Journal of Information and Information Security (JIFORTY)
Vol. 2, No. 2, Desember 2021, 227-238
e-ISSN : 2722-4058
Available Online at http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Penerapan Algoritma Advanced Encryption Standard (AES-256) Dengan Mode CBC DanSecure Hash Algorithm (SHA-256) Untuk Pengamanan Data File

Ahmad Fathurrozi[1], Selviyani[2]

Informatika; Universitas Bhayangkara Jakarta Raya, Jl Raya Perjuangan No. 81 Bekasi Utara, (021) 889558822; e-mail: fathur@dsn.ubharajaya.ac.id, selviyani17@mhs.ubharajaya.ac.id

* Korespondensi: e-mail: fathur@dsn.ubharajaya.ac.id

Diterima: 12 Des 2021; Review: 13 Des 2021; Disetujui :14 Des 2021; Diterbitkan: 15 Des 2021

Abstract

Data Protection is one of the important things to protect important messages and information from corruption, compromise or loss so that messages and information remain safe. Encryption and description techniques are considered to be able to secure data properly by protecting files from being easily read or seen by unauthorized parties. In this case, the authors used data from University of Bhayangkara Jakarta Raya to be able to secure their university data using a cryptography symmetrical algorithm called Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA) as a solution to existing problems. The AES algorithm process is divided into four steps, the first step is SubBytes, the second step is ShiftRows, the third step is MixColums and the last step is AddRoundKey. And using the SHA algorithm as the hashing function. The algorithm is applied to a desktop-based file description and encryption application with the C sharp programming language.

***Keywords**: Data Protection, Encryption, Description, Algorithm AES-256, SHA- 256*

Abstrak

Pengamanan data atau data protection merupakan salah satu hal penting untuk melindungi pesan dan informasi penting dari korupsi, kompromi atau kerugian supaya pesan dan informasi tersebut tetap aman. Teknik enkripsi dan deskripsi dinilai dapat mengamankan data dengan tepat dengan melindungi file agar tidak mudah untuk dibaca atau dilihat oleh pihak yang tidak berwenang. Pada penelitian ini penulis menggunakan data dari Universitas Bhayangkara Jakarta Raya untuk dapat mengamankan data universitas mereka menggunakan algoritma kriptografi simetris *Advanced Encryption Standard* (AES) dan *Secure Hash Algorithm (*SHA) sebagai solusi untuk masalah yang ada. Proses algoritma AES sendiri terbagi menjadi empat langkah, langkah pertama yaitu *SubBytes*, langkah kedua *ShiftRows*, langkah ketiga *MixColums* dan langkah terakhir yaitu *AddRoundKey*. Serta menggunakan algoritma SHA sebagai fungsi *hashing*-nya. Penerapan algoritma tersebut diterapkan ke dalam aplikasi enkripsi dan deskripsi file berbasis *desktop* dengan bahasa pemograman C *sharp*.

Kata Kunci : Pengamanan Data, Enkripsi, Deskripsi, Algoritma AES-256, SHA- 256

1. Pendahuluan

Data yang bersifat pribadi menjadi objek yang disenangi oleh *hacker* untuk dimanupulasi, dipermaikan dan digunakan tidak pada semestinya. Oleh karena itu data yang bersifat pribadi atau rahasia perlu dijaga keamanannya. Ada beberapa teknik pengamanan data, diantaranya adalah teknik enkripsi. Enkripsi merupakan sebuah proses pengubahan sebuah pesan atau informasi dari yang bisa dimengerti

atau dibaca menjadi sebuah pesan atau informasi yang sulit dimengerti hingga tidak terbaca sama sekali.Teknik enkripsi dapat mengamankan data karena data dapat berubah menjadi tidak terbaca sesuai dengan aslinya. Dan data yang terenkripsi dapat terbaca lagi apabila sudah di deskripsi dengan menggunakan kunci yang tepat. Dan dengan mengenkripsi data file yang penting atau rahasia dapat meningkatkan keamanan data yang bersifat rahasia tersebut.

Kriptografi merupakan studi matematika yang mempunyai hubungan dengan aspek keamanan informasi seperti integritas data, keaslian entitas dan keaslian data (Ratno Prasetyo, 2016). Dalam ilmu kriptografi terdapat dua proses penyandian yang disebut enkripsi dan deskripsi. Enkripsi dilakukan pada proses pengiriman pesan atau informasi dengan cara mengubah data asli kedalam bentuk kode kode yang menjadikannya data rahasia sedangkan deskripsi dilakukan pada proses penerimaan dengan cara mengubah data yang berisi kode kode rahasia tersebut ke dalam bentuk data yang asli dan mudah dimengerti.

Pada tanggal 29 September 2020 berita tentang serangan ransomeware yang melumpuhkan salah rumah sakit di Amereka Serikat akibatnya data data penting rumah sakit habis terenkripsi oleh sebuah virus, ransomeware sendiri ialah salah satu jenis malware berbahaya yang menyerang sistem komputer untuk mengenkripsi file didalamnya. Maka dari itu diperlukannya enkripsi file untuk file yang dianggap penting oleh user. Oleh karena itu universitas Bhayangkara Jakarta Raya sebagai perguruan tinggi swasta yang terletak di kota Bekasi, Jawa Barat. Pada Universitas Bhayangkara Jakarta Raya mempunyai banyak data file penting yang bersifat rahasia suatu lembaga, seperti data data keuangan dan data penting lainnya pada komputer atau laptop di lembaga mereka. Dan apabila data tersebut bisa saja dicuri dan dimanipulasi pada suatu kejadian yang dapat merugikan lembaga. Data keuangan yang tidak terenkripsi atau tidak dirahasiakan dapat dengan sangat mudah dimanipulasi oleh orang yang tidak bertanggung jawab untuk mengambil keuntungan di lembaga yang bergerak dibidang pendidikan tersebut, seperti dikorupsi pada jumlah pengeluaran untuk biaya operasional perusahaan tersebut dan biaya biaya lainnya dan apabila data data tersebut di hack oleh virus yang terjangkit di dalam computer seperti data keuangan dan data penting lainnya maka data tersebut akan terenkrip dengan virus dan tidak bisa dikembalikan lagi datanya. Terdapat metode algoritma kriptografi yang cocok untuk memecahkan masalah pengamaanan data lembaga tersebut, yaitu salah satunya adalah metode AES dan SHA. *Advanced Encryption Standar* (AES) adalah algoritma kriptografi simetris modern yang beroperasi dalam mode penyandian blok (*block cipher*) yang memproses blok data dengan ukuran 128-bit dengan panjang kunci 128-bit, 192-bit, atau 256-bit (Asep Suryana, 2016). Terdapat beberapa mode dalam algoritma AES diantaranya mode CBC, ECB, OFB, CTR dan CFB untuk penyadian dengan metode *block cipher*.

Tinjauan Pustaka

a. Kriptografi

Istilah kriptografi, *cryptography* berasal dari bahasa Yunani yaitu, "*cryptos*" yang artinya "*secret*" atau rahasia sedangkan "*graphien*" yang artinya "*writing*" atau tulisan, sehingga kriptografi berarti secret writing yang artinya tulisan rahasia. Pengertian kriptografi secara lebih luas adalah Kriptografi adalah ilmu yang

mempelajari mengenai bagaimana cara mengamankan suatu informasi. Pengamanan ini dilakukan dengan mengenkrip informasi tersebut dengan suatu kunci khusus (Didi Surian, 2006). Dan Menurut *Request for Comments* (RFC), kriptografi merupakan cabang ilmu matematika yang berhubungan dengan transformasi data untuk embuatnya artinya tidak dapat dipahami (untuk menyembunyikan maknanya atau isi dari sebuah data), mencegahnya dari perubahan tanpa izin, atau mencegahnya dari penggunaan yang tidak sah. Jika transformasinya dapat dikembalikan, kriptografi juga bisa diartikan sebagai proses mengubah kembali data yang terenkripsi menjadi bentuk yang dapat dipahami. Jadi dapat disimpulkan bahwa kriptografi dapat diartikan sebagai cabang ilmu matematika untuk menjaga kerahasiaan informasi dengan metode teknik matematika yang mencakup, kerahasiaan, integritas data, autentifikasi, dan non repudiasi.

b. Enkripsi dan Deskripsi

Dalam kriptografi terdapat proses didalamnya yang disebut sebagai proses enkripsi dan deskripsi. Proses penyandian pesan asli (plain text) menjadi pesan yang tidak dapat dibaca (*chipper* text) adalah enkripsi (Pandi Barita, 2018), sedangkan kebalikan dari proses enkripsi ialah deskripsi yaitu mengembalikan pesan yang sudah disandikan tersebut dan tidak dapat terbaca menjadi pesan aslinya yang dapat dibaca kembali, proses tersebut adalah deskripsi (Komariah Fitri, 2018). Pesan tersebut dapat data atau informasi yang berbentuk teks, dokumen, gambar serta suara yang bersifat penting dan rahasia.

Sistem yang mendasari terjadinya sebuah proses enkripsi dan dekripsi ialah hubungan antara dua himpunan yaitu yang berisi sebuah elemen pesan asli (plaintext) dan sebuah pesan yang berisi elemen pesan sandi (ciphertext). Enkripsi dan dekripsi merupakan fungsi transformasi antara himpunan-himpunan tersebut. P adalah notasi yang digunakan untuk plaintext, C adalah *ciphertext*, E adalah fungsi *Encryption* dan D adalah fungsi *Decryption*. Sedangkan untuk kunci dapat dinotasikan sebagai K atau *Key.*

c. *Advanced Encryption Standard* (AES-256)

Algoritma AES mendukung berbagai variasi ukuran kunci yang digunakannya. Jenis ukuran kunci yang algoritma AES terbagi tiga, yaitu AES-128, AES-193 dan AES-256. Perbedaan jenis ukuran block dan kunci yang algoritma AES miliki yaitu karena perbedaan ukuran kunci yang akan menentukan jumlah proses yang harus dilalui pada saat pengenkripsian dan pengdeskripsian atau lebih mudahnya dan dapat disimpulkan perbedaan pada banyaknya round atau putaran yang dipakai pada proses enkripsi dan deskripsi.

d. *Secure Hash Algorithm* (SHA-256)

Dalam enkripsi data dikenal suatu fungsi yang di sebut fungsi *hash* atau *hashing*. Fungsi hash adalah adalah fungsi yang menerima masukan string yang panjangnya sembarang dan dikonversikan menjadi string dengan keluaran yang panjangnya tetap (Santi Sulastri, 2018). Fungsi hash yang berbeda akan menghasilkan output-output yang berbeda ukuran, tetapi kemungkinan ukuran output dari masing-masing algoritma hashing selalu konstan. Sebagai contoh, algoritma SHA-256 hanya akan menghasilkan message digest 256 bit, sedangkan SHA-1 selalu akan menghasilkan digest 160-bit.

2. Metode Penelitian

A.1. Objek Penelitian

Adapun objek dari penelitian ini adalah pada divisi administrasi untuk pengamanan data file. Pengumpulan informasi dan data sekunder dilakukan di Fakultas Ilmu Komputer Program Studi Informatika Universitas Bhayangkara Jakarta Raya, Jl. Raya Perjuangan Bekasi Utara, Kota Bekasi, Jawa Barat 17121, Indonesia.

A.2. Pendekatan Penelitian

Adapun pendekatan penelitian yang digunakan dalam penelitian ini adalah perancangan aplikasi dimulai dari analisa sistem yang meliputi tahapan sistem yang akan dibuat sebagai konsep, objek dan keterkaitannya serta analisa solusi dari algoritma dan kebutuhan aplikasi. Analisa ini ditranlasikan kedalam bentuk pemodelan UML yaitu use case diagram, activity diagram serta sequence diagram sebagai bentuk dari peracangan sebuah aplikasi yang akan dibuat.

A.3. Pengumpulan Data

Pengumpulan data secara langsung ialah dengan mewawancarai pihak terkait dengan menanyakan jenis data apa yang biasanya bersifat rahasia untuk dijaga keamanannya, yaitu apakah data tentang keuangan yang berformat excel atau ekstensi file data rahasia lainnya. Ada 3 teknik pengumpulan data, yaitu :

a. Pengamatan Langsung (Observasi)

b. Data Sekunder

c. Studi Pustaka

3. Hasil Dan Pembahasan

A. Hasil Penelitian

Penerapan *Secure Hash Algorithm* (SHA-256)

Algoritma SHA yang digunakan ialah SHA-256, yang hanya menghasilkan message digest sebesar 256 bit. SHA-256 mengubah pesan masukan ke dalam message digest 256 bit, berdasarkan *Secure Hash Signature Standard.* Lebih mudahnya plaintext diproses dengan fungsi *hash* lalu keluaran tersebut menjadi *hash* text yang tidak dapat terbaca.

Penerapan *Advanced Encryption Standard* (AES-256)

Penerapan algoritma Advanced Encryption Standard (AES-256) dengan mode *Chiper Block Chaining* (CBC), salah satu mode operasi AES yaitu CBC atau yang disebut *Chiper Block Chaining*. Pada algoritma blok chipper seperti AES ini, plaintext atau pesan mentah yang masuk untuk diproses dengan panjang yang tetap yaitu n, akan tetapi jika ukuran datanya terlalu panjang maka dilakukan pemecahan data data tersebut menjadi blok blok dengan ukuran yang lebih kecil. Pada CBC, rangkaian bit-bit pada plaintext dibagi menjadi blok blok bit dengan panjang yang sama. Mode CBC memerlukan IV (*initialization vector*) untuk menggabungkan dengan plaintext pertama dan chipertext block sebelumnya menjadi IV di block selanjutnya.

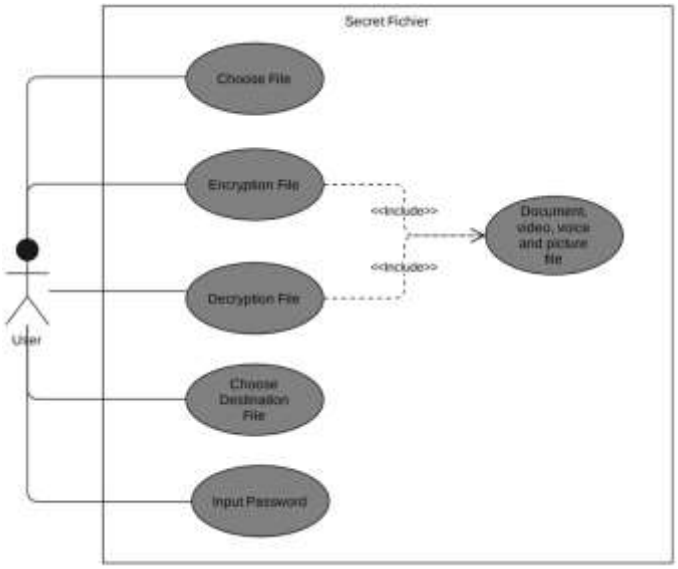
B. Pembahasan

Berdasarkan hasil penelitian yang telah dijelaskan, maka ada beberapa hal yang dibahas, antara lain sebagai berikut.

Perancangan Aplikasi

Pada tahap ini aplikasi mulai di rancang dengan permodelan UML (*Unified Modelling Language*), membuat stuktur yang ada didalam menu dan tampilan antar muka atau yang sering disebut User Interface dengan mempertimbangkan keefisiensian suatu aplikasi yang dibangun oleh peneliti. Rancangan aplikasi ini mencakup ;

a. Sistem yang ada didalam aplikasi yaitu tampilan menu utama yang berisikan penginputan suatu file dengan radio button untuk pemilihan opsi proses enkripsi atau dekripsi dan menu proses untuk pemilihan destinasi file apabila telah di proses dan penginputan password atau kunci sebelum terjadinya proses enkripsi dan deksripsi. Diharapkan dengan mengedepankan suatu aplikasi yang efisien tanpa mengurangi suatu kegunaan dari aplikasi tersebut.
b. Pemodelan aplikasi menggunakan *Unified Modelling Language* (UML), yang terdiri dari Use Case Diagram, Activity Diagram dan Sequence Diagram.



Sumber: Hasil Penelitian (2021)

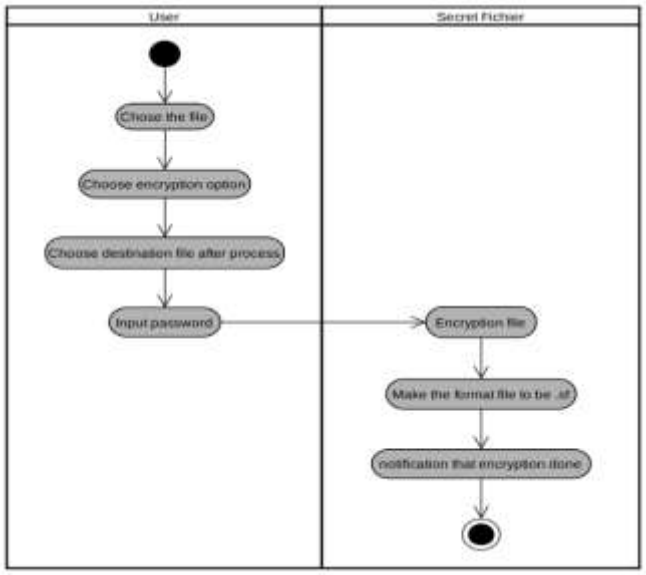
Gambar 1 Use Case Diagram Aplikasi Secret Fichier

Penjelasan gambar :

i. Pada *usecase* tersebut, actor atau user membuka aplikasi Secret Fichier maka tampilan awal dari Secret Fichier ialah form dashboard. Lalu user dapat memilih file yang akan di enkripsi atau di dekripsi dengan choose file button dengan catatan file yang akan di enkripsi ialah file tunggal bukan sebuah folder dan file yang akan di dekripsi ialah sebuah file dengan eksitensi format .sf.
ii. Lalu, setelah user memilih file yang akan di process, ada dua buah opsi radio button yaitu encryption process dan decryption process. Dengan catatan file yang akan diproses yaitu file dokumen, gambar, suara dan video. Setelah dipilih proses mana yang akan dilakukan, lalu tombol start akan aktif dan menampilkan form process.

iii. Selanjutnya di form process akan di tampilkan button file destination yang akan digunakan user untuk memilih tempat atau folder untuk file yang sudah di enkripsi atau di dekripsi.

iv. Setelahnya user harus menginput sebuah password lebih dari 8 (delapan) character untuk menguci serta memproses file tersebut. Setelah file selesai di proses maka aplikasi akan balik ke halaman awal.



Sumber: Hasil Penelitian (2021)

Gambar 2 Activity Diagram Enkripsi File

Penjelasan Gambar Activity Diagram Enkripsi File :

i. Pada awal masuk aplikasi Secret Fichier, user akan ditampilkan form dashboard yang berisikan tampilan penginputan file yang akan diproses yang dinamain choose file. File yang akan di enkripsi hanya suatu file tunggal (bukan folder) yaitu file yang berjenis dokumen, suara, gambar dan video.

ii. Lalu pada saat file diinput, tampilan text box akan menunjukan file itu berada, dan user akan memilih opsi encryption button pada radio button yang tersedia.

iii. Setelah user mengklik tombol encryption dan tombol start akan aktif, tombol tersebut menghubungkan user ke form selanjutnya yaitu form process.

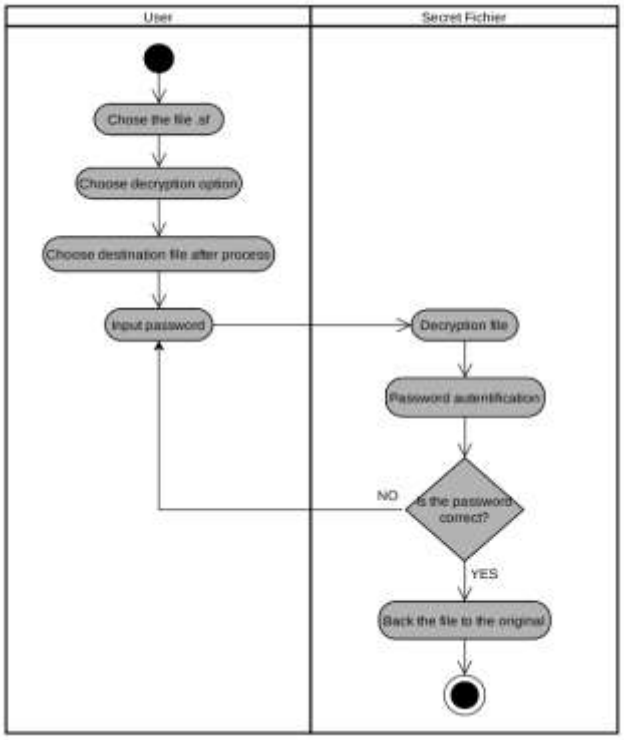
iv. Lalu user akan ditampilkan form process dimana user akan memilih tempat file yang akan ditaruh apabila proses pengenkripsian telah selesai dan penginputan password atau kunci untuk memulai pengenkripsian file tersebut.

v. User akan mengklik button destination dimana user memilih dimana file tersebut akan ditaruh setelah proses selesai. Dalam proses tersebut, user dapat me-rename file tersebut. Mengganti nama file yang ingin dienkrispi berbeda dengan file aslinya.

vi. Setelah menentukan letak file setelah proses, user harus menginputkan password atau kunci unik yang tidak mudah ditebak sebanyak 8 (delapan) character sebagai kunci file yang akan

dienkripsi, kunci tersebut berguna kembali apabila user ingin mendekripsikan kembali file yang telah di enkrip.

vii. Lalu user mengklik button process dan pengenkripsian file tersebut terjadi.



Sumber: Hasil Penelitian (2021)

Gambar 3 Activity Diagram Dekripsi File

Penjelasan Gambar Activity Diagram Dekripsi File :

i. Pada awal masuk aplikasi Secret Fichier, user akan ditampilkan form dashboard yang berisikan tampilan penginputan file yang akan diproses yang dinamain choose file. File yang akan di dekripsi hanya suatu file tunggal (bukan folder) yaitu file yang berformat .sf.

ii. Lalu pada saat file diinput, tampilan text box akan menunjukan file itu berada, dan user akan memilih opsi decryption button pada radio button yang tersedia.

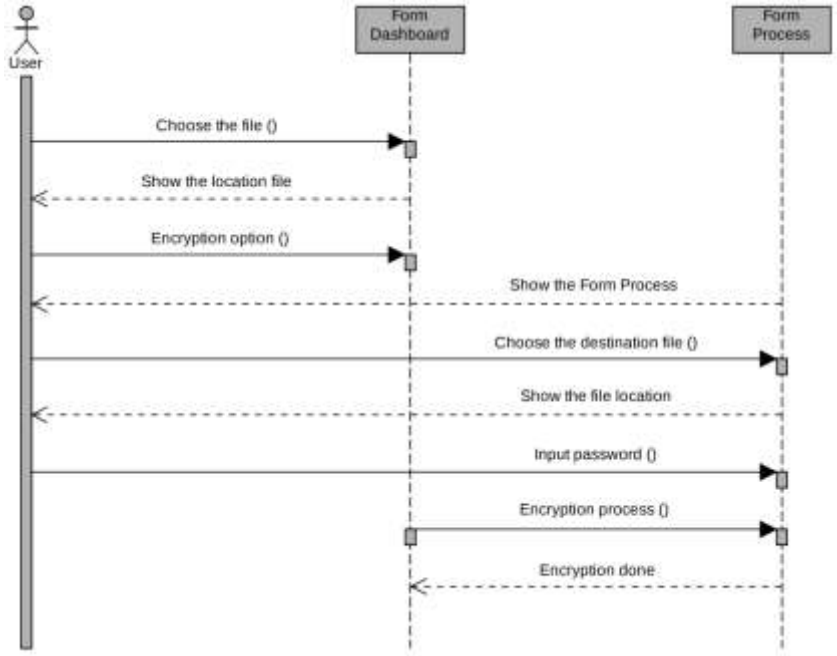
iii. Setelah itu user mengklik tombol start, dan user akan ditampilkan form process. Didalam form process tersebut process pengdekripsian terjadi.

iv. Didalam form process, user akan mengklik button destination dimana user dapat memilih dimana file tersebut akan ditaruh setelah proses selesai. Dalam proses tersebut, user dapat me-rename file tersebut. Mengganti nama file yang ingin didekrispi berbeda dengan file enkripsinya.

v. Setelah menentukan letak file setelah di proses, user diharuskan menginputkan kembali password atau kunci yang telah dibuat sebelumnya pada proses pengenkripsian file. Setelah mengklik tombol proses button, terdapat decision proses dimana kunci tersebut benar atau tidak. Jika kunci tersebut benar maka proses pendekripsian selesai.

vi. Apabila kunci yang di inputkan salah makan user akan diminta kembali memasukan kunci yang benar.

vii. Setelah proses selesai user akan di kembalikan ke form dashboard.



Sumber: Hasil Penelitian (2021)

Gambar 4 Sequence Diagram Enkripsi File

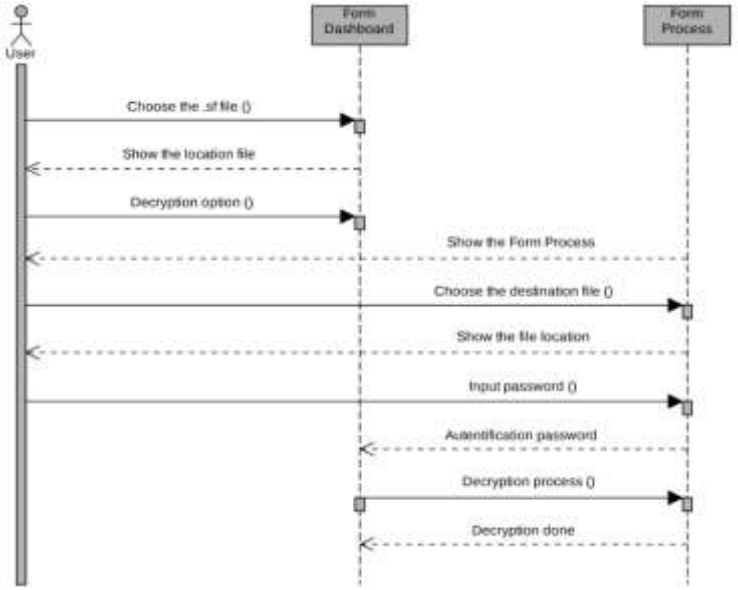
Penjelasan Gambar :

i. Dalam sequence diagram ini terdapat 1 user atau yang disebur aktor, 2 lifeline yaitu form dashboard dan form process yang ada di secret fichier, dan 9 messages.

ii. Pertama kali user membuka aplikasi, tampilan awalnya ialah form dashboard untuk menginput file yang ingin diproses,

iii. Lalu user menentukan proses dan klik start button, lalu tampilan form process muncul.

iv. Pilih destination file untuk file yang setelah di proses. Dan user menginputkan password lalu proses enkripsi terjadi.



Sumber: Hasil Penelitian (2021)

Gambar 5 Sequence Diagram Dekripsi File

Penjelasan Gambar :

i. Pada sequence diagram dekripsi file ini terdapat 1 user, 2 lifeline yaitu form dashboard dan form process yang ada di dalam aplikasi secret fichier, dan 10 messages.

ii. Pertama kali user membuka aplikasi, tampilan awalnya ialah form dashboard untuk menginput file yang ingin diproses, dalam dekripsi file di aplikasi secret fichier ini, format file harus .sf.

iii. Lalu user menentukan proses enkripsi dan klik start button, lalu tampilan form process muncul.

iv. Pilih destination file untuk lokasi file setelah di proses lalu user harus menginput kembali password awal pada pengengkripsian file.

v. Pada proses tersebut terdapat autentifikasi password, apabila password benar maka file akan kembali seperti semula, apabila password salah maka dekripsi file tidak berhasil.

c. Perancangan antar muka aplikasi yaitu penggambaran tampilan menu menu yang akan dibuat dan ditampilkan didalam aplikasi yang dibangun.

Sumber: Hasil Penelitian (2021)

Gambar 6 Desain Dashboard

Sumber: Hasil Penelitian (2021)

Gambar 7 Desain Form Process

Sumber: Hasil Penelitian (2021)

Gambar 8 Desain Tampilan *Form About*

4. Kesimpulan dan Saran

A. Kesimpulan

Kesimpulan yang dapat diambil berdasarkan hasil dari pengujian serta analisis penerapan algoritma Advanced Encryption Standard (AES-256) dengan mode Chiper Block Chaining (CBC) dan Secure Hash Algorithm (SHA-256) terhadap aplikasi yang telah dibuat yaitu aplikasi enkripsi dan dekripsi file berbasis Windows yaitu Secret Fichier. Dapat disimpulkan beberapa point sebagai berikut :

a. Aplikasi Secret Fichier dapat mengenkripsi file dengan berbagai ekstensi seperti file dokumen, file suara (voice note/mp3), file video serta file gambar dengan baik dan dapat didekripsikan kembali dengan kunci yang sama pada aplikasi Secret Fichier, apabila user ingin mengenkripsi sebuah folder, maka dari itu diharuskan meng-ekstrak menjadi .zip atau .rar terlebih dahulu.

b. Algoritma AES mode CBC dan SHA yang diterapkan di aplikasi dapat berjalan dengan baik tanpa kendala di aplikasi Secret Fichier untuk mengenkripsi file dan mendekripsikan nya di dalam sistem operasi Windows 10 64 bit.

c. Algoritma AES dan SHA dapat dibilang masih cukup aman didalam pemprosesannya dikarenakan mempunyai kunci yang panjang dan tahapan perhitungan yang cukup rumit di dalamnya.
d. Waktu proses pengenkripsian file tergantung pada besaran ukuran file yang di proses (bytes).
e. Pada proses pengenkripsian file terdapat perbedaan ukuran file asli dengan file yang dienkripsi dikarenkan adanya proses padding didalam proses pengenkripsian tersebut, sehingga menunjukan perbedaan ukuran file asli dengan file yang telah di enkripsi.

B. Saran

Untuk penelitian lebih lanjut, perlu dipertimbangkan kembali berdasarkan kesimpulan yang telah dipaparkan diatas. berikut untuk saran saran untuk penelitian selanjutnya :

a. Untuk penelitian selanjutnya, disarankan untuk dapat mengenkripsi file dengan berukuran lebih besar dan dapat dijalan di sistem operasi lainnya (tidak hanyak windows).
b. Untuk penelitian selanjutnya, pertimbangkan kembali untuk menggunakan mode operasi yang lainnya, seperti CFB (Chiper FeedBack), OFB (Output FeedBack) atau GCM (Galois Counter Mode).
c. Untuk penelitian selanjutnya, disarankan untuk dapat menggunakan seri SHA terbarukan yaitu SHA-3.
d. Untuk penelitian selanjutnya, pertimbangkan kembali untuk menggunakan algoritma asimetris. Dimana memiliki dua kunci yang berbeda untuk keamanannya.
e. Untuk penelitian selanjutnya, aplikasi Secret Fichier dapat dikembangkan dan diterapkan pada mobile atau menjadi sebuah fitur independent dalam sebuah aplikasi messenger.

DAFTAR PUSTAKA

Ambler, S. W. (2005). The Elements of UML 2.0 Style. New York: Cambridge University Press.

Ariyus, D. 2008. Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi, Yogyakarta : Andi.

Henry, Kridalaksana, A. H., & Arifin, Z. (2016). Kriptografi AES Mode CBC Pada Citra Digital Berbasis Android. Prosiding Seminar Ilmu Komputer dan Teknologi Informasi, 45-52.

Ichwan, M., Gustiana, M., & Nurjaman, N. R. (2016). Implementasi Keyed-Hash Message Authentatication Code Pada SistemKeamanan Rumah. MIND Journal, 9-18.

Menezez, Alfred., Vanstone, S., & Oorschot, P. (2006). Handbook of Applied Cryptography. Boston: Massachusetts Institute of Technology.

Prasetyo, R., & Surayana, A. (2016). Aplikasi Pengamanan Data dengan Teknik Algoritma Kriptografi AES dan Fungsi Hash SHA-1 Berbasis Desktop. Jurnal SISFOKOM, 61-65.

Renaldy, M. (2015). Implementasi Kriptografi Pada Diary Berbasis Mobile Android Dengan Menggunakan Metode AES-128 (Advanced Encryption Standard-128) Dan SHA-1 (Secure Hashing Algorithm-1). Tugas Akhir, 7- 19.

Simangunsong, P. B. N., & Fitri, K. (2018). Perancangan Aplikasi Pengamanan Citra Bewarna Dengan Algoritma RSA. Jurnal Teknik Informatika, 99-107 Surian, D. (2006). Algoritma Kriptografi AES Rijndael. Jurnal Teknik Elektro, 97-101.

Sulastri, S., & Putri, R. D. M. (2018). Implementasi Enkripsi Data Secure Hash Algorithm(SHA-256) dan Message Digest Algorithm (MD5) pada Proses Pengamanan Kata Sandi Sistem Penjadwalan Karyawan. Jurnal Teknik Elektro, 70-74.

Wiguno, H. F. (2017). Aplikasi Pengamanan File Dan Pesan Teks Menggunakan AES 256 Dan SHA 256 Berbasis Android. Tugas Akhir, 33-49.

Yusmantoro, S., Hermansyah, E., & Efendi, R. (2014). Rancang Bangun Aplikasi Pengamanan Keaslian Surat Izin Tempat Usaha Menggunakan Algoritma Elgamal Dan Secure Hash Algorithm 256 Studi Kasus : Badan Pelayanan Perizinan Terpadu (BPPT) Kota Bengkulu. Jurnal Rekursif, 28-36.