PENERAPAN SISTEM KEAMANAN DENGAN KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD* (AES) DAN *KEY ADMINISTRATOR* PADA SINKRONISASI *FILE*

Wawan Qurniawan, Hero Wintolo, Dwi Nugraheny
Teknik Informatika STTA Yogyakarta
informatika@stta.ac.id

Abstract

File synchronization is the process of homogenization or adjustment between one file at a location with other files in the event that a change to be used up and running in a system. File synchronization is generally a process of data exchange in order to have the same amount of data. To maintain the confidentiality of the data necessary to maintain services for data security.

The use of cryptographic AES (Advanced Encryption Standard) to encrypt the file and combined with the administrator as an authentication key in making additions or changes to the file is a security system that can be applied to synchronize the files so that data confidentiality will be maintained.

The results of the implementation of file synchronization application by applying the AES cryptography and key administrators who carried on the local network and the Internet as a service application data synchronization between the user and the service back-up data as manual handling if storage was damaged and can avoid the theft of data from a file synchronized.

Keywords: file synchronization, security systems, cryptography AES, administrator key, Rijndael algorithm

1. Pendahuluan

Kebutuhan akan informasi yang *realtime* saat ini merupakan salah satu kebutuhan yang tak terelakan lagi. Hal ini menunjukkan bahwa minat masyarakat untuk mencari dan bertukar informasi melalui internet semakin meningkat. Peningkatan ini menjadi salah satu komoditi yang dimanfaatkan oleh sebagian manusia, misalnya dalam hal penyimpanan data. Penyimpanan data di internet saat ini menggantikan penyimpanan manual yang biasa dilakukan, misalnya didalam *hardisk, Compact Disc* (CD), maupun *flashdisk* yang rentan terhadap kerusakan.

Semakin meningkatnya layanan internet yang diberikan semakin meningkat pula kebutuhan seseorang akan layanan tersebut. Kebutuhan akan data yang dapat diakses dari berbagai ruang kerja dan komputer, sehingga memungkinkan pengguna dapat mengakses datanya dari tempat yang berbeda, selama mereka terhubung dalam jaringan internet tanpa harus melakukan proses *upload* dan *download* setiap ingin mengakses *file* tersebut. Namun internet juga merupakan tempat dimana semua orang dapat mengaksesnya, untuk kepentingan yang baik maupun sebaliknya. Sehingga memunculkan kekhawatiran pengguna internet dalam melakukan penyimpanan maupun pertukaran data didalamnya. Sehingga diperlukan layanan untuk menjaga keamanan data tersebut.

Sinkronisasi *file* merupakan salah satu cara agar *file* ataupun data pengguna akan selalu konsisten satu sama lainnya tanpa harus melakukan pengecekan *file* secara manual. Dan juga, *file* tersimpan di jaringan internet memungkinkan pengguna dapat mengakses kapan pun dan dimanapun. Didalam sinkronisasi *file*, penggunaan kriptografi merupakan salah satu sistem pengamanan data. Penggunaan kriptografi AES (*Advanced Encryption Standard*) dalam mengenkripsi *file* dan dikombinasikan dengan *key administrator* sebagai otentifikasi dalam melakukan penambahan atau perubahan *file* merupakan salah satu sistem keamanan yang dapat diterapkan pada sinkronisasi *file* sehingga kerahasiaan akan data tersebut dapat terjaga.

Dalam proses sinkronisasi file tidak menimbulkan permasalahan yang rumit apabila dilakukan *peer-to-peer* antar 2 komputer secara langsung, tetapi jika dilakukan pada jaringan komputer yang komplek seperti internet dengan memanfaatkan sebuah server akan menimbulkan masalah. Permasalahan yang timbul adalah dapatkah *file* yang ada di komputer satu dapat tersinkronisasikan dengan komputer lainnya dengan memanfaatkan *server* yang ada di intenet dan tetap terjaga keamanannya. Oleh karena itu perancangan aplikasi sinkronisasi file dengan menerapkan sistem keamanan kriptografi AES ini akan dikaji dan diteliti lebih mendalam untuk meminimalisir pengaruh yang muncul selanjutnya.

2. Landasan Teori

2.1 Sinkronisasi File

Sinkronisasi adalah proses pengaturan jalannya beberapa proses pada saat yang bersaman. Tujuan utama sinkronisasi adalah menghindari terjadinya inkonsistensi data dan untuk mengatur jalannya proses-proses sehingga dapat berjalan dengan lancar dan terhindar dari *deadlock* (Stalling2001). Sinkronisasi umumnya dilakukan dengan bantuan suatu perangkat atau aplikasi sinkronisasi.

Sinkronisasi *file* adalah proses penyeragaman atau penyesuaian antara satu *file* pada satu lokasi dengan *file* lainnya bila mengalami perubahan agar bisa digunakan dan berjalan dalam suatu sistem tertentu secara *realtime*. Sinkronisasi *file* pada umumnya merupakan proses pertukaran data agar memiliki jumlah data yang sama dan bertujuan sebagai layanan *back-up* data ke suatu media tertentu. Sinkronisasi dapat berjalan dalam berbagai protokol jaringan komputer, misalnya FTP (*File Transfer Protocol*).

2.2 Kriptografi AES

Kriptografi merupakan sebuah kata serapan dari bahasa asing, dalam hal ini bahasa inggris, yaitu *cryptography*. *Cryptography* atau *cryptology* berasal dari bahasa Yunani, yaitu *kryptos* (tersembunyi) dan *graphō* (menulis). Kriptografi adalah ilmu atau seni untuk menyembunyikan suatu informasi. Proses menyembunyikan informasi ini dilakukan dengan teknik penyandian, atau mengubah pesan atau informasi menjadi sandi-sandi yang tidak dimengerti oleh orang lain, selain pembuat dan penerimanya.

Advanced Encryption Standart (AES) adalah acuan yang dipakai sebagai standar algoritma kriptografi pada masa sekarang. Kriptografi AES merupakan pengganti dari kriptografi DES (*Data Encryption Standard*), Karena algoritma DES sudah dianggap tidak aman lagi. *National Institute of Standard and Technology (NIST)* sebagai Agensi Perdagangan AS menetapkan algoritma *Rijndael* sebagai algoritma standar yang dipakai pada kriptografi AES atau kriptografi kunci simetris modern.

Algoritma *Rijndael* menggunakan substitusi, permutasi, dan sejumlah putaran yang dikenakan pada tiap blok yang akan dienkripsi atau didekripsi. Untuk setiap putarannya, *Rijndael* menggunakan kunci yang berbeda. Kunci setiap putaran disebut *round key*. Tetapi tidak seperti DES yang berorientasi *bit*, *Rijndael* beroperasi dalam orientasi *byte*, sehingga memungkinkan untuk implementasi algoritma yang efisien ke dalam *software* dan *hardware*. Ukuran blok untuk algoritma *Rijndael* adalah 128 bit (16 byte).

Algoritma *Rijndael* dapat mendukung panjang kunci 128 bit sampai 256 bit dengan step 32 bit. Panjang kunci berpengaruh pada jumlah putaran yang dikenakan pada tiap blok. Misalnya, untuk ukuran blok dan panjang kunci sebesar 128 bit ditentukan 10 putaran, sedangkan untuk ukuran blok 128 bit dan panjang kunci 256 bit jumlah putaran yang ditentukan adalah 14 putaran.

2.3 Key Administrator

Key administrator berasal dari istilah yang diambil dari kata key yang berarti kata kunci dan kata *administrator* yang berarti sesuatu yang dapat mengelola dan mempunyai hak akses secara penuh terhadap suatu sistem tertentu. *Key Administrator* merupakan kata kunci yang digunakan sebagai otentifikasi dalam melakukan perubahan maupun penambahan terhadap *file* yang disinkronsasikan. *Key* ini tersimpan di *registry windows* dan dienkripsi dengan MD5 memungkinkan keamanan akan tetap terjaga.

3. Perancangan

3.1 Kebutuhan Perangkat Keras

Hardware atau perangkat keras merupakan suatu komponen yang sangat mendukung dalam proses komputerisasi. *Hardware* berperan dalam *input* data, proses, dan menampilkan *output*. Berikut ini adalah spesifikasi *hardware* yang digunakan dalam membuat aplikasi ini:

1. *Processor* Intel Core 2 Duo
2. RAM 1 GB,
3. *Harddisk* 150 GB,
4. *Keyboard* dan *mouse* standar.

3.2 Kebutuhan Perangkat Lunak

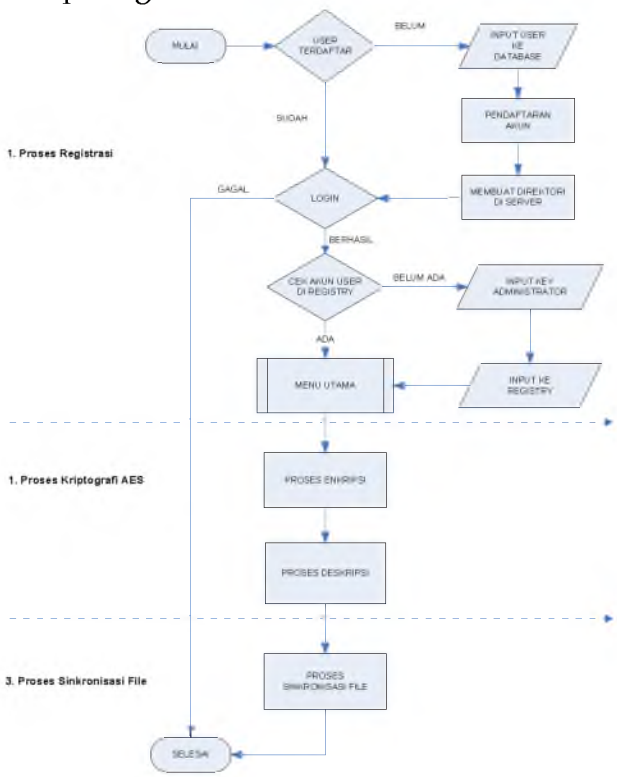
Adapun spesifikasi *software* atau perangkat lunak yang digunakan dalam pembuatan aplikasi ini adalah :

1. Sistem Operasi Windows 7 *Ultimate*
2. Delphi 7.0
3. XAMPP 1.7.1
4. Komponen Zeos *Database Connector*
5. *FTP Server*

3.3 Sistem *Flowchart*

Rancangan ini digunakan untuk mendesain dan merepresentasikan suatu program. Sebelum pembuatan program, fungsinya adalah mempermudah dalam menentukan alur logika program yang akan dibuat. Sesudah pembuatan program fungsinya adalah untuk menjelaskan alur program kepada orang lain atau *user*.

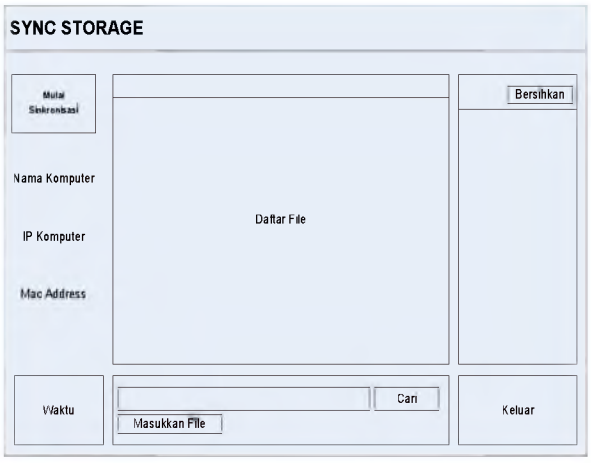
Pada rancangan *flowchart* aplikasi penerapan kriptografi AES pada sinkronisasi *file* terdiri dari 3 bagian, yaitu proses registrasi *user*, proses sinkronisasi dan proses enkripsi deskripsi. Rancangan ini dapat dilihat pada gambar 1.



Gambar 1 Perancangan *Flowchar* Penerapan Kriptografi AES dan *Key Administrator* pada Aplikasi Sinkronisasi *File*

3.4 Perancangan Antar Muka

Perancangan tampilan utama aplikasi sinkronisasi file dengan menerapkan kriptografi AES dan key administrator seperti pada gambar 1. Rancangan tersebut terdiri dari 3 bagian, yaitu tombol Mulai Sinkronisasi dan identitas computer yang digunakan untuk melakukan proses sinkronisasi, daftar file digunakan untuk menampilkan daftar list file yang disinkronsasikan, input file digunakan untuk memasukkan data ke dalam daftar file. Tampilan rancangan tesebut seperti pada gambar 2.



Gambar 2 Tampilan Rancangan Menu Utama

3.5 Peralatan Jaringan Komputer

Penelitian ini membutuhkan peralatan jaringan komputer yang akan digunakan dalam proses uji coba hasil perancangan perangkat lunak sinkronisasi yang menghubungkan tiga buah komputer dalam sebuah jaringan komputer, peralatan tersebut adalah :

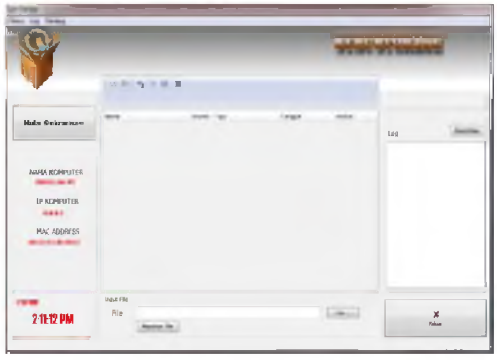
1. *Switch*
2. Modem GSM (dengan kartu Axis)

4. Uji Coba

4.1 Penjelasan Aplikasi

Sesuai rancangan pada gambar 1, didapat hasil penerapan aplikasi sinkronisasi seperti pada gambar 2 dan dapat dijelaskan sebagai berikut

1. Setelah program ini dijalankan dan berhasil memasukkan email dan password sesuai akun yang dimiliki, makan akan muncul tampilan utama aplikasi ini seperti pada gambar 3.

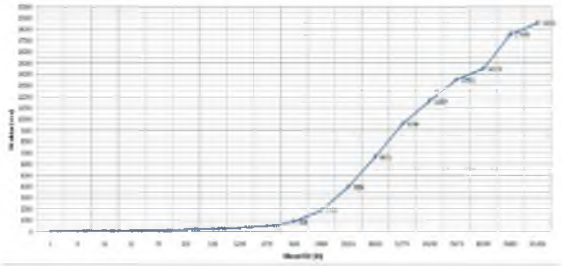


Gambar 3 Tampilan Menu Utama

2. Langkah selanjutnya adalah dengan memasukkan file yang ingin disinkronisasikan dengan cara menekan tombol "Masukkan File" dan memasukkan *key administrator* sebagai otentifikasi dalam menjalankan proses enkripsi dan *input file*.
3. Kemudian menekan tombol "Mulai Sinkronisasi" untuk memulai proses sinkronisasi dari computer lokal ke server.
4. Kemudian untuk mengecek keberhasilan proses sinkronisasi pada computer 2 dengan cara menjalakan aplikasi sinkronisasi dengan akun yang sama. Setelah masuk ke menu utama pada computer 2 yang dilakukan adalah menekan tombol "Mulai Sinkronisasi" dan file yang di tambahkan pada computer 1 akan bertambah pada computer 2.
5. Kemudian untuk proses hapus file yaitu dengan cara menghapus file yang ada di computer 1 dengan memilih file dan klik kanan "hapus file", serta menekan tombol "Mulai Sinkronisasi".
6. Pada Komputer 2 tekan kembali tombol "Mulai Sinkronisasi" maka file yang dihapus pada computer 2 akan ikut terhapus.
7. Sedangkan untuk proses deskripsi yaitu pada saat membuka file dengan cara memilih file kemudian klik kanan "Buka File". Kemudian memasukkan *key administrator* sebagai otentifikasi dan proses deskripsi akan berjalan.

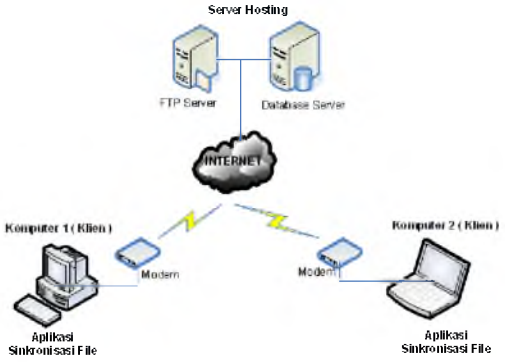
4.2 Uji Coba LAN

Uji coba LAN dilakukan dengan menggunakan 3 buah computer, 1 komputer dijadikan server dan 2 buah computer dijadikan klien. Uji sinkronisasi dilakukan dengan cara menambahkan file pada computer 2 dan di cek kedalam komputer 3. Grafik hasil dari uji coba singkronisasi dapat dilihat pada gambar 4.



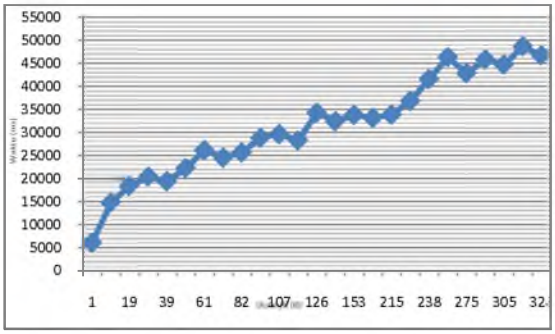
Gambar 4 Grafik Hasil Uji Coba Sinkronisasi dalam LAN

4.3 Uji Coba Internet



Gambar 5 Skema Uji Sinkronisasi *File* Dengan Internet

Uji coba internet dilakukan dengan menggunakan 2 buah computer klien, sebuah server hosting yang dijadikan server. Uji sinkronisasi dilakukan dengan cara menambahkan file pada computer 1 dan di cek kedalam computer 2. Grafik hasil dari uji coba singkronisasi dapat dilihat pada gambar 6.

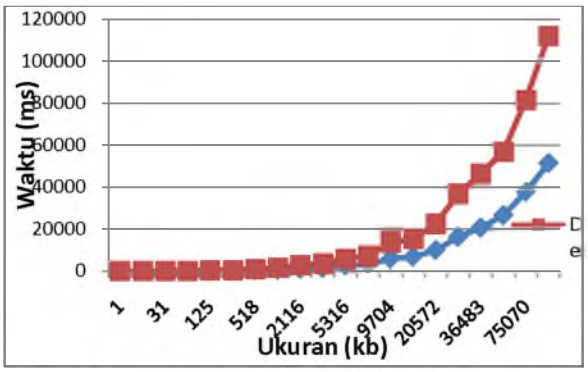


Gambar 6 Grafik Hasil Uji Coba Sinkronisasi dalam internet

4.4 Uji Coba Kriptografi

Uji kriptografi merupakan pengujian terhadap *file* yang akan diinputkan ke dalam aplikasi sinkronisasi *file*. Pengujian dilakukan untuk mendapatkan data waktu proses enkripsi deskripsi dan ukuran *file* sebelum dan sesudah enkripsi. Pengujian kriptografi meliputi

proses enkripsi pada *input file* dan proses deskripsi pada *open file*. Berikut hasil proses enkripsi ditampilkan pada grafik gambar 7.



Gambar 7 Grafik Hasil Proses Enkripsi dan Deskripsi

5. Analisa Hasil Uji Coba

Dari pengujian yang telah dilakukan dengan 2 jenis proses pengujian, yaitu pengujian sinkronisasi dan pengujian kriptografi diperoleh analisa dari hasil uji fungsi tersebut.

Uji coba yang pertama adalah uji coba sinkronisasi data dilakukan dengan menggunakan 3 buah komputer, 1 komputer dijadikan sebuah *server* dan 2 buah komputer dijadikan sebagai klien dihubungkan dalam jaringan lokal dengan media transmisi kabel LAN dan sebuah *switch* dengan maksimum 100 Mbps. Sinkronisasi dilakukan dalam pemindahan data dari komputer 2 ke komputer 3 dan kebalikannya dari komputer 3 ke komputer 2 melalui komputer *server*. Pada ukuran *file* kecil antara 1 – 1000 kb membutuhkan waktu kurang dari 0,3 detik, kemudian pada ukuran *file* 1000kb membutuhkan waktu 0,5 detik, dan ukuran *file* diatas 1000kb dengan kenaikan ukuran *file sebesar* 10000kb (10Mb) rata-rata menghasilkan estimasi waktu sekitar 2000 ms (1detik). Sehingga kecepatan rata – rata proses sinkronisasi *file* pada jaringan LAN yaitu 5000kb (5Mb) setiap 1 detik.

Sedangkan ujicoba sinkronisasi pada jaringan internet dilakukan dengan 2 komputer klien dan sebuah layanan *hosting* sebagai *server* dengan menggunakan koneksi modem kecepatan maksimal 128 Kbps. Dari hasil ujicoba proses sinkronisasi berjalan tidak teratur. Hal tersebut disebabkan kecepatan koneksi internet yang dipakai tidak stabil, sehingga waktu yang digunakan dalam melakukan proses sinkronisasi juga tidak stabil. Saat koneksi lambat proses sinkronisasi menjadi lebih lama pula. Oleh karena itu kecepatan proses sinkronisasi pada jaringan internet sangat tergantung pada kestabilan koneksi jaringan internet yang dipakai.

Dari hasil kedua ujicoba pada LAN dan internet dalam melakukan proses sinkronisasi *file* memunculkan tabel kecepatan perpindahan data yang dapat dilihat pada tabel 1 dan 2.

Tabel 1 Kecepatan perpindahan data per ukuran *file* (Mb)

No	Ukuran File (Mb)	LAN	
		Waktu	Kecepatan
1	± 1	0.3	3.3
2	± 5	1	5
3	± 10	2	5
4	± 50	10	5

5	± 100	19	5.2

Tabel 2 Kecepatan perpindahan data per ukuran *file* (Kb)

No	Ukuran File (Kb)	Internet	
		Waktu	Kecepatan
1	± 10	15	0.67
2	± 50	22	2.27
3	± 100	30	3.33
4	± 200	35	5.71
5	± 300	49	1.12

Berdasarkan analisa yang telah diperoleh dapat diambil kesimpulan bahwa kecepatan proses sinkronisasi *file* dipengaruhi beberapa faktor, yaitu ukuran *file* dan kecepatan dari koneksi yang dipakai, serta kecepatan proses sinkronisasi berbanding lurus dengan ukuran *file* yang digunakan.

Uji coba selanjutnya yaitu uji coba kriptografi AES pada aplikasi sinkronisasi *file*. Uji coba dilakukan pada saat memasukkan *file* untuk mengetahui waktu enkripsi dan saat membuka *file* untuk mengetahui waktu deskripsi. Berdasarkan uji coba yang dilakukan bahwa pada ukuran *file* kecil (kurang dari 1 Mb) waktu yang diperlukan untuk proses enkripsi hampir sama dengan waktu deskripsi, namun setelah ukuran *file* mencapai lebih dari 2 Mb waktu yang diperlukan pada proses enkripsi dan deskripsi mulai menunjukkan perbedaan. Setiap kenaikan ukuran *file* sebesar 5 Mb, waktu enkripsi lebih cepat 1 detik dari waktu deskripsi. Berikut contoh dari hasil proses enkripsi dan deskripsi dari file dengan tipe gambar (jpg) seperti pada gambar 8.1, gambar 8.2 dan gambar 8.3.

Gambar 8.1 Contoh *File* Gambar asli

Gambar 8.2 Contoh Gambar telah dienkripsi

Gambar 8.3 Contoh *File* Gambar telah dideskripsi kembali

Dari analisa yang dilakukan dapat disimpulkan bahwa menunjukkan kecenderungan kenaikan waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi. Semakin besar ukuran suatu *file* maka semakin lama pula waktu yang dibutuhkan untuk melakukan proses enkripsi dan proses dekripsi

6. Kesimpulan

Kesimpulan yang diperoleh dari hasil analisa pengujian aplikasi sinkronisasi *file* adalah sebagai berikut :

1. Aplikasi yang dirancang dalam tugas akhir ini dapat digunakan sebagai aplikasi untuk mensinkronisasikan *file* didalam suatu *directory* lokal antara dua komputer *client* yang berbeda dengan menggunakan satu akun yang sama serta juga dapat dijadikan layanan *back-up* data-data *client* yang tersimpan di *server* atau internet.
2. Penggunaan kriptografi AES dan *key administrator* memberikan keamanan terhadap aplikasi sinkronisasi dan terhadap file yang disinkronisasikan.
3. Faktor koneksi jaringan dan ukuran *file* menjadi faktor yang mempengaruhi proses sinkronisasi. Didalam jaringan internet diperlukan *bandwith* yang cukup besar agar proses sinkronisasi *file* dapat berjalan dengan lancar. Dan semakin besar ukuran *file* yang disinkronisasikan semakin besar estimasi waktu yang dibutuhkan pada proses sinkronisasi dan proses kriptografi AES yang terjadi.

Selain kesimpulan, penelitian ini juga memiliki saran yang dapat digunakan untuk pengembangan dan penelitian selanjutnya yang terkait dengan penelitian ini. Saran tersebut antara lain:

1. Aplikasi sinkronisasi *file* ini dapat dikembangkan lagi didalam berbagai platform, misalnya dapat berjalan di sistem operasi linuk, berbasis web bahkan berbasis *mobile (android, iphone, windows phone)*.
2. Apabila dijalankan pada jaringan internet dengan koneksi jaringan yang lambat, diperlukan penambahan suatu sistem untuk *kompress* data agar ukuran *file* dapat diperkecil sehingga proses sinkronisasi dalam berjalan lebih cepat dan efisien.

Referensi

[1] Husni, Membuat Aplikasi Database Client-Server dengan Delphi dan MySQL, Graha Ilmu, Yogyakarta, 2004.

[2] Kristanto, Andri., Keamanan Data Pada Jaringan Komputer, Gava Media, Yogyakarta, 2005.

[3] Rafiudin, Rahmat., Membangun Server FTP, Andi Offset, Yogyakarta, 2005 .

[4] Sadikin, Rifki., Kriptografi Untuk Keamanan Jaringan, Andi Offset, Yogyakarta, 2012.

[5] Stallings, William., *Operating Systems: Internal and Design Principles*, Fourth Edition, Prentice-Hall International, New Jersey, 2001.

[6] Stallings, William., *Cryptography and Network Security*, Fourth Edition, Pearson Education, New Jersey, 2006.

[7] Wintolo, Hero., Sinkronisasi Data pada Tabel yang Tersimpan di Dua Database Server yang Berbeda, Jurnal Ilmiah Angkasa Volume II, Nomor 1, Mei 2010.

[8] (30 Mei 2012) http://id.hicow.com/perangkat-selular/sinkronisasi-data/file-data-592152.html

[9] (10 Juni 2012) http://rendramm2.wordpress.com/2012/01/17/program-enkripsi-file-dengan-metode-aes-menggunakan-delphi-7-part-1/

[10] (10 Juni 2012) http://www.teddybdg.wordpress.com/Delphi/Index.php