KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)
Volume 4, Nomor 1, Oktober 2020
DOI: 10.30865/komik.v4i1.2590
ISSN 2597-4645 (media online)
ISSN 2597-4610 (media cetak)
Page: 78-86

Implementasi Algoritma AES (*Advanced Encryption Standard*) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan

Delisman Hulu, Berto Nadeak, Soeb Aripin*

[1] Fakultas Ilmu Komputer dan Teknologi Informasi, Program Studi Teknik Infirmatika, Universitas Budi Darma, Medan, Indonesia
Email: delishulu@gmail.com
*) Email Penulis Korespondensi

Abstrak−Keamanan suatu data sangatlah penting bagi semua pengguna sebuah sistem informasi, belakangan ini kriptografi menjadi metode yang digunakan dalam mengamankan data. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika dalam mengamankan suatu informasi atau pesan asli (*Plainteks*) menjadi sebuah teks tersembunyi (*Chiperteks*) dan kemudian di ubah menjadi pesan asli kembali. Kriptografi mempunyai tiga unsur penting yaitu pembangkitan kunci, enkripsi dan deskipsi. Dalam kriptografi di kenal algoritma block chiper yang didalamnya terdapat AES (*Anvanced Encyption Standard*) merupakan bagian dari Modern Symmetric Key Cipher, algoritma ini menggunakan kunci yang sama pada saat proses enkripsi dan deskripsi sehingga data yang kita miliki akan sulit dimengerti maknanya. Teknik algoritma tersebut digunakan untuk mengkonversi data dalam bentuk kode-kode tertentu, untuk tujuan agar informasi yang tersimpan tidak bisa di baca siapa pun kecuali orang-orang yang berhak. Oleh karena itu, sistem keamanan data sangat di perlukan dalam megirim hasil radiologi kepada pasien dikarenakan hasil radiologi bersifat rahasisa pasien.

Kata Kunci: Algoritma, AES, Enkripsi, Deskripsi, Kriptografi

Abstract−Data security is very important for all users of an information system, recently cryptography has become the method used in data. Cryptography is the study of mathematical techniques in an original information or message (plaintext) into a hidden text (Chipertext) and then converted into the original message again. Cryptography has three important elements, namely key generation, encryption and description. In cryptography, the block cipher algorithm is known, which includes AES (Advanced Encyption Standard) which is part of the Modern Symmetric Key Cipher, this algorithm uses the same key during the encryption and description processes so that the data we have will be difficult to cooperate with its meaning. The algorithmic technique is used to measure data in the form of certain codes, for the purpose of so that the stored information cannot be read by anyone except authorized people. Therefore, a data security system is needed in sending radiological results to patients because radiological results are confidential to patients.

Keywords: Algorithm, AES, Encryption, Description, Cryptography

1. PENDAHULUAN

Perkembangan digital saat ini bermunculan sebuah sistem canggih serta dapat memudahkan manusia dalam menyelesaikan pekerjaannya tanpa menghitung jarak dan waktu, perkembangan digital ini juga merambat diberabgai bidang baik instansi pemerintah maupun perusahaan swasta. Perkembangan suatu keamanan dalam menjaga suatu rahasia yang bersifat informasi atau data serta dapat dipertukarkan informasi yang sangat penting menimbulkan banyaknya tuntutan tersedianya suatu aplikasi yang mampu mengamankan data serta ancaman keamanan atau kebocoran data. Dengan adanya kemajuan tentang ilmu yang menjelaskan bagaimana langkah-langkah keamanan suatu sistem data merupakan suatu sisi positif serta mampu menyediakan suatu aplikasi keamanan data yang tujuannya untuk melindungi data yang ditrainsfer atau dikirimkan lewat jaringan telekomunikasi. Adapun ilmu yang mampu diterapkan serta lengkah-langkah bagaiaman cara pengamanan data atau yang biasa kita kenal kriptografi.

Sebelum menggunakan cara untuk keamanan sitem atau data perlu kita ketahui apa itu kriptografi murupakan ilmu yang mampu mempelajari cara-cara matematika yang berhubungan dengan tujuan keamanan suatu data dan informasi misalnya kebenaran data, mutu data dan keamanan data. Ilmu kriptografi yaitu salah satu fasilitas untuk mengerterjemahkan pesan jelas (*plainteks*) menjadi pesan yang telah kuncikan (*cipherteks*). Adapun langkah untuk melakukan suatu terjemahan disebut enkripsi (*encryption*) menerjemahkan cipherteks menjadi plainteks disebut dengan dekripsi (*decryption*) proses enkripsi dan dekripsi menggunakan kunci kriptografi [1].

Pada tahun 2000 *National institute of standards and technology* (NIST) menjadi salah satu agensi departemen perdagangan AS menetapkan sebuah acuan kriptografi yang baru yaitu Algoritma AES dan ditetapkan sebagai *Advanced Encryption Standard* (AES) [2]. AES secara umum dapat berfungsi diblok 128-bit atau 16 karakter, sehingga digunakan untuk enkripsi bentuk teks dan bentuk file dokumen yang bentuk teks dapat lebih berukuran lebih dari 16 karakter, akan tetapi AES dapat digunakan untuk keamanan atau kunci pada suatu objek yaitu dengan melakukan enkripsi simetri berbasis *cipher* blok dengan panjang kunci 128, 192 dan 256 bit berbentuk pararel agar memudahkan saat melakukan proses file yang dienkripsi dan dekripsi [2].

Sistem pengiriman hasil radiologi saat ini yang sedang berjalan masih manual atau proses konsultasi hasil radiologi harus berjumpa langsung kedokter spesialis radiologi atau hasil *print* foto *rontgen* diantar kedokternya untuk menentukan hasil pemeriksaan foto *rontgen* setiap pasien, hal ini dapat menghambat proses pengiriman foto *rontgen* dalam bentuk file *dicom* atau gambar (*jpg* dan *png*) namun penulis hanya menerapkan algoritma AES di file dalam bentuk *jpg* dan *png.* Hasil radiologi bersumber dari petugas radiologi dan melakukan pengiriman hasil kepada dokter. Oleh sebab itu membutuhkan suatu aplikasi keamanan pada file hasil radiologi yang mampu menjamin kerahasian dan keamanan file hasil radiologi agar hasil hanya dapat dibaca dokter atau tenaga medis yang terlibat, maka hal itu file

ISSN 2597-4645 (media online)
ISSN 2597-4610 (media cetak)
Page: 78-86

hasil radiologi harus di enrkispi menggunakan algoritma AES sehingga yang bisa melakukan deskripsi hanya yang memiliki kuncu atau password enkripsi.

2. METODE PENELITIAN

2.1 Metodologi Penelitian

Metodologi penelitian dilakukan supaya proses pelaksanaan penelitian ini dapat berjalan sesuai rencana dan tahapan sehingga memperoleh hasil yang diharapkan. Adapun motode yang ditetapkan pada penelitian skripsi ini yaitu sebagai berikut :

1. Studi Literatur
   Dalam tahapan ini dapat dilaksanakan tinjauan suatu jurnal, artikel, peneltian terdahulu sebagai bahan referensi yang dibutuhkan dalam melaksanakan penelitian ini, bertujuan hal ini dikerjakan agar mendapatkan suatu informasi yang berkaitan dengan algoritma AES serta bahasa pemrogramman php.
2. Perancangan dan Analisa
   Ditahapan ini difungsikan agar dapat mengatur data dari hasil literature yang kemudian dapat dilakukan sebuah analisa dan implementasi menggunakan salah satu algoritma AES dengan metode perancangan SDLC sehingga dapat menjadi sebuah sistem yang memiliki keamanan khusunya keamanan algoritma AES.
3. Impelemtasi
   Tahap ini algoritma AES dapat di implementasikan dalam pembuatan suatu sistem keamanan hasil dengan menggunakan bahasa pemrograman PHP dan menggunakan databse MySQL.
4. Pengujian
   Tahap pengujian ini melakukan uji coba apakah algoritma AES sudah berjalan dengan baik serta tidak terjadi kesalahan saat implementasi dibahasa pemrogramman php serta memperbaiki jika mengami kesalahan atau error.

2.2 Kriptografi

Kriptografi merupakan ilmu sekaligus seni untuk menjaga keamanan pesan (*Cryptography is the art and science of keeping messages secure*) selain itu ada pengertian tentang kriptografi yaitu kriptografi merupakan ilmu yang mempelajari teknikteknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Kata "seni" di dalam definisi di atas maksudnya adalah mempunyai cara yang unik untuk merahasiakan pesan. Kata "graphy" di dalam "*cryptography*" itu sendiri sudah menyiratkan sebuah seni [3].

Untuk dapat menjalankan dengan baik pada proses kriptografi haruslah terdapat empat elemen utama didalamnya, yang paling berkait satu sama lain yaitu [3] :

1. *Plain Text* Merupakan sebagai pesan awal atau pesan asli yang di kirim pada proses komunikasi. *Plain Text* inilah yang kemudian di enkripsi dan di deskripsi.
2. *Cipher Text* Merupaka pesan yang tersembunyi, yaitu pesan asli (*Pain Text*) yang telah di enkripsi dapa proses kriptografi. *Cipher Text* ini dapat diubah kembali kebentuk aslinya (*Pain Text*) memanfaatkan *Key* yang telah di sediakan.
3. *Cryptography Key* Merupakan kunci yang di gunakan untuk melakukan enkripsi dan deskripsi pada proses kriptografi. Tanpa adanya kunci (*key*) yang sama maka proses enkripsi dan deskripsi tidaka dapat dilakukan dengan baik. Kunci (*key*) merupakan informasi yang padat menjadi kendali terhadap proses terjadinya kriptografi.
4. *Encryption Decryption Algorithm* Komponen terakhir yang juga samapentingnya dalam proses kriptografi adalah algoritma yang di gunakan untuk enkripsi dan dekripsi.

Jenis serangan berdasarkan cara dan posisi seseorang untuk mendapatkan pesan dalam jaringan, yaitu [3]:

1. *Sniffing*
   Sniffing berarti 'mengendus', dalam hal ini yang diendus merupakan pesan (baik yang belum ataupun yang sudah di enkripsi) dalam suatu saluran komunikasi. Hal ini umum terjadi pada saluran publik yang tidak aman yang mengakbatkan sang pengendus dapat merekam pembicaraan yang terjadi.
2. *Replay Attack*
   Replay Attack adalah serangan jaringan dimana penyerang menyadap percakapan antara pengirim dan penerima, serta mengambil informasi autentik dengan berbagi kunci.
3. *Spoofing*
   Spoofing adalah teknik untuk memperoleh akses yang tidak sah ke suatu komputer atau informasi dimana penyerang berhubungan dengan pengguna dengan berpura-pura sebagai host yang dapat dipercaya.
4. *Man-in-the-middle*
   Serangan dunia maya di mana penyerang secara diam-diam menyampaikan dan mungkin mengubah komunikasi antara dua pihak yang percaya bahwa mereka berkomunikasi secara langsung satu sama lain.

2.3 Algoritma AES

Advanced Encryption Standard (AES) merupakan algoritma *cryptographic* yang dapat digunkan untuk mengamakan data. Algoritma AES adalah *blok chipertext simetrik* yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut *ciphertext;* sebaliknya dekripsi adalah merubah

ISSN 2597-4645 (media online)
ISSN 2597-4610 (media cetak)
Page: 78-86

ciphertext data menjadi bentuk semula yang kita kenal sebagai *plaintext*. Algoritma AES menggunakan kunci kriptografi 128, 192, dan 256 bits untuk mengenkrip dan dekripsi data [3].

Algoritma AES setiap blok dienkripsi dalam sejumlah putaran tertentu, sebagaimana halnya DES. Berikut pada Tabel 3.1 adalah banyaknya putaran kunci pada algoritma AES [4]

Tabel 1. Putaran Kunci Algoritma AES

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

Karena AES menetapkan panjang kunci adalah 128, 192 dan 256 maka dikenal sebagai AES-128, AES-192 dan AES-256. AES memiliki panjang kunci paling sedikit yaitu 128 bits, namun AES tetap tahan terhadap serangan exhaustive key search dengan teknologi saat ini. Dengan panjang kunci 128 bitsmaka terdapat sebanyak 2^{128}= 3,4 x 10^{38} kemungkinan kunci. Seperti pada DES, Rijndael atau AES menggunakan substitusi dan permutasi dan sejumlah putaran atau cipher berulang. Setiap putaran menggunakan kunci internal yang berbeda. Empat proses utama algoritma AES yaitu sebagai beriku [4]:

1. *SubBytes* (Transformasi Substitusi *Byte*)
2. *ShiftRow* (Transfornasi Pergeseran Baris)
3. *MixColumns* (Transformasi Percampuran Kolom)
4. *AddRoundKey* (Transformasi Penambahan Kunci)

Algoritma AES (*Advanced Encryption Standard*) memiliki tiga parameter yaitu sebagai berikut [4] :

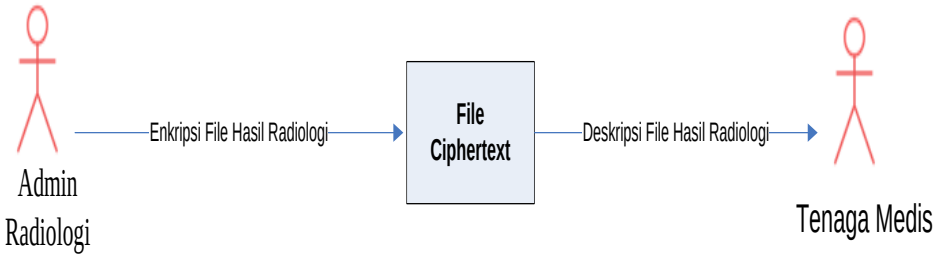
1. *Plainteks* merupakan array yang berukuran 16-byte, yang berisi data masukan.
2. *Cipherteks* merupakan array yang berukuran 16-byte, yang berisi hasil dari enkripsi.
3. *Key* merupakan array berukuran 16-byte, yang berisi kunci *ciphering* (disebut juga *cipher key*).

3. HASIL DAN PEMBAHASAN

3.1 Analisa Masalah

Adapun proses pengiriman hasil radiologi di RSU Imelda dikirim berdasarkan pasien yang sedang dirawat baik rawat jalan maupun rawat inap dimana dokter dapat melihat hasil foto radiologi berdasarkan indikasi diagnosa pasien dimana dokter yang merawat pasien baik rawat jalan maupun rawat inap. Setalah penulis amati di lapangan di RSU Imelda Medan, rata-rata kunjungan pasien per bulan rawat jalan 5.000 dan rawat inap 1.500 perbulan, kalau di totalkan rata-rata selama 1 tahun berjumlah 80.000 kunjungan. Setelah penulis menganalisa permasahan yang sedang berjalan di RSU Imelda Medan dimana hasil radiologi dikirim setelah dokter visite ke ruang rawat inap maupun rawat jalan dimana file hasil radiologi dengan format *jpg* dan *png* dikirim menggunakan *local area network* lewat *folder sharing* sehingga sering terjadi kehilangan hasil radiologi serta kurangnya keamanan file hasil radiologi karena hasil radiologi ini merupakah salah satu pemeriksaan penunjang dan rahasia pasien yang tidak perlu dikatahui oleh banyak orang. Permasalahan yang harus diselesaikan dalam melaksanakan proses skripsi ini adalah mengimplementasikan algoritma AES untuk melakukan proses enkripsi file hasil radiologi, pengiriman hasil radiologi dan proses deskripsi hasil radiologi dalam bentuk gambar *jpg* dan *png* sehingga file hasil radiologi dapat dienkripsi menggunakan algoritma AES. File hasil yang di upload salah satu mekanisme untuk enkripsi dan input password agar hasil radiologi tidak dapat di deskripsi yang tidak memiliku kunci atau password, jadi fungsi dari algoritma AES distudi kasus ini yaitu untuk enkripsi hasil dalam bentuk jpg,png dan deskripsi kembali hasil radiologi sehingga hasil radiologi dapat lebih aman lagi.

Berikut ini tahapan atau proses analisa implementasi enkripsi dan deskripsi hasil radiologi dapat di lihat di gambar berikut ini :



Gambar 1. Tahapan Analisa

Dari hasil analisa di gambar diatas pengirim membuat enkripsi kepada tenaga medis. File yang akan proses di enkripsi terlebih dahulu dengan menggunakan key atau kunci. File yang telah terenkripsi akan menghasilkan enkripsi file yang tidak bisa baca oleh tenaga medis, kemudian untuk mendeskripsikan file yang telah terenkripsi, harus

ISSN 2597-4645 (media online)
ISSN 2597-4610 (media cetak)
Page: 78-86

menggunakan key atau kunci yang telah dibuat oleh admin radiologi. File hasil radiologi yang telah terdeskripsi akan kembali menghasilkan file yang bisa dibaca oleh tenga medis.

3.2 Implementasi

Implementasi berikut ini merupakan hasil implementasi sebuah algoritma AES (*Advanced Encryption Standard*) enkripsi dan deskripsi hasil radiologi dalam format *jpg* dan *png*. Aplikasi enkripsi dan deskirpsi hasil radiologi diterapkan

Gambar 2. Halaman Login

Gambar 2. berfungsi sebagai halaman login sebelum melakukan proses enkripsi dan deskripsi hasil file radiologi di RSU Imelda.

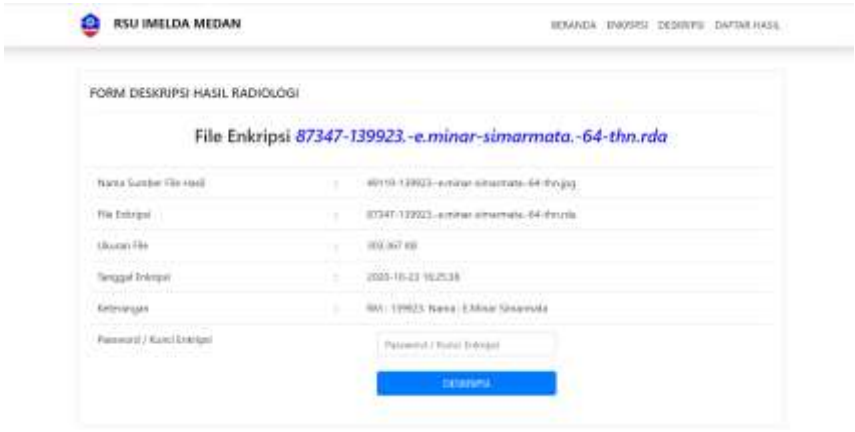
Gambar 3. Form Enkripsi Hasil Radiologi

Gambar 3. berfungsi sebagai tampilan enkripsi file, sehingga pengguna dapat melakukan upload file hasil radiologi, mengisi password sebagai kunci AES encrypt file hasil, mengisi keterangan dengan nomor rekam medis, nama pasien, jika sudah mengisi form yang diminta maka pengguna dapat melakukan enkripsi.

Gambar 4. Deskripsi File Hasil Radiologi

Gambar 4. ini merupakan tampilan file hasil radiologi yang telah di enkripsi sehingga file tersebut tidak dapat dibuka tanpa melakukan deskripsi terlebih dahulu, jika melakukan deskripsi, harus menginput password atau key enkripsi yang telah input sebelumnya di form enkripsi.

ISSN 2597-4645 (media online)
ISSN 2597-4610 (media cetak)
Page: 78-86



Gambar 5. Tampilan Form Deskripsi

Gambar 5. ini merupakan tampilan detail hasil enkripsi, dimana untuk melihat hasil radiologi yang telah dienkripsi sebelumnya harus melakukan proses input password atau key enkripsi file, jika kay yang dinput sudah benar maka proses deskripsi file hasil radiologi dapat dilihat kembali dan sebaliknya.

Gambar 6. Daftar Hasil Enkripsi dan Deskripsi

Gambar 6. ini merupakan tampilan hasil radiologi secara keseluruhan dihalaman ini dapat melihat data baik hasil radiologi yang telah dienkripsi maupun hasil yang telah di deskripsi.

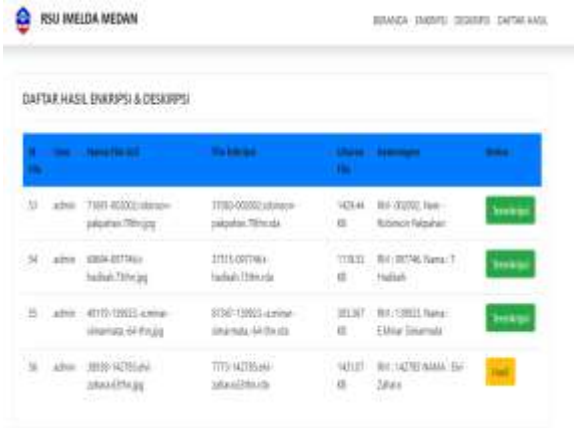
Gambar 7. Hasil Radiologi

Gambar 7. merupakan tampilan hasil radiologi yang telah di deskripsikan kembali setelah melewati tahap enkripsi dan validasi kay enkripsi.

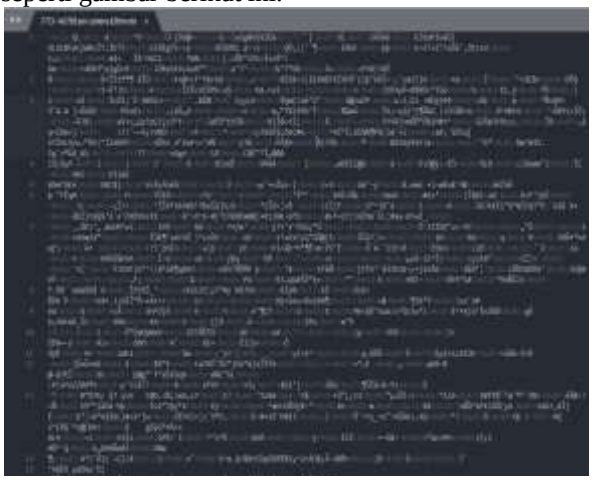
Berikut ini proses untuk melakukan pengujian terhadap file hasil radiologi yang telah di enkripsi yaitu sebagai berikut :

ISSN 2597-4645 (media online)
ISSN 2597-4610 (media cetak)
Page: 78-86

Tabel 2. Pengujian enkripsi file *jpg* dan *png*

Skenario Pengujian	Hasil Pengujian
Lengkah yang harus di lakukan	Harap pilih menu enkripsi, upload file *jpg* atau png, input password atau *kay*, buat keterangan dengan nama pasien, rekam medis, setelah itu lalu klik *button* enkripsi
Pengamatan	Aplikasi mempu memproses file hasil radiologi baik bentuk *jpg* dan bentuk *png*. 

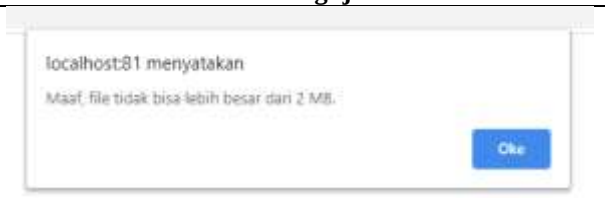
Tabel 3. Pengujian enkripsi file *jpg* dan *png*

Skenario Pengujian	Hasil Pengujian
Lengkah yang harus di lakukan	Harap pilih menu enkripsi, upload file *jpg* atau png, input password atau *kay*, buat keterangan dengan nama pasien, rekam medis, setelah itu lalu klik *button* enkripsi
Pengamatan	Jika file hasil radiologi dibuka menggunakan *sumblime text* maka maka isi gambar jpg atau jpg kurang lebih seperti gambar berikut ini. 
Kesimpulan	Sukses

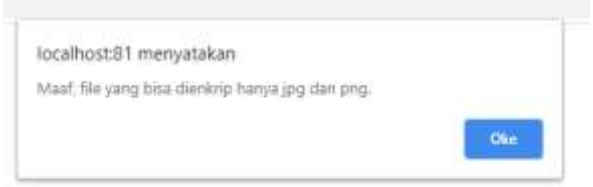
Tabel 4. Pengujian validasi upload lebih 2 *megabyte*

Skenario Pengujian	Hasil Pengujian
Lengkah yang harus di lakukan	Harap pilih menu enkripsi, upload file *jpg* atau *png*, input password atau *kay*, buat keterangan dengan nama pasien, rekam medis, setelah itu lalu klik *button* enkripsi
Pengamatan	Jika melakukan upload gambar lebih dari 2 *megabyte* maka memunculkan pesan gagal upload.

ISSN 2597-4645 (media online)
ISSN 2597-4610 (media cetak)
Page: 78-86

Skenario Pengujian	Hasil Pengujian
	
Kesimpulan	Sukses

Tabel 5. Pengujian validasi lain dari format *jpg* dan *png*

Skenario Pengujian	Hasil Pengujian
Lengkah yang harus di lakukan	Harap pilih menu enkripsi, upload file *jpg* atau *png*, input password atau *kay*, buat keterangan dengan nama pasien, rekam medis, setelah itu lalu klik *button* enkripsi
Pengamatan	Jika melakukan upload yang bukan format *jpg* dan *png* maka otomatis aplikasi memberikan pesan gagal
	
Kesimpulan	Sukses

Berikut ini proses untuk melakukan pengujian terhadap file hasil radiologi yang telah di enkripsi dan di deskripsikan agar bisa dibaca kembali:

Tabel 6. Pengujian deskripsi file radiologi

Skenario Pengujian	Hasil Pengujian
Lengkah yang harus di lakukan	Harap pilih menu deskripsi, setelah itu muncul daftar hasil radiologi yang telah di enkripsi, lalu pilih *button* deskripsi hasil, lalu muncul tampilan form deskripsi hasil dan input password atau key saat enrkipsi.
Pengamatan	Jika password / key berhasil, maka hasil deskripsi radiologi berhasil, dapat di lihat digambar berikut ini.
	
Kesimpulan	Sukses

Tabel 7. Pengujian validasi kay atau password

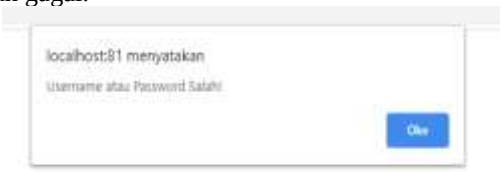
Skenario Pengujain	Hasil Pengujian
Lengkah yang harus di lakukan	Harap pilih menu deskripsi, setelah itu muncul daftar hasil radiologi yang telah di enkripsi, lalu pilih *button* deskripsi hasil, lalu muncul tampilan form deskripsi hasil dan input password atau key saat enrkipsi.
Pengamatan	Jika password tidak sesuai dengan password yang di input waktu enkripsi, bila terjadi kesalahan input, maka mancul pesan gagal.

ISSN 2597-4645 (media online)
ISSN 2597-4610 (media cetak)
Page: 78-86

Skenario Pengujain	Hasil Pengujian
	
Kesimpulan	Sukses

Berikut ini proses untuk melakukan pengujian hasil login radiologi yaitu:

Tabel 8. Pengujian Login Gagal

Skenario Pengujian	Hasil Pengujian
Lengkah yang harus di lakukan, username : admin dan password : admin Pengamatan	Buka halaman login, lalu input username dan password, lalu klik *button* login, jika berhasil makan di arahkan ke halaman admin. Jika username dan password maka memunculkan pesan gagal.  Jika username dan password benar di input maka diarahkan ke halaman utama 
Kesimpulan	Sukses

4. KESIMPULAN

Berdasarkan latar belakang dan rumusan masalah, ada beberapa point penting yang menjadi kesimpulan penulis untuk menjawab permasalahan yang ada di RSU Imelda Medan Untuk meningkatkan keamanan data hasil radiologi penulis implementasikan sebuah pengamanan data dengan menggunakan algoritma kriptografi AES (*Advanced Encription Standart*) 128 bit berbasi web dengan metode pengembangan penulis menggunakan metode yang sangat sering digunakan yaitu metode SDLC. Untuk enkripsi dan deskripsi hasil radiologi dapat diakses dengan webserver atau berbesis web sehingga memudahkan untuk mengaksesnya. Hasil radiologi yang dapat di enkripsi dan deskripsi di penelitian ini hanya berformat jpg dan png, maka diluar dari format tersebut maka otomatis sistem akan menolak proses enkripsi tidak bisa di lanjutkan. Proses kecepatan waktu dalam melakukan proses enkripsi dan deskripsi tergantung ukuran file yang akan upload atau di proses jika semakin kecil file yang akan upload maka waktu proses akan lebih cepat jika file semakin besar maka proses upload file semakin lama.

REFERENCES

[1] R. Nauri and N. Ratama, "Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping," *Journal Of Artificial Intelligence And Innovative Applications*, pp. 37-44, 2 Mei 2020.

[2] T. Rahmat Aditia, Y. Permanasari and H. Erwin, "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen," *Jurnal Matematika UNISBA*, vol. 15, pp. 1-14, 1 Mei 2016.

[3] A. A. Permana and D. Nurnaningsih, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (AES)," *Jurnal Teknik Informatika*, vol. 11, pp. 177-186, 2018.

[4] Y. A. Mulyadi, P. E. N and R. R. J.P, "implementasi Algoritma AES 128 dan SHA – 256 Dalam Pengkodean padaSebagian Frame Video CCTV MPEG-2," *urnal Teori dan Aplikasi Ilmu Komputer*, vol. 1, pp. 33-39, 2018.

[5] R. R. T, Y. Permanasari and H. Erwin, "Kriptografi Advanced Encryption Standard (AES) Kriptografi Advanced Encryption Standard (AES)," *Kriptografi Advanced Encryption Standard (AES)* , vol. 15, pp. 7-13, 2016.

[6] M. Prabowo, I. Muhimmah and R. Kurniawan, "Pemodelan Pengiriman Data Citra Medis untuk," *Seminar Nasional Informatika Medis (SNIMed)*, vol. VIII, p. 76, 2017.

ISSN 2597-4645 (media online)
ISSN 2597-4610 (media cetak)
Page: 78-86

[7] Ardiana, "Perancangan Sistem Informasi Radiologi Guna Mendukung Peningkatan Pelayanan Pada Pasien di Rumah Sakit Umum Daerah Al-Ihsan Pemprov Jabar," *Teras Kesehatan*, vol. I, pp. 2622-2396, 2019.

[8] Ansori, "Pengertian Flowchart : Jenis, Simbol, dan Contohnya," 27 Maret 2020. [Online]. Available: https://www.ansoriweb.com/2020/03/pengertian-flowchart.html.

[9] R. A. Nugraha and G. Pramukasari, "Sistem Informasi Akademik Sekolah Berbasis Web Di Sekolah Menengah Pertama Negeri 11 Tasikmalaya," *JUMIKA*, vol. IV, pp. 51-60, 2017.

[10] Y. Yudhanto and A. H. Prasetyo, Panduan Mudah Belajar Framework Laravel, Jakarta: PT. Alex Media Komputindo, 2018, pp. 1-17.

[11] A. Muahrdian, "Text Editor Visual Studio Code di Linux," 28 Juli 2017. [Online]. Available: https://www.petanikode.com/text-editor-vscode/.

[12] B. Winarso, "Apa Itu Google Chrome dan Sepenggal Sejarahnya," 23 Maret 2016. [Online]. Available: https://dailysocial.id/post/apa-itu-google-chrome/.

[13] I. M. Perkasa and B. E. Setiawan, "Pembangunan Web Service Data Masyarakat Menggunakan REST API dengan Access Token," *ULTIMA Computing*, vol. X, pp. 19-26, 2018.