Jurnal Teknologi Sistem Informasi dan Aplikasi **ISSN: 2654-3788**
Penerbit: Program Studi Teknik Informatika Universitas Pamulang **e-ISSN: 2654-4229**
Vol. 6, No. 2, April 2023 (147-153) **DOI: 10.32493/jtsi.v6i2.22694**

Implementasi Algoritma *Advanced Encryption Standart* - 128 Berbasis Dekstop pada Teks dan Dokumen

Syafril Malik[1], Aries Saifudin[2]

Teknik Informatika, Universitas Pamulang, Jl. Raya Puspitek No. 46 Buaran, Serpong, Tangerang Selatan, Banten, Indonesia, 15417
e-mail: [1]syafrilmalik11@gmail.com, [2]aries.saifudin@unpam.ac.id

Submitted Date: February 03rd, 2023 Reviewed Date: April 14th, 2023
Revised Date: April 20th, 2023 Accepted Date: April 30th, 2023

Abstract

Given the importance of information in every activity and communication process, it results in interference and threats to the security of confidential information that can be manipulated by other people who are not entitled. In this study, we will apply cryptographic techniques using the AES (advance standard encryption) method in the document security system, to minimize threats and disturbances to the security of messages and information and so that they are not seen and stolen by other unauthorized parties. implementation Based on and testing achieved in this research, the application of cryptography and in a file security system has proven to be used to increase security and proven to be able to maintain confidentiality so that it is not seen or read by other unauthorized persons.

Keywords: File Scurity; AES; Text and Document

Abstrak

Mengingat pentingnya peranan informasi dalam setiap kegiatan dan proses komunikasi mengakibatkan adanya gangguan serta ancaman terhadap keamanan informasi yang bersifat rahasia dapat dimanipulasi oleh orang lain yang tidak berhak. Dalam penelitian ini akan menerapkan teknik kriptografi menggunakan metode AES (*advance encryption standart*) dalam sistem keamanan dokumen, untuk meminimalisir ancaman dan gangguan pada keamanan pesan dan informasi serta agar tidak dapat dilihat dan dicuri oleh pihak lain yang tidak berkepentingan. Berdasarkan implementasi dan pengujian yang dicapai di penelitan ini, penerapan kriptografi dan dalam sistem keamanan *file* terbukti dapat digunakan untuk meningkatkan keamanan dan terbukti dapat menjaga kerahasiannya agar tidak dapat dilihat maupun dibaca oleh orang lain yang tidak berkepentingan.

Kata kunci: Keamanan file; AES; Teks dan Dokumen

1 Pendahuluan

Urgensi diperlukannya pengamanan data disebabkan oleh maraknya kasus penyalagunaan data seperti pencurian data, dan modifikasi data (Rumlus & Hartad, 2020). Hal tersebut merupakan perbuatan melawan hukum yang secara ekspresif verbis melanggar peraturan perundang-undangan terkait perlindungan data pribadi sehingga jika dibiarkan tentu mengakibatkan penderogasian hak-hak asasi manusia, penyelesaian permasalahan data pribadi dengan cara memberikan solusi berupa perlindungan hal ini merupakan keinginan Pasal 28 G Undang-Undang Dasar Republik Indonesia Tahun 1945 (UUD) yang mengatur hak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya. Guna melihat ketentuan tersebut sebagai ketentuan mengenai privasi dan data pribadi (Rumlus & Hartad, 2020).

Pada saat ini, kemajuan teknologi di bidang sistem informasi sangatlah berkembang pesat. Sistem informasi adalah suatu kombinasi yang tertata dari orang-orang, hardware, software, jaringan komunikasi, dan sumber daya data yang

mengumpulkan, mengubah, dan menyebarkan informasi dalam bentuk organisasi (Irviani, 2017). Sehingga mendapatkan perhatian khusus, terutama dalam aspek pengamanan informasi elektronik. Hal tersebut dikarenakan pengamanan informasi merupakan komponen penting dalam informasi elektronik yang bersifat rahasia.

Sabotase pada dokumen juga dialami oleh industri food and baverage termasuk PT. Routine Coffee and Eatery yang didirikan pada tahun 2015 oleh Munaya Sakina dan Yunila Sakina Prusahaan ini bergerak dibidang F&B (Food and Beverage), berada dijalan raya Wahid Hasyim Blok FG 14 No. 42, 1st Floor, Sektor 7 Bintaro Jaya, 15424 Tangerang Selatan. PT Routine Coffee and Eatery meiliki konsep indusrial coffee and eatery serta menyajikan menu western dan Indonesia, Memiliki kapasitas 150 orang, Tempat nyaman serta menu yang enak membuat tempat ini banyak dikunjungi para pelanggan setia. Data Security adalah cara melindungi informasi digital dari akses tidak sah, korupsi, atau pencurian di seluruh siklus hidupnya (Pujianto, 2018). Ini adalah konsep yang mencakup setiap aspek keamanan informasi dari keamanan fisik perangkat keras dan perangkat penyimpanan hingga kontrol administratif dan akses, serta keamanan logis dari aplikasi perangkat lunak. Ini juga mencakup kebijakan dan prosedur organisasi ramainya pelanggan dan kuatnya persaingan membuat coffee shop ini mengalami pencurian dan sabotase dokumen oleh pihak yang tidak berwenang, dikarenakan kurangnya pengamananan data.

Kerahasiaan dari informasi merupakan sebuah kelengkapan pelayanan yang dibuat untuk menjaga sehingga informasi yang tersimpan tidak dapat dibaca atau dibuka oleh pihak yang tidak berhak. Upaya menjaga kerahasiaan sebuah data informasi tersebut sudah tercetus sejak jaman dahulu tepatnya pada jaman romawi dengan metode pergeseran huruf atau karakter dengan dasar nilai tertentu (Sastra, 2018) untuk menjaga keamanan data-data pada dokumen tersebut diperlukan suatu metode salah satunya menggunakan kriptografi (Dilaga, 2017) algoritma Advanced Encryption Standard. Algoritma AES menggunakan kunci kriptografi 128, 192, dan 256 bits untuk mengenkrip dan dekripsi data pada blok 128 bits (Widyawan & Imelda, 2021) (Riski Tahara Shita, 2018). Enkripsi akan mengubah data yang tidak dapat lagi dibaca disebut ciphertext, sebaliknya dekripsi akan merubah ciphertext data menjadi bentuk semula yang kita kenal sebagai plaintext (Anisha Yahdiani Mulyadi, 2018). Setelah mengkaji permasalahan di atas peneliti memutuskan untuk membuat tugas akhir dengan judul "Implementasi Advanced Encryption Standard-128 Pada Dokumen Dan Teks Study Kasus : PT. Routine Coffee and Eatery", sehingga aplikasi yang dibangun diharapkan dapat menyimpan data-data penting pada PT. Routine Coffee and Eatery.

2 Metodologi

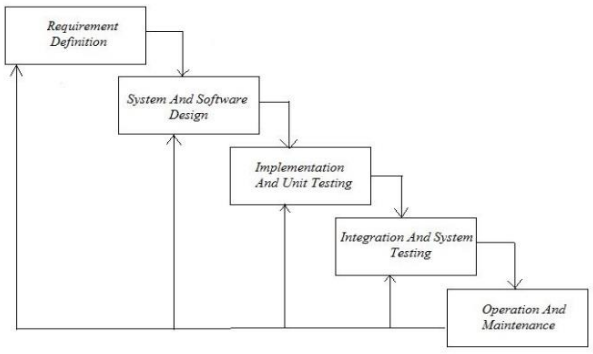
Metode yang digunakan dalam penelitian ini menggunakan metode kualitatif di mana peneliti menjadi kunci utama dalam pengumpulan data, Pengumpulan data yang peneliti lakukan dengan cara mencari referensi dari berbagai penelitian yang telah dilakukan terlebih dahulu terkait dengan penelitian ini, motivasi serta tujuan penelitian secara umum pada dasarnya adalah sama, penelitian adalah bentuk dari keinginan manusia yang selalu berusaha untuk mengetahui sesuatu. Adapun tujuan penelitian adalah penemuan, pembuktian dan pengembangan ilmu pengetahuan yang sedang diteliti.

Metodologi penelitian yang digunakan dalam penulisan ini antara lain meliputi:

a. Tahap Analisis (*Analisis*)
   Kegiatan menganalisis permasalahan yang ada dengan melakukanpengumpulan data berupa wawancara, observasi serta studi pustaka.
b. Tahap Perancangan (*planning*)
   Melakukan perencanaan untuk menentukan program aplikasi yang akan dirancang dan dijalankan pada perusahaan PT Routine Coffee and Eatery.
c. Tahap Perancangan (*Design)*
   Menentukan perancangan konsep dan tema dasar pada rancangan program yang akan dibuat sehingga diharapkan dapat mempunyai perancangan yang baik.
d. Pengkodean (*Coding*)
   Dalam tahap pekodean ini penulis melakukan implementasi dari tahap sebelumnya yaitu tahap desain kedalam bahasa pemrograman dengan menggunakan NEATBEANS.
e. Pengujian (*Testing*)

Terdapat pengujian dalam penelitian ini untuk menguji aplikasi dapat berperoses dengan baik atau tidak sehingga dapat dilakukan perbaikan jika terdapat kesalahan.

Menggunakan metode pengembangan sistem model *waterfall yang* sangat baik digunakan. Di mana sistem *waterfall* selalu berkembang baik dalam teknologi.



Gambar 1. Alur Waterfall

Berdasarkan gambar di atas, dapat dijelaskan bahwa tahapan dalam model *waterfall* (Sianturi, 2019), antara lain:

1. *Requirement Analysis and Defenition*
   Mengumpulkan kebutuhan secara lengkap kemudian dianalisis dan didefinisikan kebutuhan yang harus dipenuhi oleh program yang akan dibangun. Fase ini harus dikerjakan secara lengkap untuk bias menghasilkan desain yang lengkap.
2. *Sistem and Software Design*
   Desain dikerjakan setelah kebutuhan selesai dikumpulkan secara lengkap.
3. *Implementation and Unit Testing*
   Desain program diterjemahkan ke dalam kode-kode dengan menggunakan bahasa pemograman yang sudah ditentukan. Program yang dibangun langsung diuji baik secara unit.
4. *Integration and Sistem Testing*
   Penyelarasan program yang akan kemudian diuji secara menyeluruh.
5. *Operation and maintenance*
   Mengoperasikan program dilingkungannya dan melakukan pemeliharaan, seperti penyesuaian atau perubahan karena adaptasi dengan situasi sebenarnya.

UML meraupakan bahasa visul untuk pemodelan dan komunikasi mengenai sebuah sistem dengan menggunakan diagram dan teks-teks pendukung. UML hanya berfungsi untuk melakukan pemodelan (Sianturi, 2019). Penggunaan UML salah satunya berfungsi sebagai (*blue print*) cetak biru, karena sangat lengkap dan detail.

Analisa sistem ialah uraian dari suatu sistem yang utuh kedalam sebuah bagian komponen dengan tujuan untuk identifikasi dan evaluasi permasalahan, hambatan, dan kebutuhan yang diinginkan sehingga dapat diperbaiki ke depannya. Sistem yang dibangun ini secara umum dapat digambarkan sebagai sistem yang mampu mengamankan pesan atau menyediakan pesan. Sehingga terdapat dua proses yaitu enkripsi dokumen dan deskripsi dokumen (Aditia Rahmat Tulloh, 2016).

Proses enkripsi dokumen merupakan sebuah proses pengacakan dan penyembunyian dokumen sehingga tidak dapat dibaca dan dimengerti oleh pihak yang tidak berkepenntingan atau tidak berhak (Latif, 2015). Sedangkan proses deskripsi dokumen merupakan proses pengambilan atau membuka pesan yang sudah disembunyikan sehingga dapat dibaca dan dimengerti.

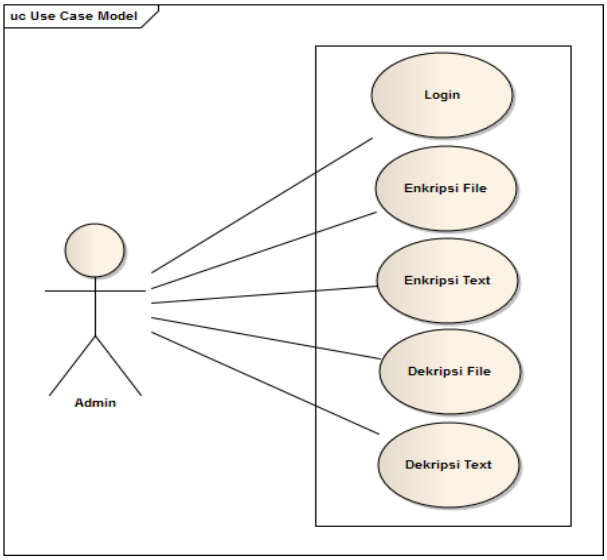
Analisa kebutuhan merupakan analisis penggunaan perangkat keras dan perangkat lunak yang dibutuhkan pada sistem keamanan yang akan mendukung pembangunan sistem dari awal pembuatan hingga pengujian sistem (Saifudin & Wahono, 2015). Adapun perangkat keras yang dibutuhkan yaitu dengan spesifikasi seperti yang terdapat di tabel berikut:

Tabel 1, Analisa Kebutuhan

PERANGKAT KERAS	
Processor	: Intel
Hard Disk Drive	: Minimum 500 GB
Memory	: Minimum 2 GB
VGA Card	: Minimum 128 MB
PERANGKAT LUNAK	
Sistem Operasi	Windows 10
Bahasa Pemograman	Java
Aplikasi Permodelan	Enterprise architect
Aplikasi Pengolah kata	Microsoft Office 2016

Perancangan sistem bertujuan untuk memberikan gambaran secara umum kepada pengguna mengenai sitem keamanan pesan,

perancangan sistem secara umum juga sudah dapat mengenal komponen sistem yang akan didesain. Penentuan persyaratan sistem dilakukan agar arah perancangan sistem dapat terarah pada sasaran oleh sebab itu sistem dirancang harus memenui batasan sistem, akan dijelaskan dalam *use case* diagram (Shalahuddin, 2015):



Gambar 2, *Use Case* diagram

Dari digram di atas dapat dijelaskan bahwa admin yang telah melakukan login dapat melakukan enkripsi file, dekripsi file, enkripsi teks dan dekripsi teks di dalam aplikasi.

3 Implementasi dan Pengujian

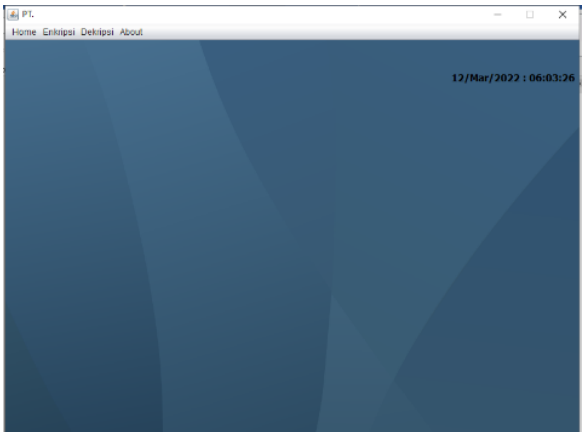
Enterprise Architech (EA) adalah kegiatan pengorganisasian data digunakan dan diproduksi oleh organisasi yang mencakup tujuan proses bisnis dari organisasi dan merupakan cetak biru yang menjelaskan bagaimana elemen TI dan manajemen informasi bekerja sama sebagai satu kesatuan. Kerangka seperti ini akan menggambarkan infrastruktur yang dibutuhkan oleh organisasi untuk mencapai tujuan dan visi dalam membentuk keamanan dokumen, EA adalah kerangka kerja yang dapat memberikan struktur konseptual tentang komponen yang harus ada tentang EA dan cara membuatnya, Komponen meliputi seperangkat model, prinsip, pendekatan, standarisasi, dan visualisasi yang digunakan sebagai pedoman dalam perkembangan (Widodo, 2018).

Berikut ini adalah implementasi User Interface Penerapan Algoritma AES 128 Pada dokumen dan teks:

a. Form Login

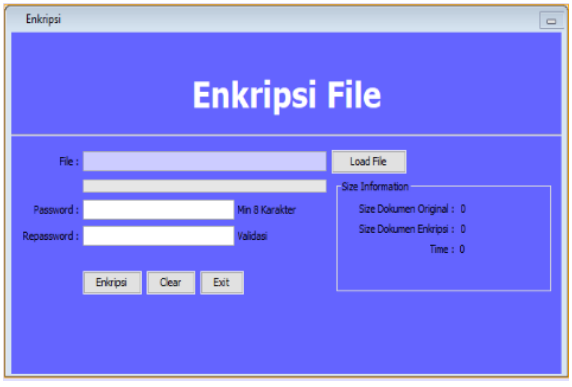
Gambar 3, User Interface Form Login

b. Home



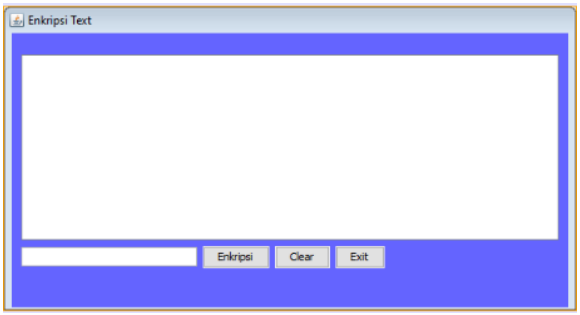
Gambar 4, User Interface Home

c. Enkripsi File



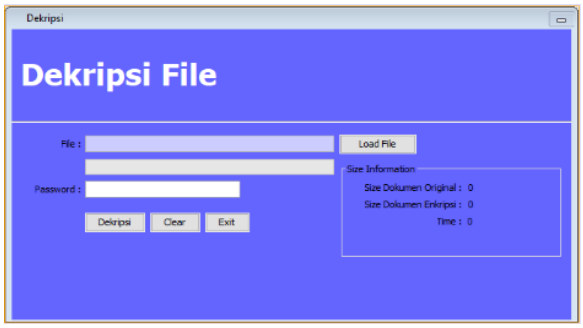
Gambar 5, User Interface Enkripsi File

d. Enkripsi Text



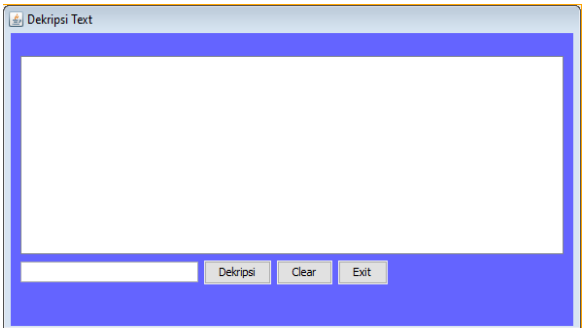
Gambar 6, User Interface Enkripsi Text

e. Dekripsi File



Gambar 7, User Interface Dekripsi File

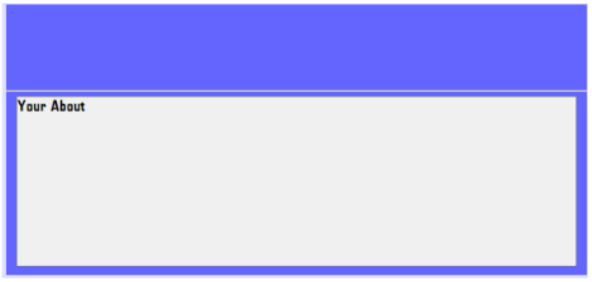
f. Dekripsi Text



Gambar 8, User Interface Dekripsi Text

a. Pengujian *Login*

g. About



Gambar 9, User Interface About

Sebelum melakukan pengujian, dilakukan identifikasi hal-hal yang akan diuji serta rencana pengujiannya. Hal ini dilakukan agar perangkat lunak yang dikembangkan dapat terukur berdasarkan input yang dimasukkan dan output yang diharapkan. Berikut adalah tabel rencana pengujian yang dibuat :

Tabel 2, Rencana Uji

No	Item Pengujian	Detail Pengujian	Jenis Pengujian
1	*Form Login*	Verifikasi *Username* dan *Password*	*Black box*
2	Enkripsi *File*	*Load File*, *Password*, Re *Password*, Enkripsi	*Black box*
3	Enkripsi *Text*	*Edit*, *Password*, Enkripsi	*Black box*
4	Dekripsi *File*	*Load File*, *Password*, Dekripsi	*Black box*
5	Dekripsi *Text*	*Edit*, *password*, Dekripsi	*Black box*

Pengujian *Black Box*

Pengujian *black box* berfokus pada persyaratan fungsional perangkat lunak. Pengujian aplikasi formulasi produk dan intruksi kerja ini menggunakan data uji berupa data input pada sistem yang telah disediakan. Skenario yang dilakukan sebagai berikut:

Tabel 3 Tabel Pengujian *Black box*

No	Skenario	Test Case	Hasil yang diharapkan	Status
1	Berhasil *Login*	Input *username* dan *password* yang valid	Sistem berhasil masuk ke halaman utama *user*.	Valid
2	Gagal *Login*	Input username dan password yang tidak valid	Sistem akan memunculkan notifikasi bahwa username atau *password* yang dimasukkan salah.	Valid

b. Pengujian Enkripsi *File*

Tabel 4, Tabel Pengujian *Black box*

No	Skenario	Test Case	Hasil yang diharapkan	Status
1	*Load file*	Tampil *panel user* direktori dan menampilkan serta menyimpan dokumen pada *field file* yang telah dipilih.	Menampilkan *panel user* direktori dan menyimpan dokumen untuk ditampilkan dalam *field file* yang telah dipilih.	Valid
2	Mengisi *password*	Isi dari *password field* akan sesuai dengan *password* yang dimasukan	*Password field* akan terisi sesuai *password* yang dimasukkan	Valid
3	Mengisi re *password*	Isi dari *text field password* sesuai dengan *password* yang dimasukan dan melakukan validasi	*Password field* akan terisi sesuai *password* yang dimasukan dan melakukan	Valid
4	Enkripsi	Proses embed berjalan pada *progress bar,* kemudian tampil panel user direktori, dan hasil proses embed berupa dokumen yang akan disimpan pada user direktori.	Sistem akan melakukan proses enkripsi, kemudian sistem akan menampilkan *panel user* direktori untuk menyimpan hasil embed berupa file dokumen.	Valid

c. Pengujian Enkripsi *Text*

Tabel 5 Tabel Pengujian *Black box*

No	Skenario	Test Case	Hasil yang diharapkan	Status
1	*Edit*	isi *textfield* bebas yang akan di enkripsi	*Textfield* akan terisi sesuai yang dimasukan	Valid
2	*Password*	Isi dari *password field* akan sesuai dengan *password* yang dimasukan	*Password field* akan terisi sesuai *password* yang dimasukkan	Valid
3	Enkripsi	Proses embed berjalan dan hasil *textfield* menyerupai kode-kode	Sistem akan bekerja dan *text* akan berubah menjadi kode-kode secara acak	Valid

d. Pengujian Dekripsi *File*

Tabel 6, Tabel Pengujian *Black box*

No	Skenario	Test Case	Hasil yang diharapkan	Status
1	*Load file*	Tampil *panel user* direktori dan menampilkan serta menyimpan dokumen pada *field file* yang telah dipilih.	Menampilkan *panel user* direktori dan menyimpan dokumen untuk ditampilkan dalam *field file* yang telah dipilih.	Valid
2	Mengisi *password*	Isi dari *password field* akan sesuai dengan *password* yang dimasukan	*Password field* akan terisi sesuai *password* yang di masukan	Valid
3	Dekripsi	Proses embed berjalan pada *progress bar,* kemudian tampil panel user direktori, dan hasil proses embed berupa dokumen yang akan disimpan pada user direktori.	Sistem akan melakukan proses Dekripsi, kemudian sistem akan menampilkan *panel user* direktori untuk menyimpan hasil embed berupa file dokumen.	Valid

e. Pengujian Dekripsi text

Tabel 7 Tabel Pengujian *Black box*

No	Skenario	Test Case	Hasil yang diharapkan	Status
1	*Edit*	*copy* hasil enkripsi, lalu isi *paste* kedalam isi *textfield* yang yang akan didekripsi	*Textfield* harus berisi hasil dari enkripsi sebelumnya	Valid
2	*Password*	Isi dari *password field* akan sesuai dengan *password* yang dimasukan	*Password field* akan terisi sesuai *password* yang dimasukkan	Valid
3	Dekripsi	Proses embed berjalan dan hasil *text* akan muncul	Sistem akan bekerja dan berhasil didekripsi menjadi kembali semula	Valid

4 Kesimpulan

Berdasarkan hasil penelitian, implementasi dan pengujian dapat diketahui bahwa aplikasi keamanan file dan teks menggunakan algoritma enkripsi standar – 128 dapat berkerja dan digunakan dengan baik untuk mengamankan data, menggunakan cara enkripsi lalu file akan melalui proses pengacakan atau tidak bisa terbaca, dan terbukti bahwa file yang sudah diamankan dapat didekripsi kembali dengan akurat tanpa mengubah wujud dan isi dari file tersebut.

Maka dapat ditarik kesimpulan:

1. Setelah melalui beberapa tahapan pengujian dalam penelitian ini didapatkan hasil bahwa metode AES dalam aplikasi keamanan file dokumen tanpa mengubah isi informasi sedikitpun di dalamnya.
2. Metode AES terbukti bisa digunakan untuk meminimalisir gangguan keamanan pada teks dan dokumen.

5 Saran

Dalam penerapan algoritma kriptografi pada aplikasi kemanan file ini masih terdapat banyak kekurangan, sehingga perlu diadakan penelitian dan pengembangan lebih lanjut tentang keamanan file. Adapun saran untuk perbaikan penelitian selanjutnya adalah sebagai berikut:

1. Aplikasi keamanan file dokumen ini masih berbasis dekstop sehingga ke depannya bisa dikembangkan lagi menjadi berbasis website dan berbasis mobile.
2. Waktu yang dibutuhkan dalam proses enkripsi yang masih tidak terlalu cepat ketika digunakan untuk mengenkripsi file yang berukuran besar, sehingga ke depannya diharapkan ditemukan cara untuk mempercepat proses enkripsi tersebut

Daftar Pustaka

Aditia Rahmat Tulloh, Y. P. (2016). Kriptografi Advanced Encryption Standard (AES) . Jurnal Matematika UNISBA.

Anisha Yahdiani Mulyadi, E. P. (2018). Implementasi Algoritma AES 128 dan SHA –256 Dalam Pengkodean pada Sebagian Frame Video CCTV MPEG-2. E-jurnal JATIKOM, 7.

Dian Widyawan, I. (2021). Pengamanan File Menggunakan Kriptografi dengan Metode AES-128 Berbasis Web di Komite Nasional Keselamatan Transportasi. Skanika. SKANIKA.

Dilaga, J. (2017). Kriptografi Hybrid Algoritma Rail Fence Dan ElGamal Dalam Pengamanan Data Berbasis Teks. mercubuana-yogya, 5-10.

Irviani, E. Y. (2017). Pengantar Sistem Informasi. Yogyakarta: BukuKita.com dan Gramedia.

Latif, A. (2015). Implementasi Kriptografi Menggunakan Metode Advanced Encryption Standar(Aes) Untuk Pengamanan Data Teks. jurnal ilmiah mustek anim ha, 10-20.

Muhamad Hasan Rumlus, H. H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi. jurnal HAM, 1-5.

Pujianto, Y. R. (2018). Perancangan dan Implementasi Aplikasi Kriptografi Algoritma AES-128 Pada File Dokumen. uksw.edu, 1-26.

Riski Tahara Shita, L. L. (2018). Implementasi Algoritma Kriptografi AES 128bit dan Elgamal untuk Pengamanan E-Mail Pada Bandara Internasional Sultan Mahmud Baharuddin II Palembang. jurnal budi luhur, 1-10.

Saifudin, A., & Wahono, R. S. (2015). Pendekatan Level Data untuk Menangani Ketidakseimbangan Kelas pada Prediksi Cacat Software. Journal of Software Engineering , 1(2), 76-85.

Sastra, A. P. (2018). Implementasi Algoritma Advanced Encryption Standard (AES). jurnal denpasar, 1-25.

Shalahuddin, m. R. (2015). Use Case Diagram. jurnal it, 35.

Sianturi, J. S. (2019). Perancangan Sistem Informasi Pemesanan Tiket Bus. Riau: Jurnal Intra-Tech.

Widodo, A. P. (2018). Enterprise Architecture Model untuk Aplikasi Government . Jurnal Masyarakat Informatika, 24.