingga 256, semakin panjang kunci semakin sulit bagi pihak yang tidak berwenang untuk mendeskripsi data yang terenkripsi [6].

Penelitian sebelumnya yang pernah dilakukan terkait dengan keamanan data kriptografi yaitu oleh Valdho Falensky & Ineke Pakereng (2022) yang membahas tentang masalah tentang kurangnya perhatian dalam keamanan data pasien pada sistem yang ada di Puskesmas Pujon Kalimantan Tengah, penelitian tersebut menggunakan Kriptografi Super Enkripsi [7]. Selanjutnya penelitian oleh Listiani *et al*., (2022) membahas tentang tidak adanya keamanan data untuk melindungi pencurian data dan perubahan *database* yang berisi sistem informasi dan membutuhkan aplikasi yang lebih baik, penelitian tersebut menggunakan metode Kriptogarfi *Rivest Shamir Adleman* (RSA) [8]. Penelitian selanjutnya terkait pengamanan data menggunakan kriptografi dilakukan oleh Kandokang *et al*., (2023) dengan hasil kesimpulan yang didapat yaitu sistem pengamanan data pasien yang dirancang menggunakan UML, sistem dapat melakukan proses enkripsi dan deskripsi yang akan ditampilkan dalam *form* rekam medis pada sistem [9]. Penelitian oleh Ridho *et al*., (2023) dengan permasalahan bahwa dalam pelaksanaan pendataan pasien masih dikerjakan dengan manual dan belum menggunakan algoritma kriptografi Caesar Cipher, setelah dilakukan analisis dan perancangan sistem tersebut sistem yang dibangun dengan aplikasi *Visual Basic* hal ini dapat memfasilitasi mekanisme kerja pemrosesan data klinis, dan berkontribusi untuk meningkatkan akurasi dan efisiensi [10].

Tata kelola rekam medis berbasis teknologi merupakan suatu pendekatan penggunaan teknologi informasi dan komunikasi untuk mengelola informasi medis pasien secara elektronik. Tujuan dari tata kelola rekam medis ini ialah untuk meningkatkan efisiensi dan juga akurasi dalam pengelolaan iinformasi medis serta dapat meningkatkan kualitas layanan kepada pasien. Rumah Sakit Umum (RSUD) Al-Ihsan Bandung merupakan rumah sakit yang sudah menerapkan teknologi informasi untuk menunjang pelayanan. Sebagai rumah sakit yang melayani pasien, Rumah Sakit ini memiliki tanggung jawab untuk menjaga keamanan dan kerahasiaan data pasien. Beberapa permasalahan yang mungkin timbul yaitu, adanya risiko kebocoran data, penyalahgunaan data, keterbatasan infrastruktur

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 837-848
DOI : https://doi.org/10.35870/jimik.v4i3.287

keamanan, dan kurangnya kesadaran tentang keamanan data pasien. Berdasarkan pada penelitian terdahulu dan juga permasalahan yang akan timbul penelitian ini berfokus pada Tata Kelola Rekam Medis Berbasis Teknologi Informasi Dalam Penanganan Kerahasiaan dan Keamanan Data Pasien. Dengan merancang sistem informasi yang dilengkapi dengan enkripsi dan deskripsi agar data pasien tidak dapat dilihat oleh sembarang orang.

2. Metode Penelitian

Ini adalah pendekatan atau rencana sistematis yang digunakan untuk mengancam, melakukan, dan menganalisis penelitian. Untuk memastikan bahwa penelitian dilakukan dengan benar dan data yang diperoleh valid dan reliabel. Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif berdasarkan fenomena langsung di Rumah Sakit Al-Ihsan, selain itu model waterfall digunakan sebagai metode untuk mengembangkan dan merancang sistem informasi. Berikut ini merupakan teknik pengumpulan data yang dilakukan yaitu:

1) Observasi
   Proses yang bertujuan menelaah atau mengumpulkan informasi tentang suatu fenomena. Proses ini dilakukan dengan cara meninjau langsung ke sistem yang sedang diterapkan di Rumah Sakit Al-Ihsan untuk memenuhi kebutuhan bahan informasi yang dibutuhkan di penelitian ini.
2) Wawancara
   Proses wawancara meliputi kegiatan dengan mengajukan beberapa pertanyaan kepada petugas rekam medis di rumah sakit tentang bagaimana upaya dalam menjaga keamanan dan kerahasiaan data pasien.
3) Studi Literatur
   Proses ini melibatkan pengumpulan informasi dan data dari berbagai sumber, termasuk jurnal, artikel, dan penelitian sebelumnya yang diperlukan untuk melakukan penelitian ini. Hal ini dilakukan untuk memperoleh sumber informasi terkait dengan kriptografi AES.

2.1 Metode Pengembangan Sistem

Dalam melakukan perancangan dan pengembangan sistem pengamanan data pasien di Rumah Sakit Al-Ihsan yaitu dengan menggunakan metode *waterfall*. Metode ini terdiri dari serangkaian fase yang berurutan. Dalam konteks kriptografi metode *waterfall* dapat digunakan untu merancang dan mengembangkan sistem keamanan informasi. fase-fase yang terdapat pada metode *waterfall* dapat diadaptasi sebagai berikut :

1) Analisis Kebutuhan
   Pada fase atau tahap ini peneliti harus melakukan analisis kebutuhan terkait dengan sistem keamanan informasi yang akan dirancang. Termasuk dalam mengidentifikasi kebutuhan keamanan dan privasi yang diinginkan oleh pengguna sistem, jenis data yang akan disimpan, serta jenis ancaman keamanan yang muncul. Analisis kebutuhan ini akan menjadi dasar dalam merancang sistem keamanan informasi yang memenuhi kebutuhan pengguna..
2) Perancangan
   Pada fase ini akan merancang sistem keamanan infomasi berdasarkan hasil analisis kebutuhan pada fase sebelumnya. Perancangan ini memiliki teknik kriptografi yang akan digunakan, desain algoritma kriptografi, pemilihan protocol komunikasi dan pengaturan kunci enkripsi yang akan digunakan untuk menjaga kerahasiaan data pasien.
3) Implementasi
   Pada fase ini sistem keamanan informasi yang telah dirancang pada fase sebelumnya diimplementasikan dalam bentuk aplikasi atau sistem. Fase ini harus memastikan bahwa sistem keamanan informasi yang dihasilkan sesuai dengan desain yang telah dirancanng pada fase sebelumnya.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 837-848
DOI : https://doi.org/10.35870/jimik.v4i3.287

4) Pengujian
Fase ini melibatkan pengujian untuk memastikan bahwa sistem keamanan informasi yang telah terpasang beroperasi dengan baik sesuai dengan persyaratan keamanan dan kerahasiaan yang telah ditetapkan sebelumnya. Tujuan dari pengujian ini adalah untuk memverifikasi dan menguji keefektifan sistem keamanan.

Dengan menerapkan metode *waterfall* dalam perancangan dan pengembangan sistem informasi dengan kriptografi diharapkan dapat memastikan bahwa sistem keamanan informasi yang dihasilkan terstruktur, sistematis dan dapat memenuhi kebutuhan keamanan dan kerahasiaan.

2.2 *Algoritma Advanced Encryption Standard (AES)*

Algoritma AES ialah implementasi dari algoritma kriptografi blok *cipher* yang disebut Rijndael. AES mengenkripsi data menjadi blok-blok kecil mengubah blok-blok tersebut menjadi blok-blok terenkripsi dengan menggunakan operasi substitusi, pergeseran, dan percampuran pada setiap blok [11]. Setiap blok data terdiri dati matriks 4x4 yang disebut dengan state, dan seluruh proses enkripsi dan deskripsi data dijalankan pada state tersebut. Rumus kriptografi AES Rijndael memproses blok-blok data dalam ukuran yang sama dan menghasilkan keluaran enkripsi yang sesuai. Dengan panjang kunci yang bervariasi dari 128 bit, 192 bit, 256 bit. Algoritma ini menggunakan penggabungan substitusi, pergeseran, dan operasi XOR yang berulang untuk menghasilkan enkripsi yang sangat aman dan efektif.

3. Hasil dan Pembahasan

3.1. Analisis Kebutuhan

Analisis kebutuhan untuk tata kelola rekam medis berbasis teknologi informasi dalam penanganan keamanan dan kerahasiaan dengan metode kriptografi yaitu,

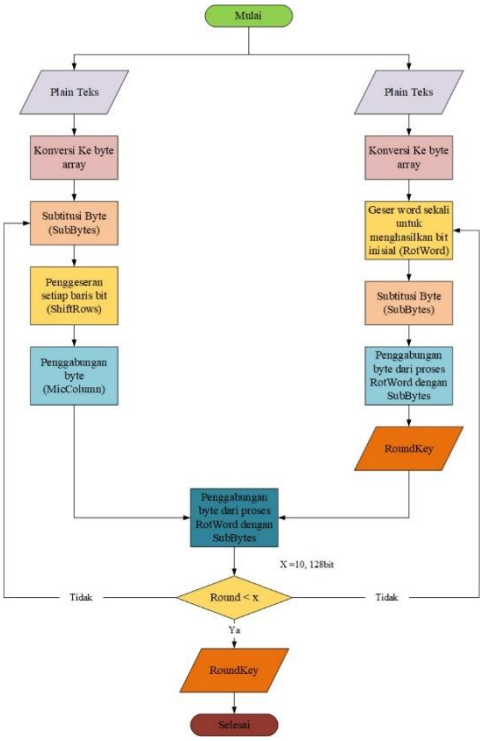
1) sistem manajemen basis data untuk penyimpanan dan pengelolaan rekam medis pasien yang berisi data terkait pasien dengan enkripsi kriptografi AES.
2) Perancangan algoritma kriptografi AES yang aman dan efisien untuk melindungi data pasien yang sensitive.
3) Pengembangan sistem manajemen kunci yang aman untuk memastikan keamanan enkripsi dan deskripsi data pasien.

Hasil analisis kebutuhan harus dapat digunakan sebagai landasan untuk merancang dan mengembangkan sistem tata kelola rekam medis berbasis teknologi informasi yang efektif, aman dan sesuai dengan kebutuhan pengguna.

3.2. Perancangan Sistem

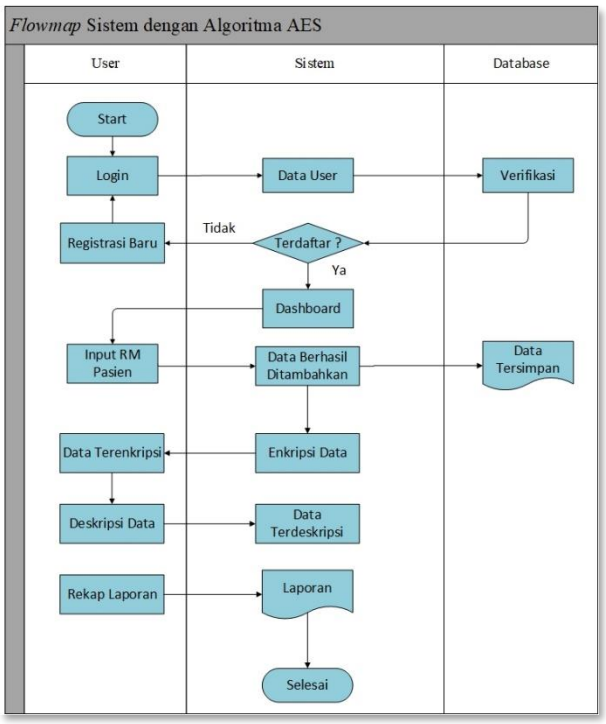
Dengan menggunakan algoritma AES *(Advanced Encryption Standard)* yang digunakan untuk melindungi data dengan kunci simetris. Perancangan ini dibuat menggunakan *Microsoft Visual Studio* dengan menggunakan algoritma AES untuk mengenkripsi dan mendeskripsi data-data. Algoritma AES diimplementasikan untuk pengamanan data. Untuk memulai proses enkripsi siapkan 2 buah *array* berukuran 4x4 yaitu *plaintext* dan *key*. Kemudian *Plaintext* dan *key* tersebut diubah kedalam bentuk bit menggunakan kode ASCII. Perancangan sistem ini bertujuan untuk menjelaskan mengenai sistem informasi yang akan dirancang dengan menggunakan bantuan tools *flowchart, flowmap,* diagram konteks, DFD sebagai berikut:

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 837-848
DOI : https://doi.org/10.35870/jimik.v4i3.287



Gambar 1. *Flowchart* AES

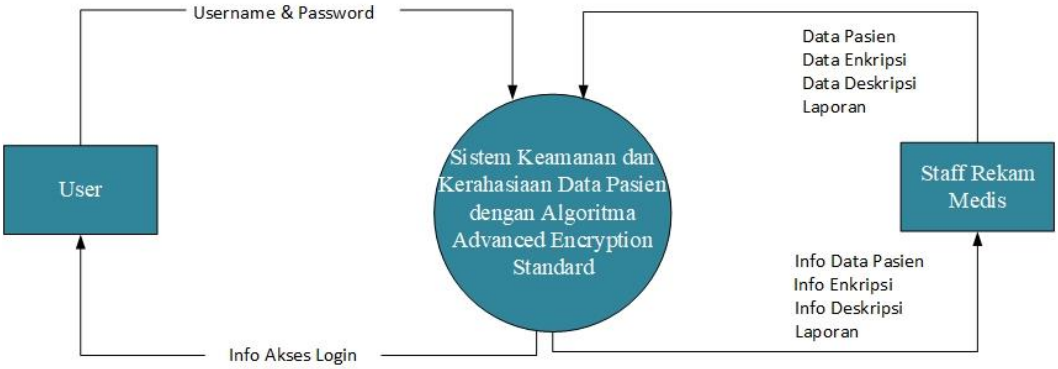
1) *Flowmap* Sistem



Gambar 2. *Flowmap* Sistem Algoritma AES

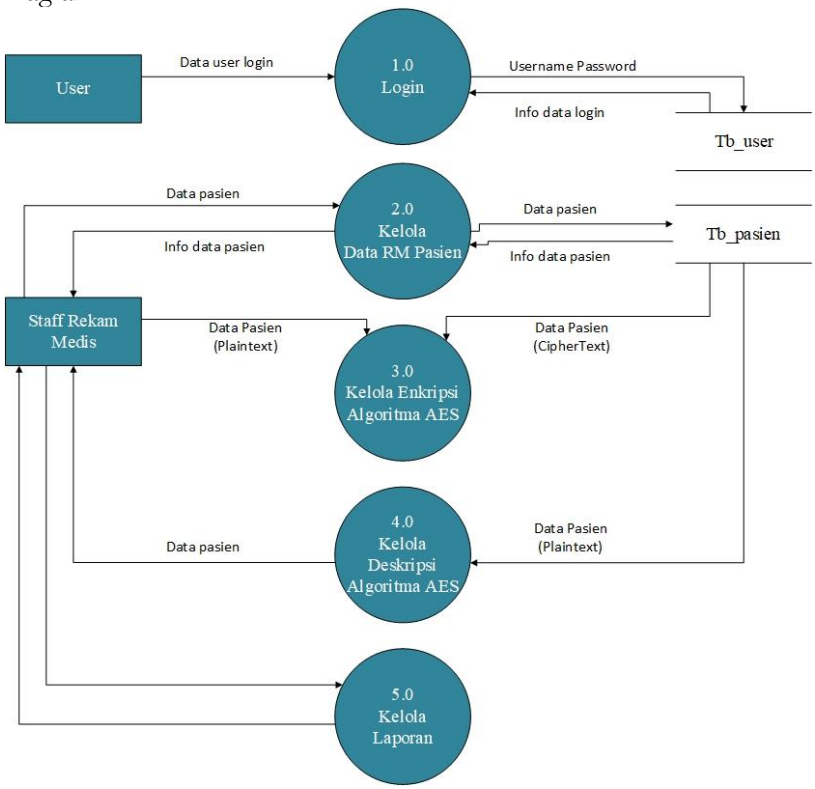
Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 837-848
DOI : https://doi.org/10.35870/jimik.v4i3.287

2) Diagram Konteks



Gambar 3. Diagram Konteks

3) Data Flow Diagram



Gambar 4. Data Flow Diagram

4) Proses Enkripsi

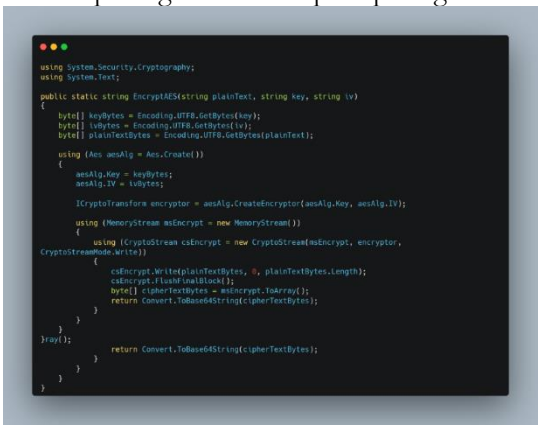
Proses enkripsi AES terdiri beberapa ronde yaitu Sub Bytes, Shift Rows, Mix Column, dan Add Round Key. Proses ronde tersebut akan terus diulang sebanyak 9 atau 11 kali tergantung pada panjang kunci enkripsi (128-bit, 192-bit, atau 256-bit) setelah ronde terakhir selesai, matriks state yang terakhir akan dienkripsi dengan kunci enkripsi terakhir untuk menghasilkan keluaran enkripsi. Langkah-langkah cara enkripsi AES:

a) Pilih kunci enkripsi yang akan digunakan, lalu buat kunci ekspansi dari kunci enkripsi tersebut.
b) Tentukan *plaintext* yang akan dienkripsi
c) Tambahkan padding (bila diperlukan) agar ukuran *plaintext* menjadi kelipatan 128 bit.
d) Buatlah vector inisialisasi (IV) dengan panjang 128 bit.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 837-848
DOI : https://doi.org/10.35870/jimik.v4i3.287

e) Bagi *plaintext* menjadi blok-blok dengan panjang 128 bit.
f) Lakukan enkripsi pada setiap blok *plaintext* menggunakan kunci ekspansi AES dan IV.
g) Gabungkan hasil enkripsi setiap blok menjadi *chipphertext*.
h) Simpan kunci enkripsi dan IV untuk melakukan deskripsi.

Ilustrasi proses enkripsi AES dapat digambarkan seperti pada gambar dibawah ini.



```
using System.Security.Cryptography;
using System.Text;

public static string EncryptAES(string plainText, string key, string iv)
{
    byte[] keyBytes = Encoding.UTF8.GetBytes(key);
    byte[] ivBytes = Encoding.UTF8.GetBytes(iv);
    byte[] plainTextBytes = Encoding.UTF8.GetBytes(plainText);

    using (Aes aesAlg = Aes.Create())
    {
        aesAlg.Key = keyBytes;
        aesAlg.IV = ivBytes;

        ICryptoTransform encryptor = aesAlg.CreateEncryptor(aesAlg.Key, aesAlg.IV);

        using (MemoryStream msEncrypt = new MemoryStream())
        {
            using (CryptoStream csEncrypt = new CryptoStream(msEncrypt, encryptor,
CryptoStreamMode.Write))
            {
                csEncrypt.Write(plainTextBytes, 0, plainTextBytes.Length);
                csEncrypt.FlushFinalBlock();
                byte[] cipherTextBytes = msEncrypt.ToArray();
                return Convert.ToBase64String(cipherTextBytes);
            }
        }
    }
}rray();

                return Convert.ToBase64String(cipherTextBytes);
            }
        }
    }
}
```

Gambar 5. Ilustrasi Proses Enkripsi

5) Proses Deskripsi

Proses deskripsi AES Rijndael mirip dengan proses enkripsi hanya saja Langkah-langkah dilakukan secara terbalik. Dalam proses deskripsi, keluaran enkripsi akan diinisialisasi sebagai matriks state yang kemudian akan melalui ronde Sub Bytes, Shift Rows, Mix Column, dan Add Round Key dengan kunci deskripsi yang sama dengan kunci enkripsi. Proses ini akan diulang sebanyak 9 atau 11 kali tergantung panjang kunci, hingga matriks state terakhir yang dihasilkan adalah blok data asli. Di bawah ini ilustrasi proses deskripsi

```
using System;
using System.Security.Cryptography;

class Program
{
    static void Main(string[] args)
    {
        string plaintext = "hello world";
        string key = "mysecretkey";

        string encrypted = Encrypt(plaintext, key);
        Console.WriteLine("Encrypted text: " + encrypted);

        string decrypted = Decrypt(encrypted, key);
        Console.WriteLine("Decrypted text: " + decrypted);
    }

    static string Encrypt(string plaintext, string key)
    {
        byte[] plaintextBytes = System.Text.Encoding.UTF8.GetBytes(plaintext);
        byte[] keyBytes = System.Text.Encoding.UTF8.GetBytes(key);

        Aes aes = Aes.Create();
        aes.Mode = CipherMode.CBC;
        aes.Padding = PaddingMode.PKCS7;
        aes.Key = keyBytes;
        aes.IV = keyBytes;

        ICryptoTransform encryptor = aes.CreateEncryptor();
        byte[] encryptedBytes = encryptor.TransformFinalBlock(plaintextBytes, 0, plaintextBytes.Length);

        return Convert.ToBase64String(encryptedBytes);
    }

    static string Decrypt(string encryptedText, string key)
    {
        byte[] encryptedBytes = Convert.FromBase64String(encryptedText);
        byte[] keyBytes = System.Text.Encoding.UTF8.GetBytes(key);

        Aes aes = Aes.Create();
        aes.Mode = CipherMode.CBC;
        aes.Padding = PaddingMode.PKCS7;
        aes.Key = keyBytes;
        aes.IV = keyBytes;

        ICryptoTransform decryptor = aes.CreateDecryptor();
        byte[] decryptedBytes = decryptor.TransformFinalBlock(encryptedBytes, 0, encryptedBytes.Length);

        return System.Text.Encoding.UTF8.GetString(decryptedBytes);
    }
}
```

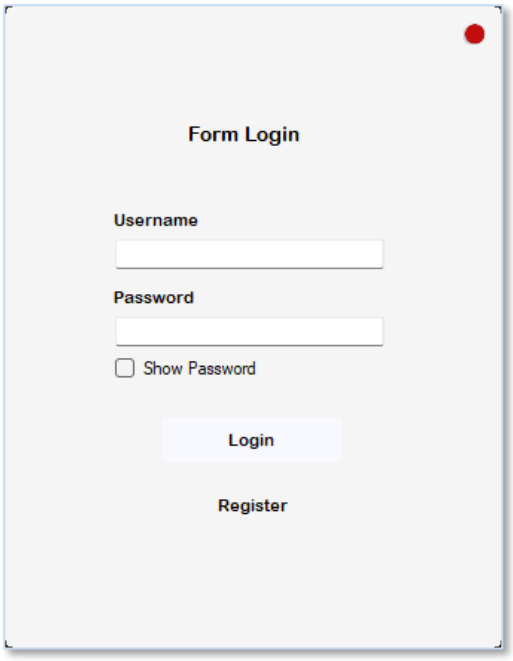
Gambar 6. Ilustrasi Proses Deskripsi

6) Implementasi Interface

Implementasi algoritma AES *(Advanced Encryption Standard)* Rijndael dibuat menggunakan *Microsoft Visual Studio* 20120. Aplikasi yang dibuat ini terdiri dari :

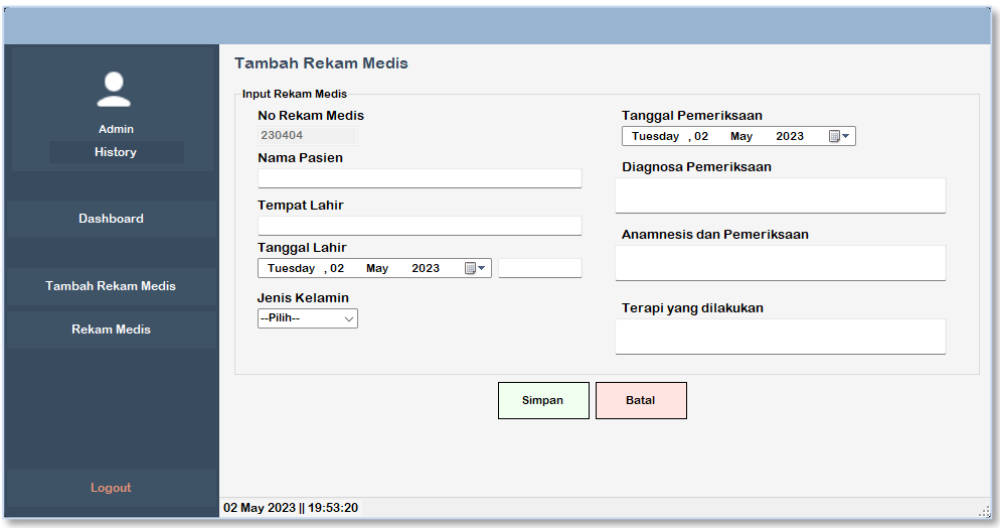
Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 837-848
DOI : https://doi.org/10.35870/jimik.v4i3.287

Tampilan *login* ini merupakan proses awal untuk mengakses aplikasi ini. Orang yang bisa mengakses ini adalah orang yang berwenang saja seperti petugas perekam medis. Setelah berhasil masuk dan memasukkan nama pengguna dan kata sandi, Anda akan melihat halaman utama.



Gambar 7. Tampilan *Login*

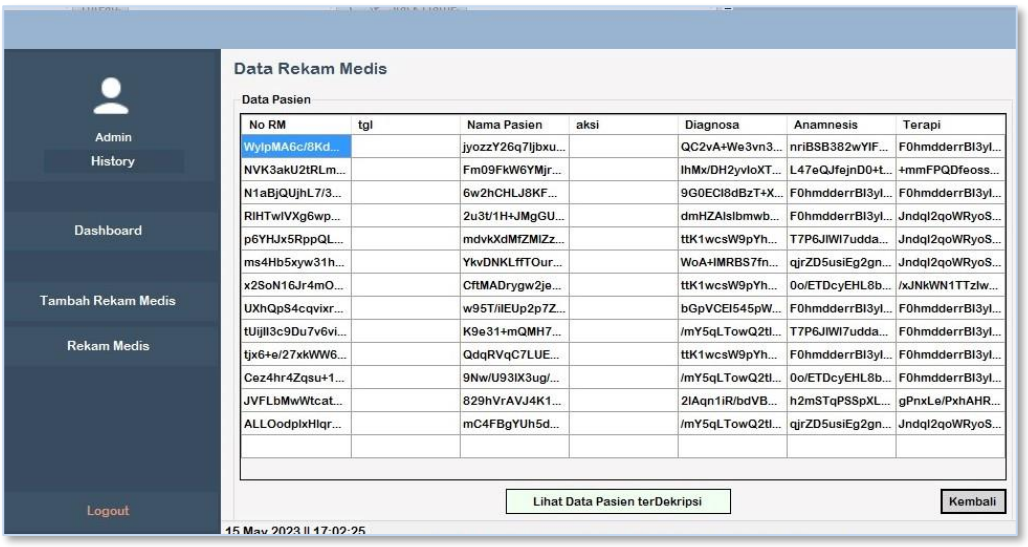
Tampilan form rekam medis untuk memasukkan dan menyimpan data rekam medis pasien, meliputi nomor rekam medis, nama pasien, tempat lahir, tanggal lahir, jenis kelamin, tanggal pemeriksaan, diagnosa pemeriksaan, riwayat penyakit, detail pemeriksaan dan detail pengobatan.



Gambar 8. Tampilan *Form* Data Rekam Medis

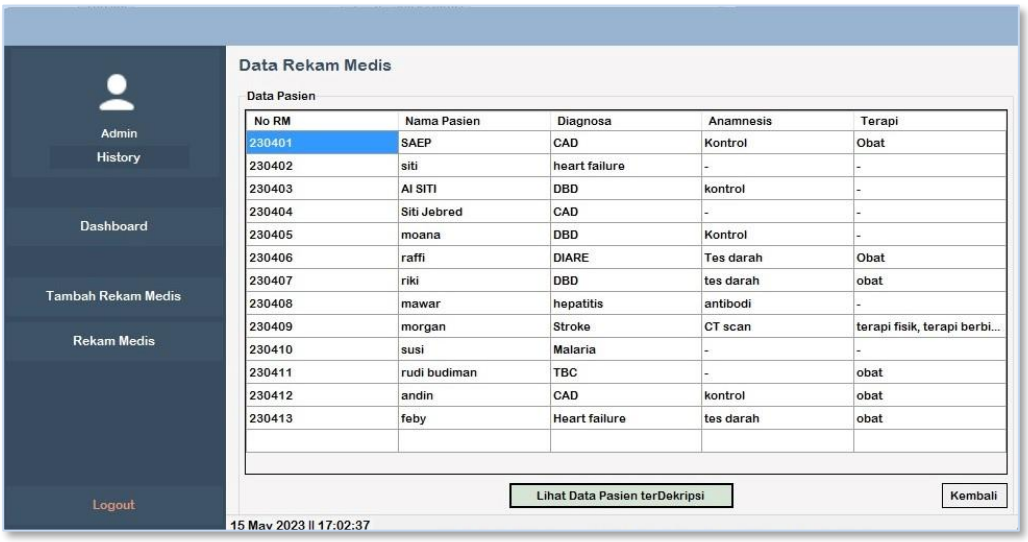
Setelah isi data rekam medis pasien tersimpan, maka dengan otomatis sistem ini langsung memproses enkripsi data dengan menggunakan algoritma AES Rijndael ini data-data pasien akan langsung terenkripsi seperti pada gambar di bawah ini.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 837-848
DOI : https://doi.org/10.35870/jimik.v4i3.287



Gambar 9. Tampilan Hasil Enkripsi Data Pasien

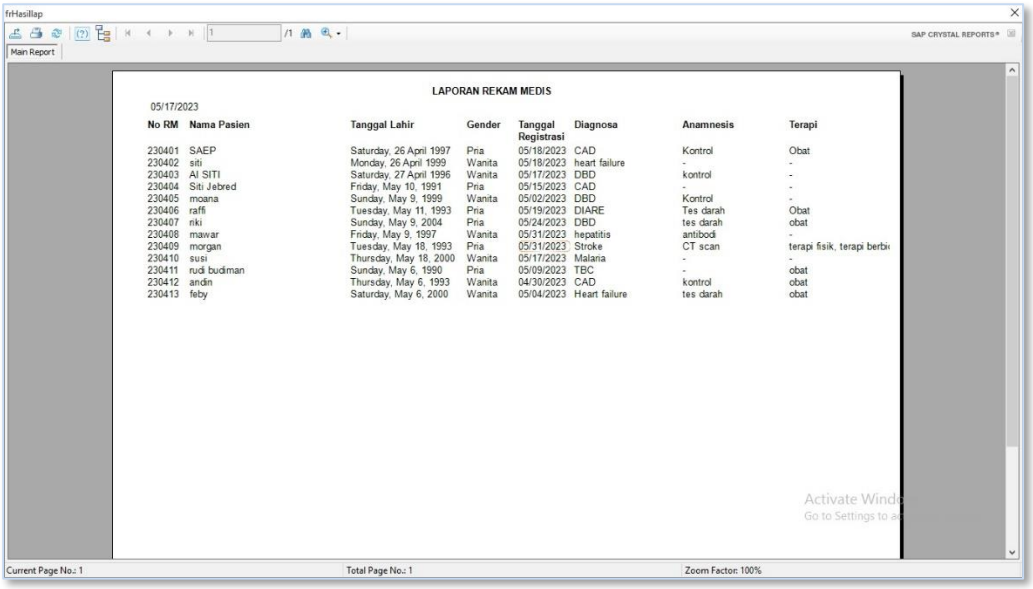
Apabila petugas perekam medis membutuhkan data-data rekam medis pasien maka harus dideskripsikan terlebih dahulu yang tadinya tidak dapat terbaca, setelah dideskripsikan maka akan muncul semua data-data pasien, seperti pada gambar 7 ini.



Gambar 10. Tampilan Hasil Deskripsi Data Pasien

Tampilan Laporan ini merupakan *output* dari sistem informasi yang telah dibuat, laporan ini dapat dicetak. Seperti pada gambar di bawah ini.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 837-848
DOI : https://doi.org/10.35870/jimik.v4i3.287



Gambar 11. Tampilan Laporan

7) Pengujian Sistem

Langkah pengujian ini dilakukan untuk memastikan bahwa sistem yang dibuat dapat berfungsi dengan sebagaimana mestinya. Sistem yang dibuat ialah bagaimana data rekam medis yang tersimpan akan terenkripsi dengan benar sesuai dengan algoritma yang digunakan sehingga data tidak akan terbaca oleh siapapun kecuali petugas yang berwenang dan dapat dideskripsikan kembali agar data dapat terbaca.

ID	Deskripsi Pengujian	Hasil yang diharapkan	Hasil Pengujian	Kesimpulan
A01	Masukkan nama pengguna dan kata sandi Anda dengan benar	Sistem yang akan muncul adalah menu halaman utama	Sistem menampilkan menu halaman utama	Sesuai
A02	Masukkan nama pengguna dan kata sandi Anda dengan salah	Sistem menolak akses masuk dan meminta nama pengguna dan kata sandi.	Sistem meminta Anda memasukkan nama pengguna dan kata sandi	Sesuai
B01	Mengisikan isian dengan data rekam medis pasien	Sistem yang menampilkan pesan bahwa data pasien telah berhasil disimpan	Sebuah pesan ditampilkan yang menyatakan bahwa data pasien telah berhasil disimpan	Sesuai
C01	Data yang tersimpan akan terenkripsi	Sistem akan menampilkan tampilan bahwa data rekam medis pasien tidak akan terbaca (terenkripsi)	Sistem menampilkan bahwa data pasien tidak dapat dibaca (terenkripsi)	Sesuai

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 837-848
DOI : https://doi.org/10.35870/jimik.v4i3.287

D01	Memilih data yang akan di deskripsikan	Sistem akan menampilkan data yang sudah di deskripsikan	Sistem menampilkan data yang berhasil di deskripsikan	Sesuai
E01	Mencetak laporan	Sistem menampilkan laporan untuk dicetak.	Sistem menampilkan laporan yang akan dicetak	Sesuai

Sistem yang dibuat berdasarkan pengujian ini dapat memenuhi kebutuhan pengguna yaitu, sistem dapat menyimpan dan mengelola data rekam medis pasien, hasil perancagan menggunakan algoritma AES Rijndael dapat melindungi data pasien yang sensitif, dan juga memastikan keamanan dan kerahasiaan data pasien.

4. Kesimpulan

Berdasarkan hasil dan pembahasan di atas, dapat disimpulkan bahwa penggunaan enkripsi AES dapat meningkatkan kerahasiaan dan keamanan data pasien dalam pengelolaan rekam medis dengan menerapkan tata kelola rekam medis berbasis teknologi informasi untuk menangani kerahasiaan dan keamanan data pasien. Penggunaan enkripsi AES telah terbukti dapat melindungi data pasien. Penggunaan teknologi informasi juga dapat memfasilitasi pengelolaan rekam medis yang efisien dan akurat.

5. Daftar Pustaka

[1] Cholik, C. A. (2021). PERKEMBANGAN TEKNOLOGI INFORMASI KOMUNIKASI / ICT DALAM BERBAGAI BIDANG. *Jurnal Fakultas Teknik*, *2*(2), 39–45. https://jurnal.unisa.ac.id/index.php/jft/article/view/83

[2] Wulandari, T., & Putra, D. M. (2020). Study Literature Riview Tentang Implementasi Pada Unit Keja Rekam Medis Rawat Jalan Dengan Metode HOT - Fit. *Jurnal Administrasi Dan Informasi Kesehatan*, *1*(2), 157–170. http://ojs.stikeslandbouw.ac.id/index.php/ahi/article/view/167

[3] Suci, N. N., Nugroho, N. B., & Murniyanti, S. (2018). Implementasi Kriptografi Untuk Keamanan Data Rekam Medis Di Klinik Pratama Siti Rahmah Menggunakan Metode Advanced Encryption Standard. *Jurnal Cyber Tech*, *1*(10), 1–13. https://ojs.trigunadharma.ac.id/index.php/jct/article/view/3622

[4] Pratiwi, R., Utami, L. C., Sakti, R. B., & Triase. (2022). Perancangan Keamanan Data Pesan Dengan Menggunakan Metode Kriptografi Caesar Cipher. *Bulletin of Information Technology …*, *3*(4), 367–373. https://doi.org/https://doi.org/10.47065/bit.v3i4.420

[5] Hulu, D., Nadeak, B. D., & Aripin, S. (2020). Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan. *KOMIK (Konferensi …*, *4*, 78–86. https://doi.org/10.30865/komik.v4i1.2590

[6] Permana, A. A., & Nurnaningsih, D. (2018). Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes). *Jurnal Teknik Informatika*, *11*(2), 177–186. https://doi.org/10.15408/jti.v11i2.7811

[7] Valdho Falensky, L., & Ineke Pakereng, M. A. (2022). Pengamanan Data Pasien Di UPT. Puskesmas Pujon Kalimantan Tengah Menggunakan Kriptografi Super Enkripsi. *Jurnal Sains Komputer & Informatika (J-SAKTI*, *6*(2), 711–725. https://doi.org/http://dx.doi.org/10.30645/j-sakti.v6i2.484

[8] Listiani, I., Nasution, M. S., Sari, W. I., & Nasution, A. B. (2022). Perancangan Keamanan Data Pasien Di Klinik Kecantikan Ratu Beauty Studio Menggunakan Metode Kriptografi RSA. *Jurnal Informatika Teknologi Dan Sains*, *4*(4), 437–443. https://doi.org/10.51401/jinteks.v4i4.2173

[9] Kandokang, L. R., Pekuwati, A. A., & Lede, P. A. L. (2023). PERANCANGAN SISTEM PENGAMANAN DATA PASIEN MENGGUNAKAN METODE KRIPTOGRAFI VIGENÈRE CIPHER. *SATI: Sustainable Agricultural Technology Innovation*, 1–9. https://ojs.unkriswina.ac.id/index.php/semnas-FST/article/view/385

[10] Ridho, R., Bisri, C., & Harahap, A. M. (2023). Penerapan Kriptografi Enkripsi Dan Deskripsi Dalam Pendataan Pasien Klinik Mama Harfas Tembung Menggunakan Visual Basic. *Jurnal Penelitian Dan …*, *2*(1), 30–33. https://doi.org/https://doi.org/10.47233/jppie.v2i1.676

[11] Ferdiansyah, Id Hadiana, A., & Rakhmat Umbara, F. (2021). Penggunaan QR Code Berbasis Kriptografi Algoritma AES (Advanced Encryption Standard) Untuk Administrasi Rekam Medis. *Journal of Information Technology*, *3*(2), 20–27. https://doi.org/10.47292/joint.v3i2.64.