semanTIK, Vol.5, No.2, Jul-Des 2019, pp. 185-194
ISSN: 2502-8928 (Online)
DOI : 10.5281/zenodo.3463988
Terakreditasi "Peringkat 4 (Sinta 4)" oleh Kemenristekdikti
Website : http://ojs.uho.ac.id/index.php/semantik

PENERAPAN ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) UNTUK MENGAMANKAN *FILE* PADA LAYANAN *INFRASTRUCTURE AS A SERVICE*

Muh.Muchsin Al-As'Ad Mirsyah*[1], L.M. Fid Aksara[2], Adha Mashur Sajiah[3]
[*1,2,3] Jurusan Teknik Informatika, Fakultas Teknik, Universitas Halu Oleo, Kendari
e-mail: *[1]alasadmirsyahm@gmail.com,[2] **fidaksara@uho.ac.id,**[3] **adha.m.sajiah@uho.ac.id**

Abstrak

Media penyimpanan berbasis *cloud* merupakan salah satu contoh bentuk perkembangan teknologi media penyimpanan pada komputer. Data disimpan di komputer dimana pengguna harus membuat akun *Cloud Storage* yang diakses dengan jaringan internet. Namun, keamanan *file* dan data pada *Cloud Storage* masih sangat rentan untuk diserang dalam *database*. Oleh karena itu dibutuhkan algoritma kriptografi yang kuat dan aman untuk meminimalisir ancaman pada keamanan data di *Cloud Storage*. Saat ini, *Advanced Encryption Standard* (AES) merupakan algoritma *cipher* yang bersifat aman untuk melindungi data atau informasi yang bersifat rahasia. Pengujian enkripsi dan dekripsi dengan algoritma AES kemudian dilakukan pada delapan jenis *file*, yaitu gambar, *.doc, *.pdf, .*xsls, *.ppt, *.txt, *.mp3, dan video. Hasil pengujian untuk enam tipe *file* menunjukkan bahwa metode AES mampu mengamankan *file*. Sedangkan dua lainnya mengalami kegagalan, yaitu pada *file* berjenis *.mp3 dan video. Hasil yang didapatkan pada penelitian ini bahwa sistem *Private Cloud Storage* dapat berjalan dengan baik dengan menerapkan algoritma AES.

Kata Kunci—*Cloud Computing, Private Cloud Storage,* AES, Enkripsi, Dekripsi

Abstract

Cloud-based storage media is one example of the development of storage media technology on computers. Data is stored on a computer where the user must create a Cloud Storage account that is accessed by the internet network. However, the security of files and data in Cloud Storage is still very vulnerable to attack in the database. Therefore, we need a strong and safe cryptographic algorithm to minimize threats to data security in Cloud Storage. Currently, the Advanced Encryption Standard (AES) is a cipher algorithm that is secure to protect data or information that is confidential. Encryption and decryption testing with AES algorithm is then performed on eight types of files, namely images,.doc, *.pdf, *.xsls, *.ppt, *.txt, *.mp3 and video. Test results for six file types show that the AES method is able to secure files. While the other two failed, namely the file type *.mp3 and video. The results obtained in this study that the Private Cloud Storage system can run well by applying the AES algorithm.*

Keywords— *Cloud Computing, Private Cloud Storage, AES, Encryption, Decryption*

1. PENDAHULUAN

Perkembangan teknologi mempengaruhi perkembangan media penyimpanan pada komputer dari masa kemasa. Salah satu jenis berkembangnya adalah media penyimpanan berbasis *cloud*. *Cloud* adalah metafora dari internet, sebagaimana awan yang sering digambarkan pada diagram jaringan komputer. *Cloud Computing* merupakan suatu paradigma dimana informasi tersimpan di *server* internet dan tersimpan secara sementara di komputer pengguna (*client*) dengan kata lain *Cloud Storage* adalah bagian dari sistem *Cloud Computing* tersebut.

Cloud Storage sendiri merupakan media penyimpanan yang dalam pengaksesannya memerlukan jaringan internet. *File* dan data disimpan di komputer dimana pengguna harus membuat akun *Cloud Storage* terlebih dahulu. Selama komputer yang digunakan terhubung dengan internet, pengguna tidak perlu lagi menggunakan *flashdisk*, *harddisk* atau perangkat keras penyimpanan lainnya untuk keperluan mobilitas penyimpanan data.

Fakultas Teknik Universitas Halu Oleo dalam teknik penyimpanan datanya itu masih secara *hardcopy* dan disimpan dalam satu tempat penyimpan yang dimana pada suatu saat data itu akan memenuhi ruang penyimpanan (*storage*) baik *hardisk, USB*, dan lain–lain. Data-data tersebut seperti data dosen, data jurusan-jurusan yang berada di fakultas teknik, mahasiswa, alumni ataupun arsip penting lainnya. Kegiatan tersebut akan menghasilkan sejumlah data yang banyak setiap harinya dalam periode tahunan penyimpanan yang baru yang akan menghabiskan dana yang tidak sedikit akan menambah limbah, dan apabila terjadi bencana masalah kehilangan data yang menjadi aset informasi tersebut.

Keamanan *file* dan data pada *Cloud Storage* masih sangat rentan untuk di serang atau diambil *file*-nya dalam *database* dalam hal ini *server*, seiring dengan perkembangan teknologi komputer yang semakin canggih, maka dunia teknologi informasi membutuhkan algoritma kriptografi yang lebih kuat dan aman. Saat ini, *Advanced Encryption Standard* (*AES)* merupakan algoritma *cipher* yang aman untuk melindungi data atau informasi yang bersifat rahasia.

Berdasarkan pemaparan pada paragraf sebelumnya dan melihat permasalahan yang ada, maka penulis akan membuat layanan *Cloud Storage* yang sering digunakan pada umumnya seperti *dropbox*. Aplikasi *Cloud Storage* dalam hal ini *dropbox* memiliki batas ketika pengguna akan meng-*upload file* 2GB bisa dilakukan secara gratis berbeda dengan *Cloud Storage* yang akan dibuat ini adalah user dapat meng*upload file* secara gratis berapapun kapsitas *file*, tetapi disesuaikan dengan kapasitas *server* yang diatur oleh admin dan memiliki kemanan *file* yang sangat baik di dalam *database*.

2. METODE PENELITIAN

2.1 *Cloud Computing*

Pada dunia teknologi informasi dan komunikasi para ahli telah banyak memberikan definisi atau pengertian tentang komputasi awan. Salah satu definisi *cloud computing* pada sebuah jurnal yang dipublikasikan oleh IEEE pada tahun 2008, *cloud computing* adalah sebuah paradigm dimana informasi secara permanen tersimpan di *server* di awan (internet) dan tersimpan secara sementara di komputer pengguna, termasuk di dalamnya adalah PC, desktop, *computer tablet*, *notebook* dan lain-lain.

Teknologi *cloud computing* dapat didefinisikan secara sederhana sebagai sebuah perusahaan dengan pusat data yang menyediakan *rental space storage*. Maksudnya adalah teknologi *cloud computing* merupakan teknologi yang berbasiskan pada permintaan pengguna. Teknologi ini merupakan salah satu titik perubahan yang tidak hanya pada aplikasi perangkat lunak yang berbasis *cloud computing* tetapi juga pada *platform*, infrastrutur basis data maupun layanan semuanya berbasiskan *cloud computing*.

Sedangkan tiga jenis model layanan dijelaskan oleh NIST (Mell dan Grance) sebagai berikut:

1. *Cloud Software as a Service (SaaS)*

Kemampuan yang diberikan kepada konsumen untuk menggunakan aplikasi penyedia dapat beroperasi pada infrastruktur awan. Aplikasi dapat diakses dari berbagai perangkat klien melalui antarmuka seperti *web browser* (misalnya, email berbasis *web*).

Konsumen tidak mengelola atau mengendalikan infrastruktur awan yang mendasari termasuk jaringan, *server*, sistem operasi, penyimpanan, atau bahkan kemampuan aplikasi individu, dengan kemungkinan pengecualian terbatas terhadap pengaturan konfigurasi aplikasi pengguna tertentu.

2. *Cloud Platform as a Service (PaaS)*

Kemampuan yang diberikan kepada konsumen untuk menyebarkan aplikasi yang dibuat konsumen atau diperoleh ke infrastruktur komputasi awan menggunakan bahasa pemrograman dan peralatan yang didukung oleh *provider*. Konsumen tidak mengelola atau mengendalikan infrastruktur awan yang mendasari termasuk jaringan, *server*, sistem operasi, atau penyimpanan, namun memiliki kontrol atas aplikasi disebarkan dan memungkinkan aplikasi melakukan *hosting* konfigurasi.

3. *Cloud Infrastructure as a Service (IaaS)*

Kemampuan yang diberikan kepada konsumen untuk memproses, menyimpan, berjaringan, dan komputasi sumber daya lain yang penting, dimana konsumen dapat menyebarkan dan menjalankan perangkat lunak secara bebas dapat mencakup sistem operasi dan aplikasi. Konsumen tidak menge-lola atau mengendalikan infrastruktur awan yang mendasari tetapi memiliki kontrol atas sistem operasi, penyimpanan, aplikasi yang disebarkan, dan mungkin kontrol terbatas komponen jaringan yang pilih (misalnya, *firewall host*)[1].

2.2 *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 [2].

2.3 Pemrograman PHP

PHP merupakan bahas pemrograman yang ditujukan untuk membuat aplikasi *web*. Ditinjau dari pemrosesannya, PHP tergolong berbasis *server side*. Artinya, pemrosesan dilakukan di *server*. Hal ini berkebalikan dengan bahasa seperti *javascript*, yang pemrosesannya dilakukan di sisi klien. PHP sering dikatakan sebagai bahasa untuk membuat aplikasi *web* yang dinamis. Pengertian dinamis di sini adalah memungkinkan untuk menampilkan data yang tersimpan dalam *database*. Dengan demikian, halaman *web* akan menyesuaikan dengan isi *database* [3]

2.4 Kriptografi

a. Definisi Kriptografi

Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan dan ketika data di kirim dari suatu tempat ke tempat lain. Dalam perkembangannya, *kriptografi* juga digunakan untuk mengedintifikasi pengeriman data dan tanda tangan digital dan keaslian data dengan sidik jari digital.

b. Macam-macam Algoritma Kriptografi

Algorithma kriptografi dibagi menjadi dua berdasarkan kunci yaitu:

1) Kriptografi Simetri

Kriptografi simetri menggunakan kunci sama dengan kunci yang di pakai untuk melakukan dekripsi. Istilah lain untuk enkripsi dan dekripsi ini adalah kriptografi kunci privat (*Private-key cryptography)* atau kriptografi kunci rahasia (*secret-key cryptography)*. Penerapan algoritma akan menghasilkan outputyang berbeda sesuai dengan kunci yang dipakai. Mengubah kunci berarti juga mengubah *output* dari algoritma yang di pakai.

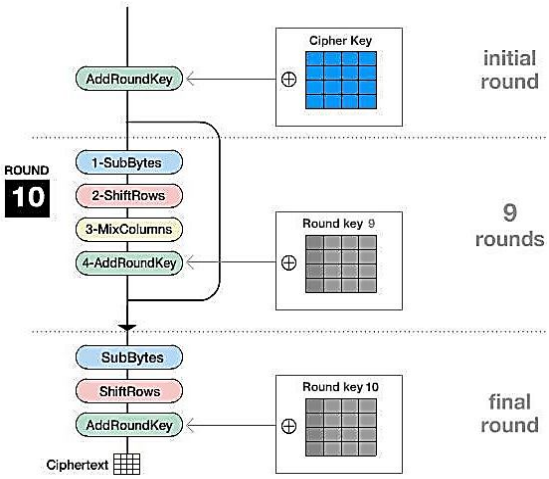
2) Kriptografi Asimetri

Kriptografi asimetri adalah algoritma yang memakai kunci berbeda untuk proses enkripsi dan dekripsinya. Kriptografi asimetri disebut juga sebagai system kriptografi *public-key* karena kunci untuk enkripsi dibuat secara umum (*publickey)*. Proses dekripsinya yang dibuat satu, yakni hanya orang yang berwenang untuk mendekripsinya (disebut

Private-key). Keuntungan kriptografi asimeti ini, untuk berkorespondensi secara rahasia dengan banyak pihak tidak diperlukan kunci rahasia sebanyak jumlah pihak tersebut, cukup membuat dua buah kunci (disebut *public-key*) bagi para koresponden untuk mengenkripsi pesan, dan *Private-key* untuk mendekripsi [4]

2.5 Advanced Encryption Standart (AES)

AES atau *Advanced Encryption Standard* merupakan standar enkripsi kunci simetri yang pada awalnya diterbitkan dengan algoritma Rijndael. Algoritma ini dikembangkan oleh dua kriptografer Belgia, Joan Daemen dan Vincent Rijmen. *Advanced Encryption Standard* (AES) dipublikasikan oleh NIST (*National Institute of Standard and Technology*) pada tahun 2001. AES merupakan blok kode simetris untuk menggantikan DES (*Data Encryption Standard*). Algoritma AES merupakan algoritma simetris yaitu menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma AES memiliki tiga pilihan kunci yaitu tipe : AES-128, AES-192, dan AES-256. Masing-masing tipe menggunakan kunci internal yang berbeda yaitu round key untuk setiap putaran.



Gambar 1**.** Skema Kerja AES-128[5]

Proses putaran enkripsi AES-128 dikerjakan sebanyak 10 kali (a=10), yaitu sebagai berikut:

a. Addroundkey
b. Putaran sebanyak a-1 kali, proses yang dilakukan pada setiap putaran adalah: SubBytes, ShiftRows, MixColumns, dan AddRoundKey.
c. Final Round, adalah proses putaran untuk putaran terakhir yang meliputi SubBytes, ShiftRows, MixColumn, dan AddRoundKey.

Sedangkan pada proses dekripsi AES-128, proses putaran juga dikerjakan sebanyak 10 kali (a=10) seperti yang ditunjukkan pada Gambar 1.

2.6 Linux Ubuntu

Ubuntu merupakan salah satu distribusi *Linux* yang berbasiskan *Debian* dan didistribusikan sebagai perangkat lunak bebas. Nama *Ubuntu* berasal dari filosofi dari Afrika Selatan yang berarti "kemanusiaan kepada sesama". *Ubuntu* dirancang untuk kepentingan penggunaan pribadi, namun versi *Server Ubuntu* juga tersedia, dan telah dipakai secara luas. Proyek *Ubuntu* resmi disponsori oleh *Canonical Ltd.*, yang merupakan sebuah perusahaan yang dimiliki oleh pengusaha Afrika Selatan *Mark Shuttleworth*. Tujuan dari distribusi *Linux Ubuntu* adalah membawa semangat yang terkandung di dalam filosofi *Ubuntu* ke dalam dunia perangkat lunak. *Ubuntu* adalah sistem operasi lengkap berbasis *Linux*, tersedia secara bebas, dan mempunyai dukungan baik yang berasal dari komunitas maupun tenaga ahli profesional.

Ubuntu terdiri dari banyak paket, kebanyakan berasal dari distribusi di bawah lisensi lisensi *software* bebas. Namun, beberapa *software* khususnya *driver* menggunakan *Proprietary software*. Lisensi yang pada umumnya adalah *GNU General Public License* (*GNU GPL*) dan *GNU Lesser General Public License* (*GNU LGPL*), dengan tegas menyatakan bahwa pengguna dengan bebas dapat menjalankan, menggandakan, mempelajarai, memodifikasi, dan mendistribusikan tanpa pembatasan apapun. Namun tetap ada *software proprietary* yang dapat berjalan di *Ubuntu*. *Ubuntu* berfokus pada ketersediaan kegunaan pada orang disfungsi, keamanan dan stabilitas. *Ubuntu* juga berfokus pada internasionalisasi dan aksesibilitas untuk dapat menjangkau sebanyak-banyaknya orang. Dalam hal keamanan, perangkat *sudo* dapat meningkatkan *privilege* secara sementara untuk melakukan tugas administratif, sehingga akun *root* dapat terus terkunci, dan mencegah orang tidak *terauthorisasi* melakukan

perubahan sistem atau membuka kelemahan keamanan.

Varian sistem operasi *Ubuntu* untuk melayani kebutuhan komputasi skala *Server*. *Ubuntu Server* menyediakan platform yang terintegrasi dengan baik yang akan memudahkan anda melakukan *deploy Server* dengan fasilitas layanan *internet* standar: *mail, web, DNS, file-serving* hingga manajemen *database*. Sebagai turunan dari distribusi *Debian*, karakter alami *Ubuntu Server* yang diwariskan dari *Debian* adalah faktor keamanan (*security*). *Ubuntu Server* tidak membiarkan keberadaan *port* yang terbuka setelah proses instalasi, dan hanya akan memuat *software-software* yang *esensial* dan dibutuhkan untuk membangun sebuah sistem *Server* yang aman [6]

3. HASIL DAN PEMBAHASAN

3.1 Implementasi

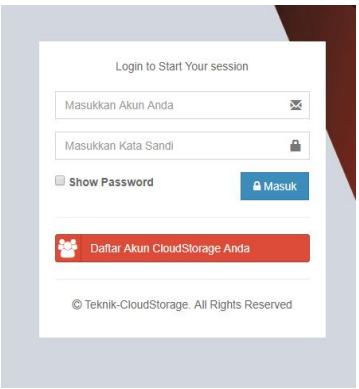
Implementasi rancangan antarmuka, yaitu:

1. Interface Aplikasi

Pada *interface* Aplikasi di antaranya :

a. Halaman Login

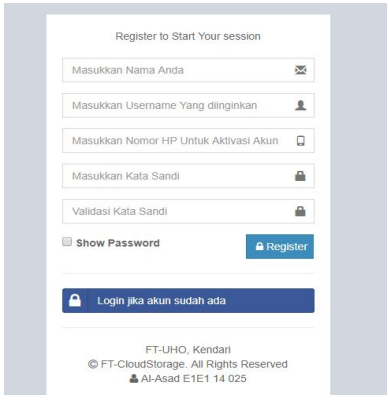
Pada halaman ini *Form login* merupakan form yang harus diisi oleh *user* untuk dapat mengakses menu dan fitur yang ada di dalam sistem. Pada *form* ini *user* diminta untuk memasukkan *username* dan *password* dapat dilihat pada Gambar 2.



Gambar 2 Halaman *Login*

b. Halaman Registrasi User

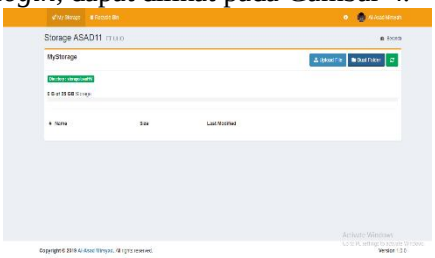
Tampilan halaman registrasi *user*, sebelum *user* menggunakan sistem *Cloud Storage user* harus terlebih dahulu registrasi agar dapat memiliki akun dapat dilihat pada Gambar 3.



Gambar 3 Halaman Registrasi User

c. Halaman Beranda

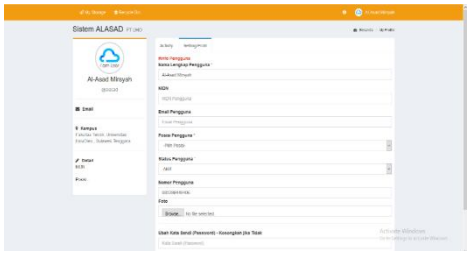
Halaman beranda merupakan halaman setelah step *login*, dapat dilihat pada Gambar 4.



Gambar 4 Halaman Beranda

d. Halaman Edit Profil

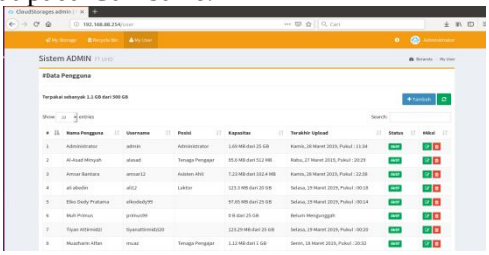
Tampilan edit profil yang berfungsi untuk melengkapi data diri *user* dapat dilihat pada Gambar 5.



Gambar 5 Halaman Edit Profil

e. Halaman Admin

Tampilan admin, pada form admin ini adalah tempat admin mengelolah *user*, *user* dapat menggunakan sistem *Cloud Storage* apabila admin telah menyetujui *user* tersebu dapat di lihat pada Gambar 6.



Gambar 6 Halaman Admin

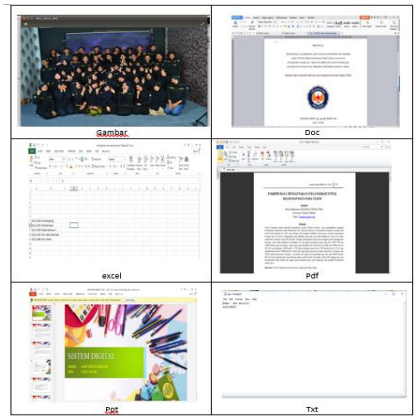
3.2 Pengujian Sistem

Pengujian merupakan bagian tahap dari proses pengembangan perangkat lunak pengujian ini bertujuan untuk mengetahui kualitas pada perangkat lunak telah dibuat. Pengujian ini dilakukan untuk mengetahui apakah program yang dibuat telah sesuai seperti rencana dan rancangan sebelumnya. Pengujian dalam system ini, penulis menggunakan metode pengujian *black box* dan *stress testing*.

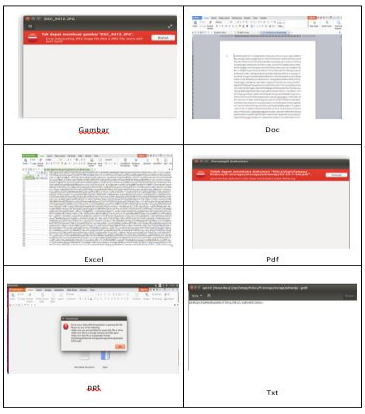
1. Pengujian Black Box

a. Enkripsi

Pengujian Enkripsi bertujuan untuk mengetahui kebenaran *file* yang di *upload* telah terenkripsi dengan benar dapat di lihat pada gamabar 7 dan 8.



Gambar 7 *File* sebelum dienkripsi

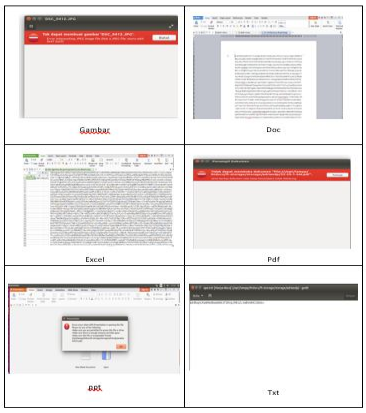


Gambar 8 *File* setelah dienkripsi

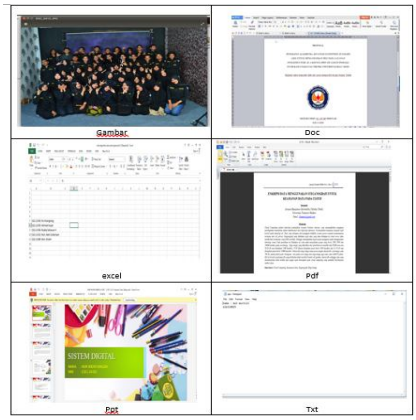
Dari hasil Enkripsi perubahan yang terjadi pertama pada *file* gambar adalah *file*nya terbuka tetapi gambarnya tidak terlihat, ke dua pada *file doc file*nya terbuka tetapi isi dari kalimatnya teracak tidak seprerti aslinya, ke tiga *file excel file*nya terbuka tetapi isi dari kalimatnya teracak, ke empat *file* pdf terbuka tetapi ada notifikasi tidak dapat membuka dokumen, ke lima *file* ppt terbuka tetapi muncul notifikasi *error* dan ke enam *file* txt terbuka tetapi isi kalimatnya teracak. Kemudian dari nama-nama *file*nya dan ukurannya tidak berubah sama sekali masih sama seperti sebelum dienkripsi.

b. Dekripsi

Pengujian dekripsi bertujuan untuk mengetahui kebenaran *file* yang diunduh telah terdekripsi dengan benar dapat di lihat pada gambar 9 dan 10.



Gambar 9 *File* sebelum didekripsi



Gambar 10 *File* setelah didekripsi

Dari hasil dekripsi perubahan yang terjadi pertama pada *file* gambar berhasil terbuka dan gambarnya terlihat lalu kualitas gambarnya juga masih bagus, ke dua *file doc* berhasil terbuka dan isi kalimatnya tidak teracak lagi seperti dengan aslinya, ke tiga *file excel* terbuka dan isinya tidak teracak lagi

seperti dengan aslinya, ke empat *file* pdf terbuka dan isinya bisa terlihat, ke lima *file ppt* terbuka dan isinya terlihat dan ke enam *file txt* terbuka kemudian isinya tidak teracak lagi. Nama *file* dan ukuran *file*nya tidak berubah sama sekali.

2. Jenis *File* yang terenkripsi dan terdekripsi

Tabel 1 Hasil Pengujian Enkripsi Dan Dekripsi

Hasil Uji *File* Enkripsi dan Dekripsi		
Jenis *File*	Enkripsi	Dekripsi
Gambar	Berhasil	Berhasil
Doc	Berhasil	Berhasil
Excel	Berhasil	Berhasil
Pdf	Berhasil	Berhasil
Ppt	Berhasil	Berhasil
Txt	Berhasil	Berhasil
Mp3	Gagal	Gagal
Video	Gagal	Gagal

Pada Tabel 1 di atas menunjukan terjadinya kegagalan enkripsi dan dekripsi pada jenis *file mp3* dan *video* dikarenakan algoritma yang digunakan tidak mampu mengenkripsi dan mendekripsi jenis *file* tersebut.

3. Pengujian Stress test

Pada pegujian s*tress test* bertujuan untuk mengetahui lama waktu *upload file* secara bersamaan dari ukuran-ukuran *file* yang di tentukan dan lama waktu download.

Tabel 2. Hasil uji 1 User

Hasil Uji 1 User			
Ukuran *file*	Waktu *Upload*	Waktu Download	keterangan
10 Mb	9,03 (detik)	20,72(detik)	Berhasil
20 Mb	20,29 (detik)	39,73 (detik)	Berhasil
50 Mb	1.40,25 (menit)	55,19 (detik)	Berhasil

Pada Tabel 2 yang tertera di atas, dari pengujian terhadap satu *user* dapat terlihat bahwa semakin besar ukuran *file* yang di *upload* dan di *download*, maka waktu yang dibutuhkan juga semakin lama.

Tabel 3 Hasil uji 10 *User*

Hasil Uji 10 User				
Ukuran *file*	User	Waktu *Upload*	Waktu Download	Keterangan
	C1	1.36,60 (menit)	19,89(detik)	Berhasil
	C2	3.46,61 (menit)	29,64(detik)	Berhasil
	C3	4.16,32 (menit)	35,71(detik)	Berhasil
	C4	5.20,21 (menit)	38,74(detik)	Berhasil
	C5	5.23,96 (menit)	42,75(detik)	Berhasil
10 Mb	C6	5.34,41 (menit)	43,89(detik)	Berhasil
	C7	5.35,64 (menit)	49,98(detik)	Berhasil
	C8	5.42,87 (menit)	51,18(detik)	Berhasil
	C9	6.02,20 (menit)	55,64(detik)	Berhasil
	C10	6.07,35 (menit)	56,86(detik)	Berhasil
	C1	10.24,13(menit)	21,45(detik)	Berhasil
	C2	13.33,10(menit)	32,91(detik)	Berhasil
	C3	14.40,23(menit)	36,01(detik)	Berhasil
	C4	15.34,87(menit)	40,50(detik)	Berhasil
20 Mb	C5	15.44,43(menit)	45,95(detik)	Berhasil
	C6	16.10,02(menit)	50,16(detik)	Berhasil
	C7	17.11,41(menit)	56,22(detik)	Berhasil
	C8	18.25,45(menit)	1.00,42(menit)	Berhasil
	C9	20.21,53(menit)	1.01,11(menit)	Berhasil
	C10	20.54,19(menit)	1.02,02(menit)	Berhasil
	C1	46.51,07(menit)	9.11,04(menit)	Berhasil
	C2	55.54,89(menit)	9.13,10(menit)	Berhasil
	C3	59.37,80(menit)	11.48,30(menit)	Berhasil
	C4	01.00.35(jam)	13.15,63(menit)	Berhasil
	C5	01.00.53(jam)	13.38,02(menit)	Berhasil
50 Mb	C6	01.01.19(jam)	13.46,29(menit)	Berhasil
	C7	01.01.27(jam)	13.53,33(menit)	Berhasil
	C8	01.01.41(jam)	13.55,13(menit)	Berhasil
	C9	01.01.59(jam)	13.55,85(menit)	Berhasil
	C10	01.02.04(jam)	13.56,02(menit)	Berhasil

Pada Tabel 3 menunjukan pada pengujian yang dilakukan terhadap sepuluh user yang melakukan proses *upload* dan *download* secara bersamaan, selain besaran ukuran *file* juga banyaknya *user* menjadi faktor yang mempengaruhi lamanya rentang waktu yang dibutuhkan dalam proses itu.

Tabel 4 Hasil uji 20 *User*

Hasil Uji 20 User				
Ukuran *file*	User	Waktu *Upload*	Waktu Download	Keterangan
	C1	3.36,20(menit)	38,25(detik)	Berhasil
	C2	9.16,61(menit)	58,41(detik)	Berhasil
	C3	12.38,32(menit)	1.10,89(menit)	Berhasil
	C4	15.56,19(menit)	1.16,71(menit)	Berhasil
	C5	16.63,92(menit)	1.24,78(menit)	Berhasil
	C6	18.43,40(menit)	1.26,65(menit)	Berhasil
	C7	19.35,18(menit)	1.38,01(menit)	Berhasil
	C8	21.24,82(menit)	1.42,12(menit)	Berhasil
	C9	22.08,20(menit)	1.50,41(menit)	Berhasil
	C10	23.10,36(menit)	1.52,86(menit)	Berhasil
	C11	25.36,62(menit)	1.54,15(menit)	Berhasil
10 Mb	C12	27.11,22(menit)	1.58,33(menit)	Berhasil
	C13	29.14,02(menit)	2.01,25(menit)	Berhasil
	C14	29.20,91(menit)	2.07,80(menit)	Berhasil
	C15	29.34,40(menit)	2.11,65(menit)	Berhasil
	C16	29.42,88(menit)	2.18,23(menit)	Berhasil
	C17	30.01,15(menit)	2.21,42(menit)	Berhasil
	C18	30.08,32(menit)	2.25,07(menit)	Berhasil
	C19	30.10,56(menit)	2.28,40(menit)	Berhasil
	C20	30.15,73(menit)	2.30,96(menit)	Berhasil
	C1	30.54,20(menit)	1.02,41(menit)	Berhasil
	C2	39.11,10(menit)	1.14,01(menit)	Berhasil
	C3	42.42,23(menit)	1.22,91(menit)	Berhasil
	C4	45.30,19(menit)	1.30.95(menit)	Berhasil
	C5	48.44,53(menit)	1.40,50(menit)	Berhasil
	C6	51.10,02(menit)	1.50,16(menit)	Berhasil
	C7	52.11,41(menit)	2.02,11(menit)	Berhasil
	C8	55.21,60(menit)	2.10,22(menit)	Berhasil
	C9	01.03.25(jam)	2.22,02(menit)	Berhasil
	C10	01.10.36(jam)	2.30,42(menit)	Berhasil
	C11	01.15.02(jam)	2.45,04(menit)	Berhasil
	C12	01.18.05(jam)	2.59,85(menit)	Berhasil
	C13	01.20.28(jam)	3.12,29(menit)	Berhasil
	C14	01.25.15(jam)	3.28,16(menit)	Berhasil
	C15	01.26.52(jam)	3.36,18(menit)	Berhasil
	C16	01.27.30(jam)	3.45,33(menit)	Berhasil
	C17	01.28.05(jam)	3.54,04(menit)	Berhasil
	C18	01.28.34(jam)	3.59,96(menit)	Berhasil
	C19	01.29.14(jam)	4.02,28(menit)	Berhasil
	C20	01.29.56(jam)	4.05,32(menit)	Berhasil
	C1	02.18.51(jam)	18.21,13(menit)	Berhasil
	C2	02.45.54(jam)	18.23,60(menit)	Berhasil
	C3	02.57.37(jam)	22.58,35(menit)	Berhasil

Hasil Uji 20 User				
Ukuran *file*	User	Waktu *Upload*	Waktu Download	Keterangan
50 Mb	C4	03.24.35(jam)	26.15,11(menit)	Berhasil
	C5	03.35.53(jam)	29.38,01(menit)	Berhasil
	C6	03.42.19(jam)	31.14,02(menit)	Berhasil
	C7	03.50.27(jam)	34.21,57(menit)	Berhasil
	C8	03.58.41(jam)	36.01,32(menit)	Berhasil
	C9	04.05.59(jam)	37.11,15(menit)	Berhasil
	C10	04.15.04(jam)	39.39,01(menit)	Berhasil
	C11	04.23.07(jam)	40.43,82(menit)	Berhasil
	C12	04.30.46(jam)	41.20,88(menit)	Berhasil
	C13	04.34.25(jam)	42.26,28(menit)	Berhasil
	C14	04.39.10(jam)	43.45,73(menit)	Berhasil
	C15	04.42.38(jam)	44.05,19(menit)	Berhasil
	C16	04.43.01(jam)	44.25,52(menit)	Berhasil
	C17	04.43.49(jam)	44.46,20(menit)	Berhasil
	C18	04.44.29(jam)	44.55,61(menit)	Berhasil
	C19	04.45.17(jam)	44.55,38(menit)	Berhasil
	C20	04.45.54(jam)	44.58,72(menit)	Berhasil

Pada Tabel 4 menunjukan pada pengujian *upload* dan *download* yang dilakukan terhadap dua puluh *user*, sebagaimana pengujian sebelumnya waktu yang dibutuhkan mengalami peningkatan yang cukup signifikan dikarenakan bertambahnya jumlah *user* meskipun ukuran *file* yang diujikan sama seperti sebelumnya.

Dari hasil penelitian yang dilakukan di atas, secara keseluruhan dapat diambil kesimpulan bahwa semakin banyak user yang melakukan *uploading* dan *downloading* secara bersamaan, maka semakin lama waktu yang dibutuhkan dalam prosesnya.

4. KESIMPULAN

Berdasarkan penelitian dan hasil pengujian yang dilakukan, maka dapat ditarik kesimpulan, di antaranya:

1. Sistem *Private Cloud Storage* dapat berjalan dengan baik dapat dilihat dari hasil pengujian sistem *Private Cloud Storage* ini, semua menu yang ada dapat berjalan dan berfungsi dengan baik.
2. Dari hasil pengujian enkripsi dan dekripsi yang dilakukan pada delapan jenis *file*, pengujian terhadap enam jenis *file* berhasil yaitu gambar, .doc, .pdf, .xsls, .ppt, dan .txt yang dimana enam *file* ini aman berdasarkan pengujian kemanan *file doc, xsls,* dan *txt* ketika dibuka maka *file* menjadi teracak kemuadian untuk *file* gambar, *pdf,* dan *ppt* ketika dibuka muncul tampilan *error*. Sedangkan dua lainnya mengalami kegagalan, yaitu pada *file* berjenis .mp3 dan video dikarenakan algoritma yang digunakan tidak mampu mengenkripsi dan mendekripsi jenis *file* tersebut.
3. Pada pengujian *stress test*, yang terdiri dari pengujian *upload* dan *download*, lamanya waktu yang dibutuhkan dipengaruhi oleh besaran ukuran *file* dan banyaknya *user*. Semakin banyak *user* yang melakukan *upload* dan *download* secara bersamaan, maka waktu yang dibutuhkan akan semakin lama.

5. SARAN

Saran yang dapat diberikan, agar ke depannya spesifikasi dan konfigurasi *server* dioptimalkan sehingga dapat menangani proses *client* ke *server* menjadi lebih baik, juga untuk penelitian selanjutnya diharapkan untuk menerapkan algoritma yang mampu bekerja lebih baik dalam proses enkripsi dan dekripsi *file*.

DAFTAR PUSTAKA

[1] J. Jamaluddin, "Untuk Pembuatan Dokumen dan Presentasi," *Maj. Ilm. Methoda*, Vol. 5, pp. 63–68, 2015.

[2] A. Setiawan and B. Yanto, "Prototype Sist. Deteksi Dini Kebakaran Hutan dengan Sensormatik," *SISFOTEK*, Vol. 2, No. 1, pp. 228–236, 2018.

[3] Hasanah, Ridarmin, and S. Adrianto, "Aplikasi Sistem Pakar Pendeteksi Kerusakan Laptop / PC Dengan Penerapan Metode Forward Chaining Menggunakan Bahasa Pemrograman PHP," *Informatika*, Vol. 9, No. 2, pp. 40–50, 2017.

[4] T. Asprina, M. Yamin, and Sutardi, "Pembangunan Aplikasi Keamanan Pesan Chatting dengan Menerapkan Algoritma Tiny Encryption Algorithm (TEA) Berbasis Client Server," *semanTIK*, Vol. 4, No. 2, pp. 57–64, 2018.

[5] A. Arif and P. Mandarani, "Rekayasa Perangkat Lunak Kriptografi Menggunakan Algoritma Advanced Encryption Standard (AES) 128 Bit pada Sistem Keamanan Short Message Service (SMS) Berbasis Android,"

Teknoif, Vol. 4, No. 1, pp. 84–93, 2016.

[6] R. F. Nurmadyansyah and A. Arifin, "Perancangan dan Implementasi Sistem Kendali Robot Tangan Prensilia," *Jurnal Teknik Pomits*, Vol. 3, No. 1, pp. F-1–F-6, 2014.