Terbit online pada laman web jurnal : **http://seminar.iaii.or.id**

PROSIDING
SEMINAR NASIONAL SISFOTEK
(Sistem Informasi dan Teknologi)
Padang, 4 – 5 September 2018 ISSN Media Elektronik 2597-3584

Implementasi Algoritma AES dalam Mengenkripsi Berkas Terintegrasi dengan Layanan *Cloud Storage* Berbasis Android

Dedi Kurniawan[a], Rita Afyenni[b], Rahmat Hidayat[c]
[a]Program Studi Teknik Komputer, Teknologi Informasi, Politeknik Negeri Padang, awanchaniago5@gmail.com
[b]Program Studi Manajemen Informatika, Teknologi Informasi, Politeknik Negeri Padang, afyennirita@gmail.com
[c]Program Studi Teknik Rekayasa Perangkat Lunak, Teknologi Informasi, Politeknik Negeri Padang, mr.rahmat@gmail.com

Abstract

In the development of increasingly advanced technology, the security of a data is something that must be considered in maintaining the confidentiality of information. The data contained in the file contain information that can only be known by certain parties. In general, files are stored or shared into a storage that can be accessed using the internet or known as cloud storage. There are ways to secure information on a file so that it cannot be hacked or read to unauthorized parties, namely by using cryptographic methods. Cryptography is a technique to improve the security aspect of information. Cryptography is used to convert information that can be read into unreadable and return an information that was previously unreadable to be legible. In this study cryptography uses the Advanced Encryption Standard (AES) algorithm and Google Drive cloud storage services.

Keywords: encryption, decryption, cloud storage, AES, android

Abstrak

Pada perkembangan teknologi yang semakin maju, keamanan suatu data merupakan hal yang harus diperhatikan dalam menjaga kerahasiaan informasi. Data yang ada di dalam berkas mengandung informasi-informasi yang hanya boleh diketahui oleh pihak-pihak tertentu. Pada umumnya, berkas disimpan atau dibagikan ke dalam suatu penyimpanan yang dapat diakses dengan menggunakan internet atau yang dikenal dengan penyimpanan awan atau *cloud storage*. Ada cara untuk mengamankan informasi suatu berkas agar tidak dapat diretas atau dibaca kepada pihak yang tidak berwenang, yaitu dengan menggunakan metode kriptografi. Kriptografi merupakan suatu teknik untuk meningkatkan aspek keamanan suatu informasi. Kriptografi digunakan untuk mengubah suatu informasi yang dapat dibaca menjadi tidak dapat dibaca dan mengembalikan suatu informasi yang sebelumnya tidak dapat dibaca menjadi bisa terbaca. Pada penelitian ini kriptografi menggunakan algoritma Advanced Encryption Standard (AES) dan layanan *cloud storage* Google Drive.

Kata kunci: enkripsi, dekripsi, *cloud storage*, AES, android

1. Pendahuluan

Pada perkembangan teknologi saat ini keamanan suatu data merupakan hal yang harus diperhatikan dalam menjaga kerahasiaan informasi. Khususnya informasi yang hanya boleh diketahui oleh pihak tertentu. Pada umumnya, data atau informasi yang dikirim tanpa melakukan proses pengamanan. Hal ini berisiko terhadap adanya upaya penyadapan sehingga informasi tersebut diketahui oleh pihak lain yang tidak berhak.

Salah satu upaya untuk pengamanan data adalah dengan melakukan proses enkripsi pada data tersebut. Enkripsi merupakan suatu cara dalam proses perubahan kode dari yang dapat dimengerti menjadi tidak dapat dimengerti atau tidak terbaca. Enkripsi memiliki kode atau *chiper*. *Chiper* menggunakan algoritma yang dapat mengkodekan semua aliran data yang disebut *stream bit* sehingga pesan menjadi *cryptogram* yang tidak dapat dimengerti. Selanjutnya, pengembalian informasi asli dapat dilakukan dengan proses dekripsi menggunakan kunci yang benar.

Algoritma digunakan untuk menjaga keamanan data. Baik data berupa dokumen, audio, gambar, dan video. Jenis algoritma yang biasa digunakan untuk mengamankan data diantaranya AES, XOR256 Block, DES, SEAL dan RSA. Pembahasan berikut ini akan menggunakan algoritma AES untuk pengamanan data

dan menggunakan *cloud storage* sebagai media penyimpanan hasil file yang sudah dienkripsi. *Cloud storage* merupakan media penyimpanan yang dalam pengaksesannya memerlukan jaringan internet dan tidak memiliki bentuk fisik dalam penggunaannya. Dalam keamanan *cloud storage* dilindungi oleh kata sandi yang bisa saja diketahui oleh pihak lain dan beberapa sistem *cloud storage* menyediakan fungsi agar pihak tertentu dapat mengakses data yang dimiliki sehingga informasi dalam data dapat diketahui oleh pihak lain.

Implementasi algoritma AES pada semua jenis berkas diharapkan dapat meningkatkan keamanan data yang disimpan pada *cloud storage* agar terhindar dari penyadapan serta informasi tidak dapat diketahui oleh pihak lain.

2. Tinjauan Pustaka

2.1 Definisi Kriptografi

Kriptografi adalah cara dalam menjaga keamanan informasi atau pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak dapat dibaca. Bentuk tersandi tersebut hanya bisa dibaca atau diketahui oleh pihak yang berhak untuk membacanya seperti penerima atau pengirim pesan. Pesan atau informasi yang belum disamarkan disebut dengan *plaintext*, sedangkan pesan yang sudah disamarkan disebut dengan *chipertext*. Enkripsi merupakan cara penyamaran sebuah pesan asli menjadi tidak terbaca, sedangkan proses mengembalikannya menjadi dapat terbaca disebut dengan dekripsi[1].

Kriptografi didukung dengan algoritma yang baik sehingga membutuhkan watu yang lebih agar memecahkan pesan yang sudah tersandikan. Seiring dengan perkembangan teknologi, membutuhkan algoritma kriptografi yang lebih aman dan kuat. Algoritma kriptografi modern terbagi dalam dua kategori, yaitu algoritma kunci simetrik dan kunci asimetrik. *Advanced Encryption Standard* (AES) termasuk dalam algoritma kriptografi kunci simetrik yang sangat baik, dan merupakan algoritma *chiper block* yang menggunakan teknik permutasi, subtitusi dan sejumlah putaran pada setiap blok yang akan dienkripsi[1].

2.2 Advanced Encryption Standard (AES)

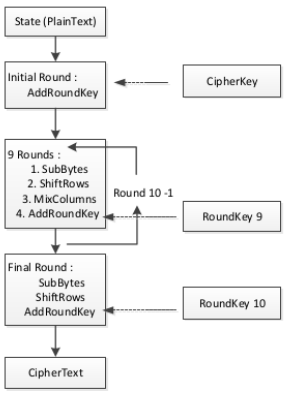
AES merupakan algoritma kriptografi bernama Rijndael yang dirancang oleh Vincent Rijmen dan John Daemen yang berasal dari Belgia. Mereka merupakan pemenang kontes algoritma kriptografi pengganti *Data Encryption Standard* (DES) yang diadakan oleh *National Institutes of Standards and Technology* (NIST) di Amerika Serikat pada tanggal 26 November 2001. Algoritma Rijndael inilah yang kemudian dikenal sebagai AES. Pada tanggal 22 Mei 2006 AES mengalami proses penyesuaian oleh NIST, kemudian diangkat menjadi ukuran algoritma kriptografi. AES merupakan algoritma *cipher block* dengan menggunakan sistem subtitusi dan permutasi (P-Box dan S-Box) bukan dengan jaringan *Feistel* yang digunakan oleh cipher block pada umumnya. Jenis AES terbagi menjadi tiga, yaitu AES-128, AES-192, dan AES 256. Kelompok AES ini berdasarkan dari panjang kunci yang digunakan pada proses enkripsi dan dekripsi. Angka yang terdapat di belakang kata AES merupakan panjang kunci yang akan digunakan oleh AES untuk mengenkripsi. Terdapat perbedaan pada masing-masing AES dalam menggunakan sejumlah round yang digunakan seperti pada tabel 1.[3]

Tabel 1.Perbedaan Jenis AES dalam Pengoperasian Enkripsi dan Dekripsi

Jenis AES	Panjang Kunci	Panjang Blok Input	Jumlah Putaran
AES-128	128 bit	128 bit	10
AES-192	192 bit	128 bit	12
AES-256	256 bit	128 bit	14

1 Enkripsi AES

Algoritma *Advanced Encryption Standard* memiliki empat jenis perubahan bytes, yaitu *MixColumns, SubBytes, ShiftRows* dan *AddRoundKey*. Dalam proses enkripsi, masukan yang telah disalin ke dalam *state* akan mengalami perubahan *byte AddRoundKey*. Setelah itu , state akan mengalami perubahan *MixColumns, SubBytes, ShiftRows* dan *AddRoundKey* secara berulang-ulang sebanyak *Nr*. Proses tersebut dalam algoritma AES dikenal dengan *round function*. Pada round terakhir memiliki perbedaan seperti *round* sebelumnya, karena pada *round* terakhir *state* tidak mengalami perubahan *Mixcolumns*. Proses enkripsi AES dapat dilihat pada gambar 1.[4]

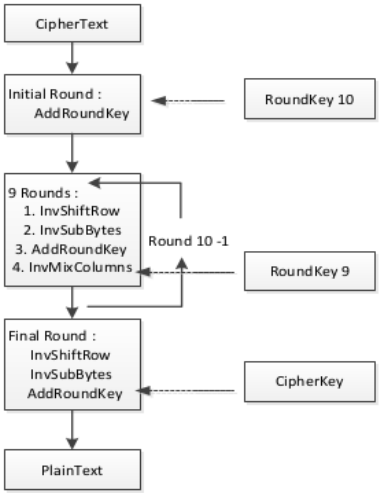


Gambar 1. Proses Enkripsi AES

2 Dekripsi AES

Perubahan dari sebuah *cipher* dapat diimplementasikan dan dibalikkan dengan arah yang tidak sama agar menghasilkan *inverse cipher* yang dapat dipahami dalam algoritma AES. *Inverse cipher* yang menggunakan transformasi *byte* adalah *InvMixColumns, InvSubBytes, InvShiftRows,* dan

AddRoundKey. Proses dekripsi AES dapat dilihat pada gambar 2.[4]



Gambar 2. Proses Dekripsi AES

2.3 *Cloud Storage*

Cloud storage atau biasa dikenal dengan penyimpanan awan merupakan salah satu layanan yang diberikan oleh teknologi *cloud computing* (komputasi awan) dimana layanan berada pada sumberdaya yang digunakan bersama (shared resources) dalam suatu pusat data dengan menggunakan internet.

Cloud storage adalah sebuah layanan penyimpanan data online yang disatukan dan disesuaikan secara online dan dapat diakses dengan berbagai jenis perangkat (Windows, Linux, Android, iOS, Symbian, dan lain-lain). *Cloud storage* tidak memiliki bentuk fisik dalam penggunaannya sehingga data yang disimpan tidak akan hancur ataupun hilang.[5]

2.4 Android

Android merupakan perangkat keras mobile berbasis Linux yang merupakan cakupan dari sistem operasi, middleware dan aplikasi. Para pengembang dapat menciptakan aplikasi Android karena Android merupakan platform terbuka yang tidak dibatasi dalam pembuatan aplikasi berbasis Android. Pada awalnya Android dikembangan oleh perusahaan Android Inc., kemudian perusahaan tersebut diambil alih oleh perusahaan Google Inc. Dalam mengembangkan perangkat keras Android, dibentukah organisasi Open Handset Alliance (OHA), konsorsium dari 34 perusahaan telekomunikasi, perangkat keras dan perangkat lunak, termasuk Google, HTC, Intel, Qualcomm, Nvidia, Motorola dan T-Mobile. Android terdiri dari beberapa arsitektur yaitu:

1. *Application* dan *Widget*

Application dan Widget adalah layer yang berhubungan dengan aplikasi saja, dimana aplikasi di *download* lalu dilakukan instalasi kemudian aplikasi dijalankan.[6]

2. *Application Frameworks*

Application Frameworks merupakan layanan utnuk aplikasi dalam bentuk kelas java. Dalam *Application Frameworks* terdapat *Activity Manager, Content Providers, Resource Manager, Notification Manager* dan *View System*.[7]

3. *Libraries*

Libraries merupakan *layer* yang dimana fitur-fitur Android berada. *Libraries* digunakan untuk menjalankan aplikasi. Beberapa *libraries* terdiri dari berbagai jenis seperti *libraries* Media untuk memutar audio atau video, *libraries Graphic* untuk menjalankan tampilan, *libraries* SQLite digunakan untuk dukungan *database*, dan berbagai jenis *libraries* lainnya.[8]

4. *Android Run Time*

Android Runtime (ART) adalah waktu proses default dalam menjalankan perangkat keras Android. Selama proses ART sejumlah fitur meningkatkan kemulusan dan kinerja platform Android.[9]

5. Linux *Kernel*

Platform Android didasari dengan Linux *kernel* untuk menjalankan fungsionalitas dasar seperti manajemen memori tingkat rendah dan *threading* data. Dalam linux *kernel* dapat mengamankan Android dari segala macam virus atau *malware* yang dapat merusak sistem Android itu sendiri. Linux *kernel* yang digunakan oleh Android merupakan linux *kernel release* 2.6. [10]

3. Metodologi Penelitian

Metode yang digunakan dalam penelitian ini yaitu menggunakan metode Waterfall yang terdiri dari beberapa tahap, yaitu:

3.1 Tahap Analisa Kebutuhan

Pada tahap ini dilakukan menganalisis algoritma *Adavanced Encryption Standard* (AES) dengan perangkat lunak yang akan dibuat.

3.2 Tahap Perancangan

Pada tahap ini dilakukan perancangan terhadap perangkat lunak seperti perancangan proses, antar-muka pengguna dan struktur perangkat lunak dengan menggunakan UML.

3.3 Tahap Pengkodean

Pada tahap ini akan dilakukan proses implementasi algoritma AES ke dalam perangkat lunak dengan menggunakan bahasa pemrograman Java dengan *Integrated Development Environment* (IDE) Android Studio.

3.4 Tahap Pengujian

Pada tahap ini akan dilakukan pengujian enkripsi, dekripsi dan unggah ke dalam *cloud storage* dengan menggunakan format berkas yang berbeda.

4. Hasil dan Pembahasan

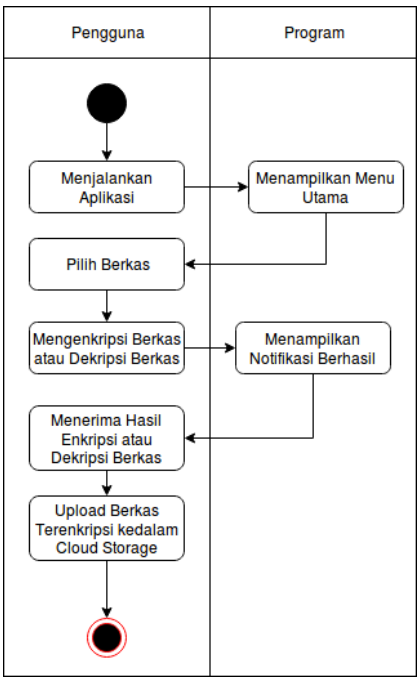
Setelah menerapkan metode penelitian maka hasil dari penelitian ini adalah aplikasi enkripsi dekripsi yang terintegrasi dengan cloud storage berbasis Android dengan menggunakan algoritma Advanced Encryption Standard (AES)

4.1 Perancangan Proses

Dalam merangcang proses aplikasi membutuhkan alat bantu UML (*Unified Modeling Language*) yang berupa *Activity* Diagram dan *Use-case* Diagram

1. *Activity* Diagram

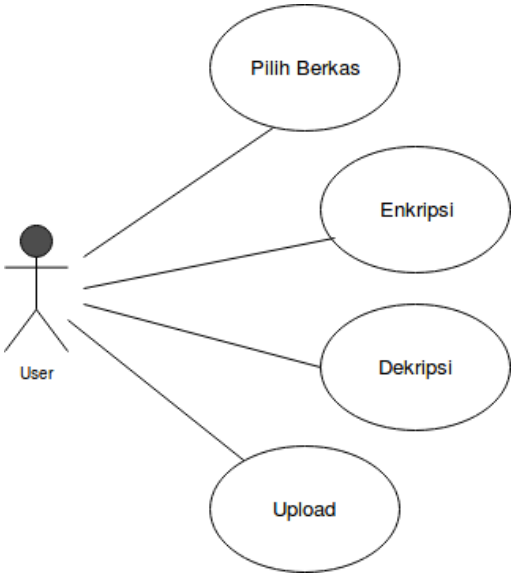
Activity diagram merupakan proses alur aktifitas dalam suatu program yang sudah dirancang secara rinci. Dalam perancangan *Activity* diagram pada aplikasi dijelaskan pada gambar 3.



Gambar 3. *Activity* Diagram Aplikasi

2. *Use-case* Diagram

Use-case Diagram merupakan interaksi antar satu atau lebih aktor dengan sistem yang akan dibuat. Interaksi yang digunakan pada perangkat lunak ini memiliki *Use-case* yang dapat dilihat pada gambar 4.



Gambar 4. *Use-case* Diagram Aplikasi

Berikut adalah deskripsi *Use -case* diagram di atas dapat dilihat pada tabel 2 dan tabel 3.

Tabel 2.Deskripsi Aktor

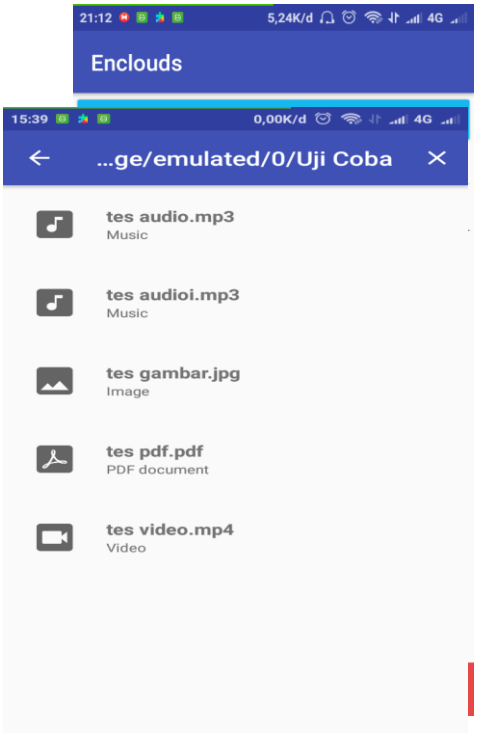
Actor	Deskripsi
User	Aktor yang berperan sebagai user atau pengguna adalah orang yang melakukan enkripsi dan dekripsi berkas.

Tabel 3.Deskripsi *Use-case*

No	Use-case	Deskripsi
1	Pilih Berkas	User atau pengguna memilih berkas yang akan dienkripsi atau didekripsi sebelum diunggah ke *cloud storage*.
2	Enkripsi	Berkas yang sudah dipilih oleh Berkas user akan dienkripsi.
3	Dekripsi	Berkas yang sudah dipilih oleh Berkas user akan didekripsi.
4	Upload	Hasil berkas yang sudah dienkripsi akan disimpan ke dalam penyimpanan data *cloud storage.*

4.2 Tampilan Aplikasi

Pada aplikasi enkripsi dekripsi yang terintegrasi dengan layanan *cloud storage* berbasis Android dengan algoritma AES memiliki beberapa komponen pada antar-muka aplikasi, yaitu lima tombol dan dua *edit text* yang dapat dilihat pada gambar 5.



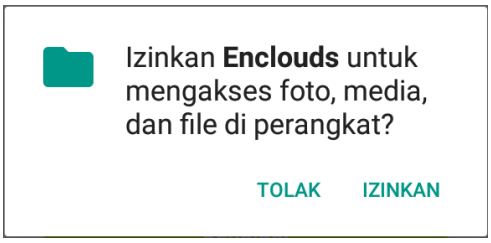
Gambar 5. Tampilan

4.3 Pengujian Aplikasi

Setelah membuat dan mengimplementasikan algoritma AES ke dalam aplikasi enkripsi dan dekripsi yang terintegrasi oleh layanan *cloud storage* di Android Studio, langkah selanjutnya adalah tahap pengujian. Tahap pengujian dilakukan untuk mengetahui apakah perangkat lunak sudah berjalan dengan baik. Berikut tahapan uji coba yang dilakukan.

1. Pengujian Izin Perangkat Android

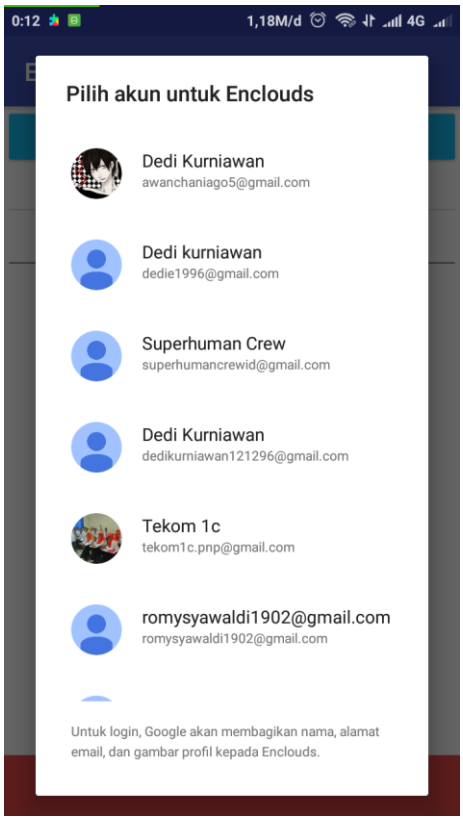
Ketika aplikasi pertama kali diinstal, maka akan muncul sebuah notifikasi yang akan memberitahukan fitur yang akan digunakan ketika pengguna menggunakan perangkat lunak enkripsi dan dekripsi yang terintegrasi oleh layanan *cloud storage* berbasis Android dengan algoritma AES seperti pada gambar 6.



Gambar 6. Izin pengaksesan data perangkat

2. Pengujian Akun *Cloud Storage* Pengguna

Ketika aplikasi pertama kali digunakan maka akan muncul sebuah *pop-up window* akun layanan *cloud storage* Google Drive yang dimiliki oleh pengguna. Akun Google ini akan terhubung dengan layanan Google Drive sehingga berkas yang akan diunggah dalam aplikasi terintegrasi dengan akun Google Drive yang dipilih seperti pada gambar 7.

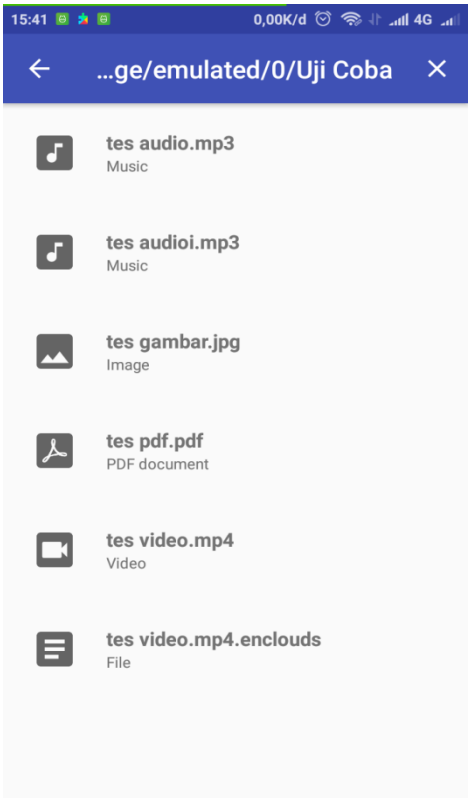


Gambar 7. Akun *cloud storage* google drive pengguna

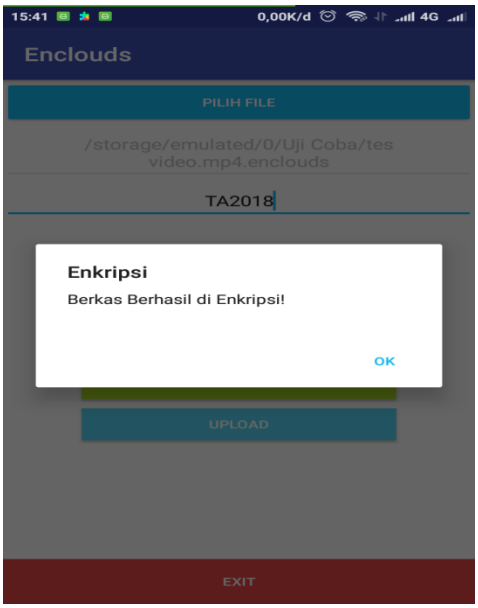
3. Pengujian Enkripsi Berkas

Langkah pertama untuk mengenkripsi ialah dengan memilih berkas yang akan dienkripsi dengan memilih tombol ‘Pilih File’ seperti pada gambar 8. Setelah memilih berkas yang akan dienkripsi maka berikan kata sandi sebagai kunci rahasia untuk mengembalikan berkas tersebut agar bisa dibaca kembali, kemudian tekan tombol ‘Enkripsi’ seperti pada gambar 9. Jika kata sandi tidak diberikan maka akan muncul sebuah notifikasi yang akan memberitahukan pengguna bahwa kata sandi belum diberikan seperti pada gambar 10.

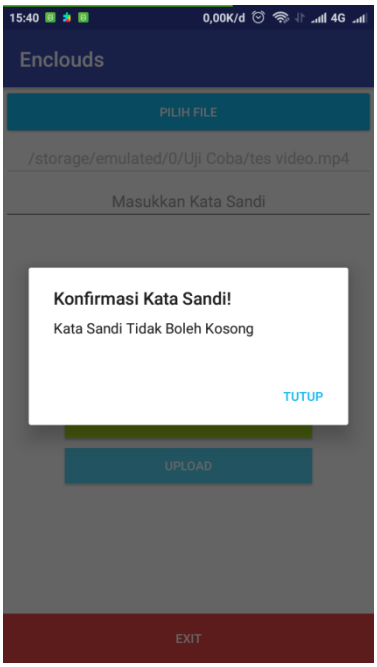
Ketika berkas berhasil dienkripsi maka akan muncul berkas baru yang berekstensi .enclouds sebagai penanda bahwa berkas sudah dienkripsi seperti pada gambar 11.



Gambar 8. Memilih berkas yang akan dienkripsi



Gambar 9. Notifikasi berkas berhasil dienkripsi

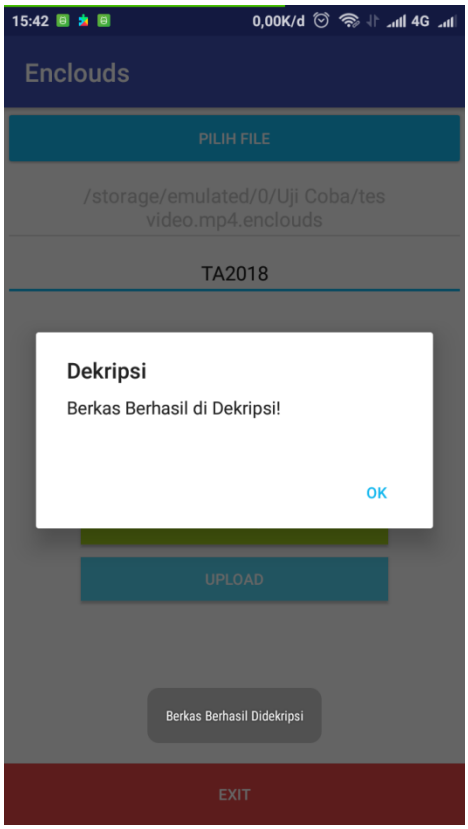


Gambar 10. Notifikasi jika kata sandi kosong

Gambar 11. Hasil berkas terenkripsi

4. Pengujian Dekripsi Berkas

Pada tahap ini pengguna dapat melakukan dekripsi berkas yang sudah dienkripsi dengan kunci rahasia yang sesuai. Langkah pertama untuk melakukan dekripsi berkas yaitu memilih berkas yang sudah terenkripsi dengan memilih tombol ‘Pilih File’ seperti pada gambar 8, kemudian masukkan kata sandi yang sesuai, lalu memilih tombol ‘Dekripsi’, jika berhasil akan muncul notifikasi berhasil seperti pada gambar 12. Jika kata sandi tidak diberikan maka akan muncul notifikasi yang akan memberitahukan pengguna bahwa kata sandi belum diberikan seperti pada gambar 10.

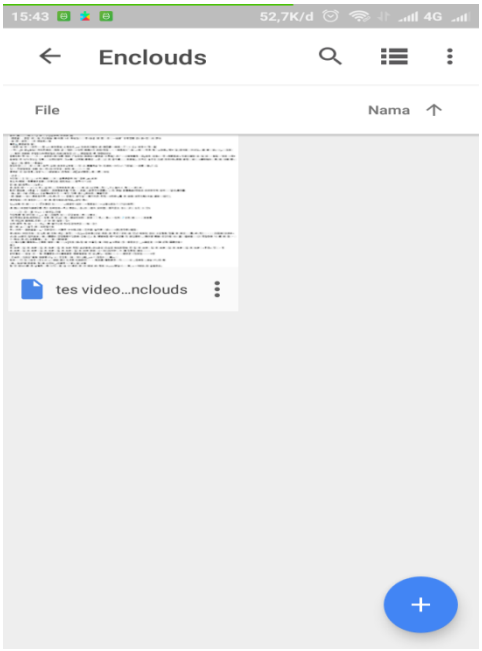


Gambar 12. Notifikasi berkas berhasil didekripsi

5. Pengujian Unggah Berkas

Pada tahap ini berkas yang sudah terenkripsi akan disimpan ke dalam *cloud storage* Google Drive. Langkah pertama memilih berkas yang sudah terenkripsi dengan memilih tombol 'Pilih File' kemudian memilih tombol 'Upload' maka berkas yang sudah terenkripsi dalam proses unggah ke dalam Google Drive seperti pada gambar 13. Pada Google Drive terdapat sebuah folder dengan nama Enclouds yang berguna untuk menyimpan semua hasil berkas yang sudah terenkripsi yang dilakukan oleh perangkat lunak enkripsi dan dekripsi yang terintergrasi oleh *cloud storage* berbasis Android dengan algoritma AES dapat dilihat pada gambar 14.

Gambar 13. Proses unggah berkas terenkripsi ke dalam *cloud storage* Google Drive



Gambar 14. Berkas terenkripsi berhasil disimpan ke dalam layanan *cloud storage* Google Drive

6. Hasil Pengujian Enkripsi, Dekripsi

Pada tahap ini akan dilakukan pengujian terhadap berkas video, audio, gambar, dan dokumen sebanyak masing-masing sepuluh (10) berkas untuk dienkripsi, didekripsi dan diunggah ke dalam *cloud storage* Google Drive. Hasil pengujian dapat dilihat pada tabel 4.

Tabel 4.Hasil pengujian berkas

No	Kode Berkas	Format Berkas	Ukuran (MB)	Proses Enkripsi dan Dekripsi	Lama Proses Enkripsi dan Dekripsi (Detik)	Proses Unggah Google Drive
1	Video 1	mp4	15.65	Berhasil	56	Berhasil
2	Video 2	mp4	1.93	Berhasil	7	Berhasil
3	Video 3	mp4	7.02	Berhasil	25	Berhasil
4	Video 4	mkv	2.49	Berhasil	10	Berhasil
5	Video 5	mkv	7.26	Berhasil	26	Berhasil
6	Video 6	mkv	3.63	Berhasil	13	Berhasil
7	Video 7	mkv	52.44	Berhasil	182	Berhasil
8	Video 8	avi	1.45	Berhasil	5	Berhasil
9	Video 9	avi	1.82	Berhasil	7	Berhasil
10	Video 10	avi	5.69	Berhasil	21	Berhasil
11	Audio 1	mp3	19.70	Berhasil	71	Berhasil
12	Audio 2	mp3	10.01	Berhasil	36	Berhasil
13	Audio 3	mp3	15.44	Berhasil	56	Berhasil
14	Audio 4	mp3	8.60	Berhasil	31	Berhasil
15	Audio 5	wav	35.46	Berhasil	128	Berhasil
16	Audio 6	wav	21.22	Berhasil	77	Berhasil
17	Audio 7	wav	29.69	Berhasil	108	Berhasil
18	Audio 8	flac	23.33	Berhasil	86	Berhasil
19	Audio 9	flac	40.91	Berhasil	155	Berhasil
20	Audio 10	flac	38.38	Berhasil	141	Berhasil
21	Gambar1	gif	2	Berhasil	7	Berhasil
22	Gambar 2	gif	0.2	Berhasil	1	Berhasil
23	Gambar 3	bmp	3.1	Berhasil	11	Berhasil
24	Gambar 4	bmp	4.4	Berhasil	16	Berhasil
25	Gambar 5	jpg	2.2	Berhasil	10	Berhasil
26	Gambar 6	jpg	1.32	Berhasil	5	Berhasil
27	Gambar 7	jpg	1	Berhasil	4	Berhasil
28	Gambar 8	png	6.2	Berhasil	22	Berhasil
29	Gambar 9	png	4.1	Berhasil	15	Berhasil
30	Gambar 10	png	0.3	Berhasil	1	Berhasil
31	Dokumen 1	pdf	0.1	Berhasil	1	Berhasil
32	Dokumen 2	pdf	11.4	Berhasil	40	Berhasil
33	Dokumen 3	pdf	0.2	Berhasil	1	Berhasil
34	Dokumen 4	pdf	3.03	Berhasil	11	Berhasil
35	Dokumen 5	docx	5.1	Berhasil	9	Berhasil
36	Dokumen 6	docx	4.6	Berhasil	8	Berhasil
37	Dokumen 7	docx	1.3	Berhasil	3	Berhasil
38	Dokumen 8	txt	2.3	Berhasil	5	Berhasil
39	Dokumen 9	txt	0.9	Berhasil	2	Berhasil
40	Dokumen 10	txt	0.5	Berhasil	1	Berhasil

5. Kesimpulan

Bagian terdiri atas kesimpulan penelitian dan saran atas hasil penelitian.

5.1 Kesimpulan Penelitian

Kesimpulan penelitian yang telah dilakukan sebagai berikut:

1. Perangkat lunak enkripsi dan dekripsi yang terintegrasi oleh layanan *cloud storage* berbasis Android dengan algoritma A*dvanced Encryption Standard* (AES) berhasil diciptakan. Dalam menjalankan aplikasi sebaiknya terkoneksi dengan internet, baik dari data seluler maupun wifi.
2. Aplikasi sudah dapat mengamankan informasi berkas yang akan disimpan ke dalam layanan *cloud storage* Google Drive dengan proses enkripsi dan dekripsi dengan algoritma *Advanced Encryption Standard* (AES).
3. Dari proses tahapan yang sudah dilakukan maka perangkat lunak dapat melakukan enkripsi, dekripsi dan unggah ke *cloud storage* Google Drive tanpa ada kendala.
4. Ukuran berkas yang sudah diuji adalah 1 – 100 MB. Semakin besar ukuran berkas maka semakin lama proses enkripsi dan proses unggah ke Google Drive.

5.2 Saran

1. Terdapat berbagai saran dari pembuatan perangkat lunak enkripsi dan dekripsi yang teintegrasi oleh *cloud storage* berbasis Android dengan algoritma AES sebagai berikut.
2. Perangkat lunak sebaiknya dioperasikan pada smartphone Android dengan sistem operasi minimal versi 4.4.4 (KitKat).
3. Sebelum menggunakan perangkat lunak sebaiknya memiliki akun Google Drive agar dapat berjalan tanpa kendala.
4. Sebaiknya perlu dikembangkan lebih lanjut tentang lama waktu yang digunakan pada enkripsi atau dekripsi pada berkas yang berukuran besar.

Daftar Rujukan

[1] Abdullah Salahul Haq, 2017. *Pengertian Kriptografi*. Available at : https://fit.labs.telkomuniversity.ac.id/pengertian-kriptografi. [Accessed 18 August 2018]

[2] Anna Kurniwati, Muhammad Dwiky Darmawan, 2016. *Implementasi Algoritma Advanced Encryption Standard (AES) untuk Enkripsi dan Dekripsi Dokumen Teks*. Universitas Gunadarma.

[3] Imamah, Arif Djunaidy, Muchammad Husni 2014., *Penerapan AES untuk Otentikasi Akses Cloud Computing*. ISSN 2088-2130, Vol 13. No.1.

[4] Fresly Nandar Pabokory, Indah Fitri Astuti, Awang Harsa Kridalaksana., *Implementasi Kriptografi Pengamanan Data pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard*. Vol 10, No.1.

[5] Ahmad Pram Prayogo Pangestu, 2016. *Pengertian Cloud Storage*. Available at : https://www.duosia.id/web/pengertian-cloud-storange/. [Accessed 18 August 2018]

[6] Murtiwiyati, Glenn Lauren., 2013., *Rancang Bangun Aplikasi Pembelajaran Budaya Indonesia Untuk Anak Sekolah Dasar Berbasis Android*. ISSN 1412-9434, Vol 12. No.2.

[7] Badell Maman, 2016., *Android – Arsitektur Sistem Operasi Android*. Available at : http://www.kapalomen.com/2016/07/android-arsitektur-android-sistem-operasi-android.html. [Accessed 18 August 2018]

[8] Hafizh Herdi, 2012., *Android – Arsitektur Sistem Operasi Android*. Available at : https://www.twoh.co/2012/09/18/mengenal-arsitektur-sistem-operasi-android/. [Accessed 18 August 2018]

[9] Android Developer, 2018., *Memverifikasi Perilaku Aplikasi pada Android Runtime (ART)*. Available at : https://developer.android.com/guide/practices/verifying-apps-art?hl=id. [Accessed 18 August 2018]

[10] Android Developeri, 2018., *Arsitektur Platform*. Available at : https://developer.android.com/guide/platform/?hl=id. [Accessed 18 August 2018]