IMPLEMENTASI ENKRIPSI AES DAN 3DES PADA APLIKASI FTP CLIENT PT. ALAM SUTERA REALTY, TBK

Ferdiansyah[1], Ammar Haikal Addimasqi [2], Dolly Virgian Shaka Yudha Sakti [3]

Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Ciledug Raya, Petukangan Utara, Kebayoran Lama, Jakarta Selatan, 12260
Telp. (021) 5853753, Fax (021) 5866369
[1]ferdiansyah@budiluhur.ac.id, [2]haikal.addimasqi@gmail.com, [3]dollyvirgian.shaka@budiluhur.ac.id

ABSTRAK

Dewasa ini banyak isu yang berkembang tentang keamanan data. Seiring dengan berkembangnya teknologi informasi yang didukung dengan infrastruktur jaringan komputer maha besar (internet), menyebabkan semakin mudahnya bagi seseorang untuk mendapatkan data, baik dengan cara yang legal, ataupun tidak legal. Keamanan data adalah hal yang sangat penting dalam menjaga kerahasiaan informasi yang ada pada data tersebut. Apabila suatu data tidak diamankan dengan suatu metode enkripsi data, bilamana data tersebut dicuri, data tersebut akan sangat mudah dibuka dan informasi yang ada didalamnya dapat diketahui oleh orang yang mencurinya. Hingga saat ini dokumen-dokumen hardcopy yang bersifat rahasia di PT. Alam Sutera Realty, Tbk dipindai (scan) dan disimpan dengan format pdf pada File Transfer Protocol (FTP) server tanpa diberikan pengamanan dengan suatu algoritma enkripsi data. Keamanan data tersebut hanya dibatasi dengan otentikasi user FTP saja. AES dan 3DES merupakan algoritma kunci satu arah (simetris) yang digunakan untuk melindungi data. Munculah ide untuk mengembangkan sebuah aplikasi FTP Client dimana data yang akan diunggah ke FTP server di enkripsi dengan suatu kunci dan mengimplementasikan algoritma AESdan 3DESdalam proses enkripsinya, dan data akan didekripsikan dengan kata kunci yang sama pada saat data dienkirpsi, ketika data tersebut akan diunduh dari FTP server.

Kata kunci : File Transfer Protocol (FTP), AES, 3DES, enkripsi, dekripsi, keamanan data

I. PENDAHULUAN

FTP server yang ada di PT. Alam Sutera Realty, Tbk hanya dapat diakses dari jaringan lokal, namun ada rencana kedepannya dari Perusahaan untuk publish FTP server ini ke internet, dan dapat diakses dimana saja, kapan saja. Tidak dienkripsinya data yang diunggah ke FTP server merupakan masalah paling mendasar dalam keamanan data itu sendiri. Keamanan data yang ada di FTP server hanya dibatasi oleh otentikasi user login ke FTP server saja. Jika otentikasi user login ke FTP server tersebut diketahui oleh orang lain yang tidak berhak, data-data rahasia yang ada didalamnya dapat dengan mudah dicuri dan dibaca, serta tidak menutup kemungkinan untuk disalah gunakan.

II. LANDASAN TEORI

2.1. Definisi Keamanan Komputer

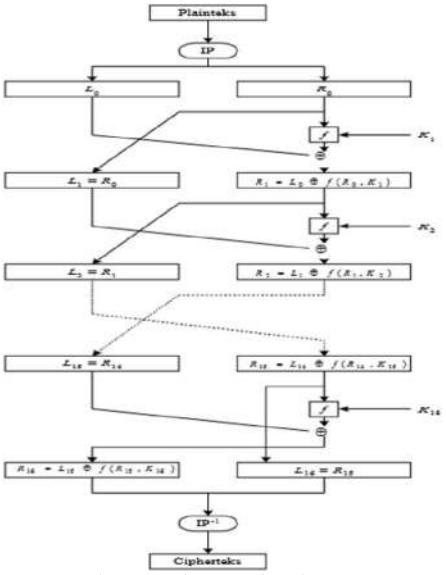
Keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak betanggung jawab[1].

2.2. Definisi Kriptografi

Kriptografi berasal dari bahasa Yunani yang terdiri dari dua suku kata, yaitu kripto dan graphia. Kripto artinya menyembunyikan dan graphia berarti tulisan. Secara definisi kriptografi adalah ilmu yang mempelajari teknikteknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data serta autentikasi data[2].

2.3. Algoritma Simetris DES

DES merupakan blockcipher yang beroperasi dengan blok berukuran 64 bit dan kunci 56 bit.



Gambar 1 : Skema Algoritma DES

DES mengenkripsikan 64 bit plaintext menjadi 64 bit ciphertext dengan menggunakan 56 bit kunci. Blok plaintext dipermutasi dengan matriks permutasi awal (*initial permutation* atau IP), dan hasil dari permutasi ini kemudian dilakukan enciphering sebanyak 16 kali dengan menggunakan kunci internal yang berbeda. Hasil dari enciphering ini kemudian dipermutasi dengan matriks permutasi kebalikan (*inverse initial permutation* IP^{-1}) menjadi ciphertext .

2.4. Algoritma Simetris 3DES

3DES (*Triple Data Encryption Standard*) merupakan salah satu algoritma simetris pada kriptografi yang digunakan untuk mengamankan data dengan cara menyandikan data. Algoritma 3DES adalah suatu algoritma pengembangan dari algoritma DES (*Data Encryption Standard*). 3DES menggunakan 3 kunci yang panjangnya 168 bit yang masing-masing panjangnya 56 bit. [3]

2.5. Algoritma Simetris AES Algoritma AES mengenkripsi data dalam 4 (empat) langkah dasar yaitu :

a) Transformasi SubBytes()

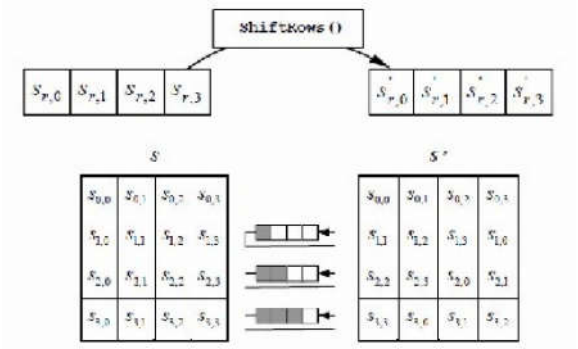
Transformasi SubBytes() memetakan setiap byte dari array state dengan menggunakan tabel subtitusi S-Box. AES hanya memiliki 1 (satu) buah S-Box ,tidak seperti DES yang memiliki S-Box berbeda pada tiap putaran.

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Gambar 2 : S-Box algoritma AES

b) Transformasi ShiftRows()

Transformasi ShiftRows() melakukan pergeseran secara *wrapping* (siklik) pada 3 (tiga) baris terakhir dari array state. Jumlah pergeseran bergantung pada nilai baris (r). Baris r =1 digeser sejauh 1 byte, r = 2 digeser sejauh 2 byte, dan r = 3 digeser sejauh 3 byte, sedangkan baris r = 0 tidak digeser[4].



Gambar 3 : Transformasi ShiftRows() AES

c) Transformasi MixColumns()

Transformasi MixColumns() mentransformasikan state kolom demi kolom.

Operasi ini dilakukan pada state kolom, dengan mengkonversi setiap kolom sebagai polinomial a(x) mod (x4 + 1). Setiap kolom diperlakukan sebagai polinom 4 suku pada GF (28).

d) Transformasi AddRoundKey()

Transformasi ini melakukan operasi XOR terhadap sebuah roundkey dengan array state, dan hasilnya disimpan di array state.

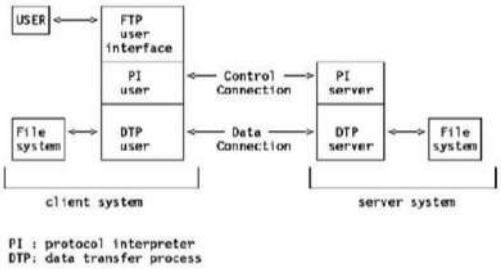
e) Ekspansi Kunci

Algoritma AES mengambil cipherkey (K) yang diberikan oleh pengguna, dan memanggil fungsi KeyExpansion() untuk membangkitkan sejumlah *roundkey* (banyaknya key (kunci) tergantung pada jumlah putaran). Kunci direpresentasikan dengan word (w[i]) serupa dengan state, akan tetapi elemen state-nya adalah cipherkey. Ekspansi kunci yang diperlukan AES dapat direpresentasikan dengan Nb(Nr+1) word. Adapun proses-proses yang ada dalam key schedule antara lain :

RotWord(), SubWord() dan Rcon().

2.6. *File Transfer Protocol* (FTP)

File transfer protocol (FTP) adalah suatu internet protokol *client-server* yang digunakan untuk mentransfer data (file) dari komputer *host ke server* dan sebaliknya, dalam suatu jaringan dengan menggunakan koneksi TCP port 21. FTP membutuhkan otentikasi username dan password untuk mengaksesnya[5].



Gambar 4: Skema FTP

III. RANCANGAN SISTEM DAN APLIKASI

3.1. Analisa Masalah

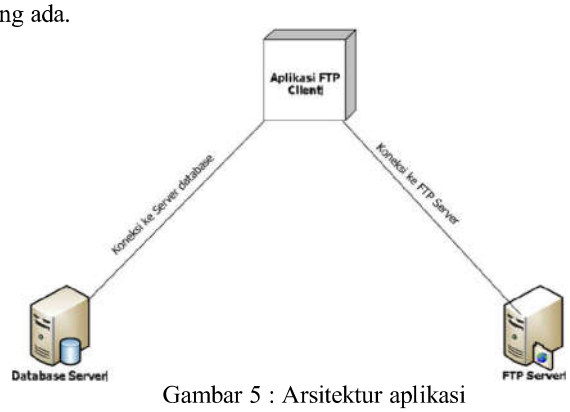
Masalah yang dihadapi saat ini adalah lebih menitik beratkan pada keamanan data yang diunggah ke FTP server itu sendiri. Keamanan data menjadi masalah utama jika memang kedepannya FTP server yang diperuntukan untuk menyimpan file-file hasil pemindaian dokumen-dokumen yang bersifat rahasia tersebut di-publish ke internet. Keamanan data hanya ada pada otentikasi user login pada FTP server, jika otentikasi user ini diketahui oleh orang yang tidak berhak, data-data didalam FTP server tersebut dapat disalahgunakan, ataupun bahkan dapat dihapus dari FTP server.

3.2. Penyelesaian Masalah

Dari analisa masalah diatas, maka perlu dibuatnya suatu aplikasi layaknya FTP client yang bersifat tertutup sebagai interface dimana seluruh file-file perjanjian yang berformat pdf dienkripsi dengan kunci tertentu dan diunggah ke FTP server. Adapun algoritma yang digunakan untuk mengenkripsi file tersebut adalah AES dan 3DES (TripleDES). Dimana file akan dienkripsi terlebih dahulu dengan algoritma AES dengan kunci yang diberikan setelah itu file hasil enkripsi akan dienkripsi kembali dengan algoritma 3DES dengan kunci yang sama. Jika proses enkripsi ini berhasil, file akan diunggah ke FTP server. Panjang kunci yang digunakan adalah 192 bit atau dengan kata lain 24 byte (24 karakter).

3.3. Arsitektur Aplikasi

Aplikasi FTP client akan melakukan koneksi ke Database server terlebih dahulu untuk mengakses database yang berhubungan dengan aplikasi FTP client. Setelah itu aplikasi akan melakukan koneksi ke FTP server untuk mengakses folder yang ada pada FTP server sesuai dengan otentikasi login yang ada.



Gambar 5 : Arsitektur aplikasi

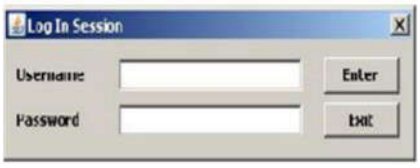
IV. HASIL DAN PEMBAHASAN

4.1. Spesifikasi Hardware dan Software Implementasi Program

Aplikasi yang dibangun akan bertindak sebagai FTP client, dimana aplikasi ini akan membuka akses ke FTP server. Dalam ujicoba implementasi aplikasi ini dibutuhkan aplikasiaplikasi pendukung seperti Netbean IDE 7.3, JDK 7, XAMPP v3.2.1, HeidiSQL. Adapun komputer yang digunakan dalam mengembangkan adalah sebuah laptop dengan spesifikasi processor Core 2 Duo T6500 @ 2.10 GHZ, RAM 4 GB dan Harddisk 300 GB.

4.2. Implementasi Program

a) Tampilan Layar Dialog Login (Session)



Gambar 6 : Tampilan layar dialog Login (Session)

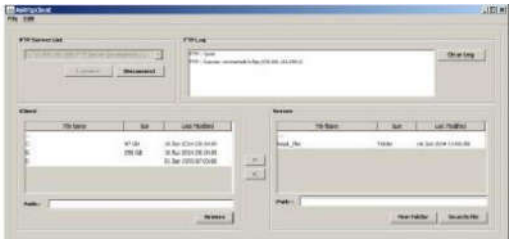
b) Tampilan Layar Frame GUI

Gambar 7 : Tampilan layar frame GUI

c) Tampilan Layar Frame GUI (*Button Connect Action Performed*)

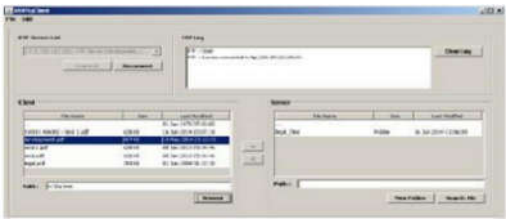
Gambar 8 : Tampilan layar list FTP Log *error* koneksi

Gambar 9 : Tampilan layar list FTP Log *error login* FTP



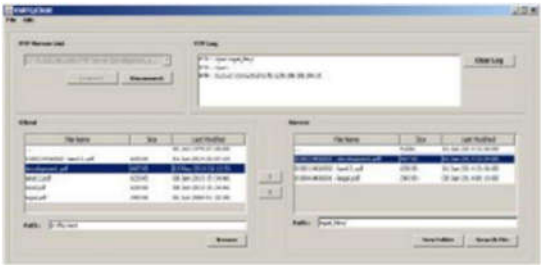
Gambar 10 : Tampilan layar frame GUI koneksi ke FTP *server*

d) Tampilan Layar Frame GUI (*Table File/Folder Client Mouse Clicked*)



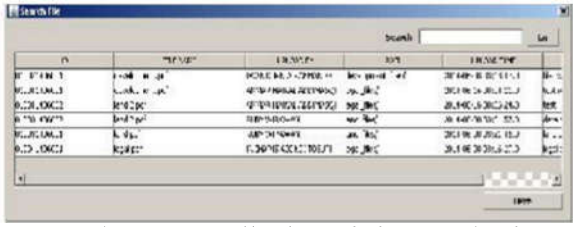
Gambar 11 : Tampilan layar frame GUI (*tabel File/Folder Client mouse clicked*)

e) Tampilan Layar Frame GUI (*Tabel File/Folder FTP Server Mouse Clicked*)



Gambar 12 : Tampilan layar frame GUI (*tabel File/Folder Server mouse clicked*)

f) Tampilan Layar *Dialog Search File*

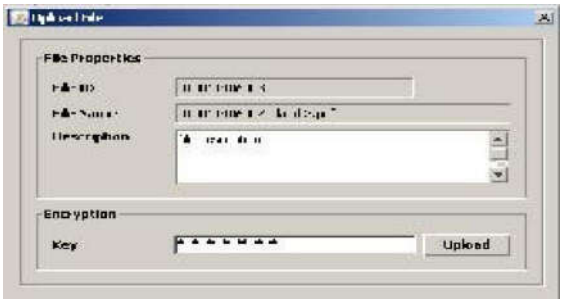


Gambar 13 : Tampilan layar *dialog Search File*

g) Tampilan Layar *Dialog Input Folder Name*

Gambar 14 : Tampilan layar *dialog Input Folder Name*

h) Tampilan Layar *Dialog Upload File*



Gambar 15 : Tampilan layar *dialog Upload File*

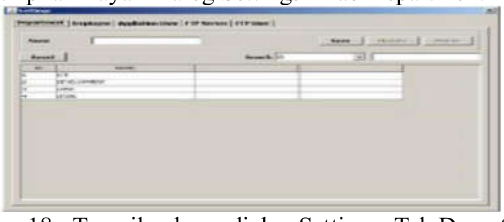
i) Tampilan Layar *Dialog Download File*

Gambar 16 : Tampilan layar *dialog Download File*

j) Tampilan Layar *Dialog Change Password*

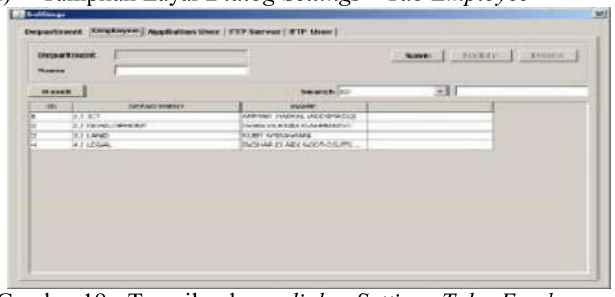
Gambar 17 : Tampilan layar *dialog Change Password*

k) Tampilan Layar Dialog Settings - Tab Department



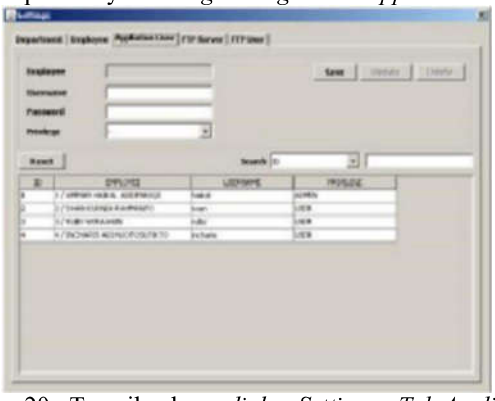
Gambar 18 : Tampilan layar dialog Settings -Tab Department

l) Tampilan Layar *Dialog Settings – Tab Employee*



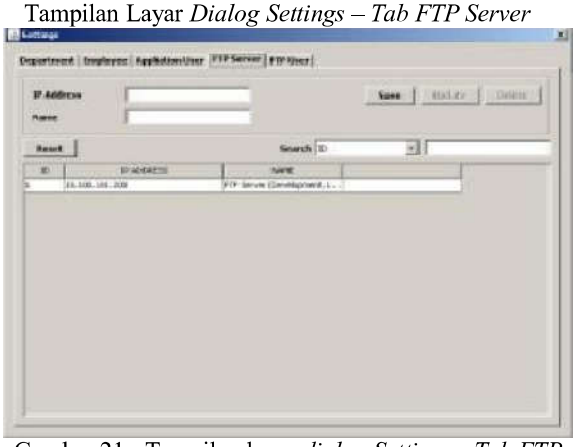
Gambar 19 : Tampilan layar *dialog Settings Tab - Employee*

m) Tampilan Layar *Dialog Settings - Tab Application User*



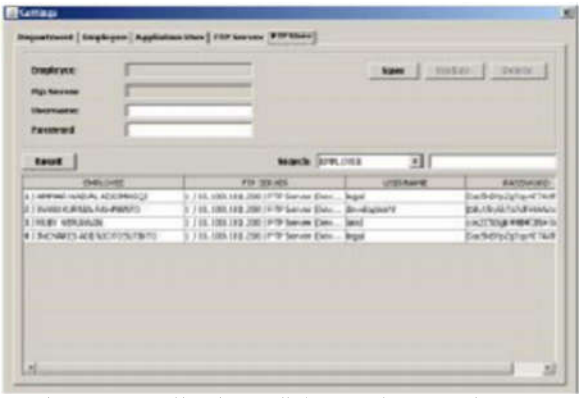
Gambar 20 : Tampilan layar *dialog Settings - Tab Application User*

n) Tampilan Layar *Dialog Settings – Tab FTP Server*



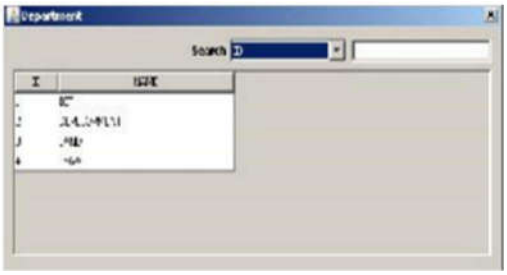
Gambar 21 : Tampilan layar *dialog Settings - Tab FTP Server*

o) Tampilan Layar Dialog Settings – Tab FTP User



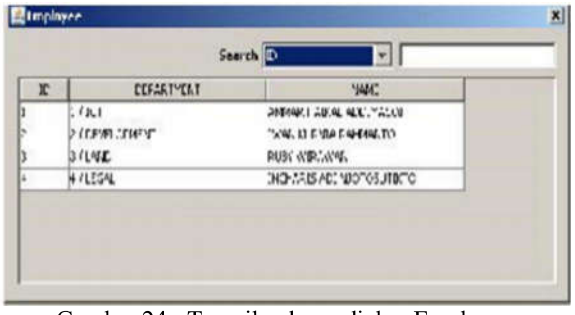
Gambar 22 Tampilan layar dialog Settings – Tab FTP User

p) Tampilan Layar Dialog Department



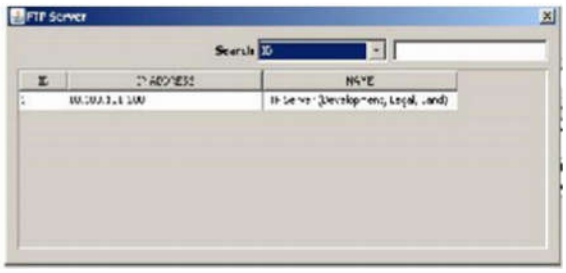
Gambar 23 : Tampilan layar dialog Department

q) Tampilan Layar Dialog Employee



Gambar 24 : Tampilan layar dialog Employee

r) Tampilan Layar Dialog FTP Server



Gambar 25 : Tampilan layar dialog FTP Server

4.3. Kelebihan dan Kekurangan Program

a) Kelebihan Program

Program ini memiliki kelebihan sebagai berikut :

- Tampilan GUI dari program ini dibuat dengan konsep user friendly, dimana pengguna dengan pengetahuan IT yang minim diharapkan dapat dengan mudah menggunakannya.
- Program ini membuat file-file yang disimpan pada FTP Server menjadi lebih aman dikarenakan file-file dienkripsi dengan kunci yang dimasukan pada saat proses mengunggah file ke FTP Server.
- Ukuran file program yang kecil dalam artian tidak membutuhkan space banyak pada hardisk dan mudah untuk didistribusikan dalam format jar.

b) Kekurangan Program

Program ini memiliki kekurangan sebagai berikut :

- Program ini masih belum sempurna dan dibutuhkan beberapa perbaikan untuk bugs yang teridentifikasi pada saat implementasi. Jika pengguna membuka aplikasi dan melakukan koneksi ke salah satu FTP Server dan pengguna tidak melakukan aktifitas apapun di program ini (idle) dalam waktu yang lama, lalu pengguna melakukan aktifitas baik untuk mengunggah file, mengunduh file ataupun mengakses file/folder dalam tabel FTP server, aplikasi akan menampilkan pesan error pada list FTP Log yang mengartikan bahwa koneksi ke FTP Server ditutup. Namun hal ini dapat diatasi dengan melakukan koneksi ulang ke FTP Server.
- Proses upload yang cukup lama ketika pengguna mengunggah file dengan ukuran besar. Hal ini dikarenakan file dienkripsi terlebih dahulu dengan 2 kali enkripsi yaitu AES dan 3DES setelah itu aplikasi akan melakukan proses mengunggah file ke FTP Server.
- Program ini membatasi penggunanya untuk mengubah nama file atau folder dan menghapus file atau folder yang terdapat dalam FTP Server. Hal ini dilakukan agar data atribut file yang disimpan didalam database seperti nama file dan lokasi file (path) yang diunggah ke FTP Server tetap valid. Hal ini menjadi sebuah isu ketika otentikasi login ke FTP server diketahui oleh seseorang yang tidak berhak, dan melakukan perubahan-perubahan pada file atau folder yang ada didalam FTP Server. Sehingga perlu adanya optimalisasi pada FTP server dalam *file and folder permission* untuk mengatasi isu ini.

V. KESIMPULAN

Berdasarkan kepada analisa permasalahan dan penyelesaian masalah yang dibahas didalam BAB-BAB sebelumnya, penulis membuat beberapa kesimpulan terhadap aplikasi yang dirancang, antaralain :

a. Dengan adanya aplikasi ini file yang disimpan ke FTPserver tingkat keamanannya akan bertambah karena file tersebut dienkripsi terlebih dahulu dengan menggunakan 2 (dua) algoritma kriptografi.
b. Penggunaan algoritma kriptografi AES dan 3DES dapat diimplementasikan dengan baik dengan menggunakan kunci yang sama dan diterapkan dengan metode block cipher ECB (ElectronicCodeBook), dimana tiap blok akan dienkripsi.
c. Program yang dikembangkan bersifat tertutup. Jika pengguna ingin mengunduh file yang ada pada FTPserver diharuskan menggunakan program ini. Hal ini dikarenakan adanya proses dekripsi data pada saat pengguna mengunduh file dari FTPserver.
d. Keamanan otentikasi login untuk FTPServer tidak sepenuhnya aman, otentikasi login dapat saja diketahui oleh orang yang tidak berhak. Dengan dienkirpsinya file yang diunggah ke FTPServer, orang yang tidak berhak ini dapat saja melakukan otentikasi login ke FTPServer dan mengunduh suatu file, namun file yang diunduh tidak akan dapat direpresentasikan sebagai data yang dapat dibaca.

Penulis sadar bahwa permasalahan yang telah dikembangkan masih jauh dari sempurna, sehingga perlu dilakukan penyempurnaan dalam rancangan program. Saran yang dapat dikembangkan antara lain:

a. Program ini perlu dikembangkan dimana pengguna dapat memilih metode enkripsi yang diinginkan, secara rancangan program file akan dienkripsi dahulu dengan algoritma AES selanjutnya dienkripsi kembali dengan algoritma 3DES. Pengguna dapat memilih apakah file tersebut akan dienkripsi dengan 3DES lalu dilanjutkan dengan AES atau sebaliknya.
b. Perlu dikembangkan program serupa berbasis mobile, hal ini akan mempermudah bagi pengguna dalam hal ini adalah karyawan dari PT. Alam Sutera Realty, Tbk dalam mengakses file dari perangkat mobile.
c. Memperbaiki algoritma program yang dibuat sehingga program dapat berjalan dengan lebih baik, efisien dan proses enkripsi ataupun dekripsi lebih cepat.

DAFTAR PUSTAKA

[1] D. Setiawan, *Sistem Keamanan Komputer*. Elex Media Komputindo, 2005.

[2] B. Schneier, *Applied Cryptography*, Second Edi. Wiley Computer Publishing, John Wiley & Sons, Inc., 1996.

[3] G. S, "Analisa Perbandingan QoS: Pengaruh Implementasi Enkripsi 3DES dan AES pada MPLS-VPN Untuk Layanan IP-Based Video Telephony," Universitas Indonesia, 2009.

[4] C. Beierle, P. Jovanovic, M. M. Lauridsen, G. Leander, and C. Rechberger, "Analyzing Permutations for AES-like Ciphers : Understanding ShiftRows."

[5] I. W. A. Sapura and C. R. A. Pramartha, "Perancangan FTP (File Transfer Protocol) Melalui SCTP (Stream Control Transmission Protocol) Menggunakan Socket Programming," in *Jurnal Elektronik Ilmu Komputer Universitas Udayana*, 2012.