Perbandingan Performansi Pengamanan File Backup LPSE Menggunakan Algoritma DES Dan AES

I Putu Agus Eka Darma Udayana[1], Nyoman Putra Sastra [2]

***Abstract*— LPSE is an institution that was established to provide services for the procurement of goods and services electronically which facilitates the ULP. LPSE has a main server that contains data of procurement of goods and services. To ensure availability of per transaction data and to support the availability of the server, the server backup devices are provided. In the mechanism, the backup data from the main server to the backup server transmision over the network LAN is implemented. In the process of data transfer, a method for maintaining data security is required. Encryption and description methods used in this study are DES and AES algorithms. Because it contains the encryption process, it is required a computational processes that would burden the server. From the test results, the AES method is better than the DES method with an average time of 195.4 seconds for each encryption file, 189.1 seconds faster than DES method. The file size of encryption is not much different, so it would make the time required in the backup process is not much different. With less time required in the security process, the server load also decreased.**

***Intisari*— LPSE merupakan suatu lembaga yang didirikan dengan tujuan untuk menyelenggarakan sistem pelayanan pengadaan barang dan jasa secara elektronik dengan memfasilitasi ruang lingkup kerja ULP. LPSE mempunyai server utama yang berisi data penting pengadaan barang dan jasa. Untuk menjaga availability data setiap transaksi dan mendukung availability sistem tersebut, maka disediakan perangkat server cadangan. Dalam mekanismenya dilakukan backup data dari server utama menuju server backup melalui jaringan LAN. Pada proses transfer data diperlukan suatu metode agar keamanan data dapat dijaga. Mekanisme keamanan data enkripsi dan deskripsi yang digunakan adalah algoritma DES dan AES. Karena adanya proses enkripsi ini, diperlukan komputasi yang secara tidak langsung akan membebani server. Dari hasil pengujian, metode AES lebih unggul daripada metode DES dengan rata-rata waktu enkripsi setiap file sebesar 195,4 detik, lebih cepat 189,1 detik dari metode DES. Ukuran file hasil enkripsi juga tidak jauh berbeda, sehingga membuat waktu yang dibutuhkan dalam proses backup juga tidak jauh berbeda. Dengan semakin sedikit waktu yang dibutuhkan dalam proses pengamanan, maka beban server juga akan semakin berkurang.**

***Kata Kunci*— Enkripsi, Deskripsi, DES, AES**

I. PENDAHULUAN

LPSE (Layanan Pengadaan Secara Elektronik) merupakan suatu unit kerja yang didirikan pada seluruh Kementerian/Lembaga/Satuan Kerja Perangkat Daerah/ lnstitusi Lainnya (K/L/D/I) dengan tujuan untuk menyelenggarakan suatu sistem pelayanan pengadaan barang maupun jasa yang bersifat secara elektronik serta memberikan fasilitasi untuk membantu kinerja ULP atau Pejabat Pengadaan dalam melaksanakan proses pengadaan barang dan jasa secara elektronik. Ketika suatu ULP atau Pejabat Pengadaan suatu instansi tidak memiliki layanan LPSE, maka ULP tersebut dapat menggunakan atau meminjam fasilitas LPSE terdekat dengan wilayah kedudukannya untuk dapat melaksanakan pengadaan secara elektronik [1]. Selain memiliki fungsi memfasilitasi ruang kerja ULP atau Pejabat Pengadaan dalam proses melaksanakan pengadaan barang dan jasa secara elektronik, LPSE juga memiliki kewajiban untuk melayani registrasi rekanan penyedia barang dan jasa yang berdomisili pada wilayah kerja LPSE yang bersangkutan. Proses pengadaan barang dan jasa secara elektronik tentunya akan dapat meningkatkan transparansi dan akuntabilitas, akses pasar serta persaingan yang sehat antar persaingan usaha, dapat mengefisiensi proses pengadaan, membantu proses monitoring, audit dan tentunya akan memenuhi informasi yang *real time* dengan tujuan untuk mewujudkan *clean and good government* dalam proses pengadaan barang dan jasa dana pemerintah.

Pada hakikatnya layanan LPSE berdiri pada sebuah layanan *server* aplikasi dan *server database*. Semua data transaksi yang dilakukan melalui layanan LPSE akan disimpan pada *database* maupun file *system server* LPSE. Untuk mendukung *availability* layanan LPSE dibutuhkan *server* cadangan atau *server backup* untuk mengantisipasi jika terjadi hal-hal yang tidak diinginkan pada *server* utama layanan LPSE. Proses *backup* tersebut dilakukan melalui media transmisi jaringan LAN. Ketika berbicara jaringan LAN, suatu jenis kejahatan bisa dilakukan untuk memanipulasi data yang ada dalam jaringan tersebut. Salah satu jenis kejahatan yang bisa dilakukan dalam jaringan LAN tersebut adalah *man of middle attack*. Dimana jenis kejahatan ini akan mengambil atau melakukan penyadapan terhadap data yang melewati jaringan LAN. Mengingat data LPSE merupakan sesuatu yang bersifat rahasia tentunya hal ini akan menjadi masalah besar untuk mekanisme *backup* data secara berkala tersebut. Untuk mengatasi maslah tersebut perlu dilakukan mekanisme enkripsi pada file yang akan ditransfer dari *server* utama menuju *server backup*.

Terdapat beberapa metode ataupun mekanisme yang dapat digunakan sebagai algoritma pendukung dalam melakukan pengamanan data LPSE tersebut. Adapun metode-metode keamanan data yang dapat digunakan adalah metode OTP, DES, RC2, RC4, RC5, RC6, IDEA, *Twofish*, *Magenta*, FEAL, SAFER, LOKI, CAST, AES, DES, Blowfish, GOST, A5, *Kasumi* dan lain lain [2]. Dalam kasus ini metode enkripsi yang digunakan adalah metode DES dan AES. Penggunaan kedua metode ini karena metode DES dan AES merupakan jenis algoritma pengamanan yang menggunakan kunci simetris sehingga waktu proses enkripsi yang diperlukan oleh algoritma ini relatip cepat. Cepatnya waktu proses enkripsi ini

[1]*Mahasiswa, Magister Sistem Informasi Dan Komputer Universitas Udayana, Denpasar, Bali 80232 (telp: 0361-239599; fax: 0361-239599; e-mail: agus.ekadarma@gmail.com)*

[2,] *Dosen Jurusan Teknik Elektro dan Komputer Fakultas Teknik Universitas Udayana, Jln. Jalan Kampus Bukit Jimbaran 80361 INDONESIA (telp: 0361-703315; fax: 0361-4321; e-mail: putra.sastra@unud.ac.id)*

disebabkan karena adanya efisiensi pada proses pembangkitan kunci pada proses enkripsi [3]. Dengan semakin cepatnya proses enkripsi yang terjadi pada *server* LPSE, maka beban kerja *sever* akan dapat lebih fokus pada sistem pelayanan pengadaan berbasis *web*. Dari implementasi tersebut nantinya akan dilakukan pengujian seberapa lama waktu yang dibutuhkan dari masing-masing metode dalam melakukan proses enkripsi dan deskripsi.

II. METODE KRIPTOGRAFI

A. *Kriptografi*

Kriptografi berasal dari bahasa Yunani yang dibagi menjadi dua buah kata yaitu kripto yang dapat berarti suatu rahasia dan graphia yang dapat berarti suatu tulisan [4]. Kriptografi secara harpiah dapat diasumsikan sebagai suatu ilmu dan sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna [5]. Bentuk tersandi ini hanya dapat dibaca oleh pihak yang berhak membacanya. Pesan yang akan dirahasiakan sebelum disamarkan disebut *plainteks*, sedangkan pesan setelah disamarkan disebut *chiperteks*. Proses penyamaran *plainteks* ke *chiperteks* disebut enkripsi, sedangkan pengembalian *chiperteks* menjadi *plainteks* semula disebut dekripsi.

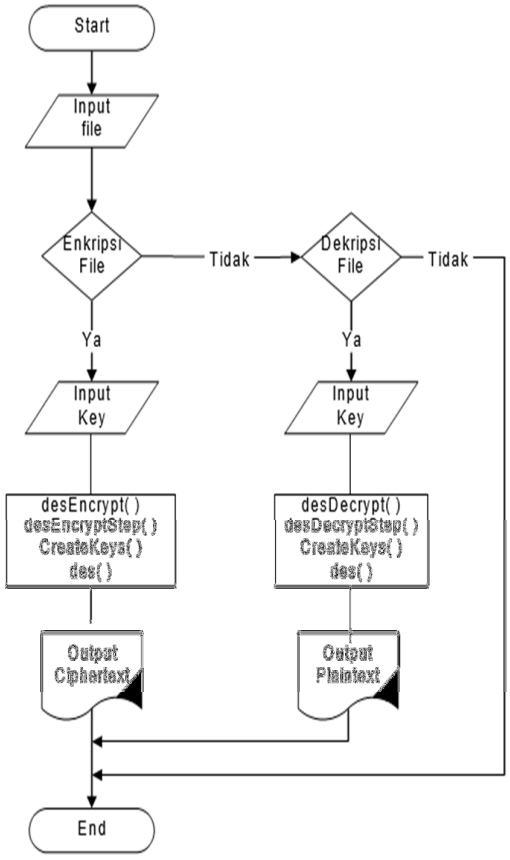
B. *Kriptografi Simetris Dan Asimetris*

Algoritma simetris menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data [6]. Untuk mendekripsikan data, penerima menggunakan kunci yang sama dengan kunci yang digunakan pengirim untuk mengenkripsi data. Contoh dari algoritma ini adalah *Data Encryption Standard* atau disingkat dengan DES, *International Data Encryption Algorithm* atau sering disebut IDEA dan *Advanced Encryption Standard* yang dikenal dengan AES, serta masih ada beberapa algoritma kriptografi yang termasuk dalam ranah kriptografi simetris. Dalam penelitian yang dilakukan, algoritma DES dan AES akan dibahas lebih lanjut sebagai metode penelitian.

Pada algoritma asimetris, digunakan dua buah kunci yang berhubungan yang disebut dengan kunci umum dan kunci pribadi. Kunci umum dapat dipublikasikan sehingga pesan dapat dienkripsikan tetapi tidak dapat didekripsikan dengan kunci tersebut. Kunci pribadi hanya boleh digunakan oleh pihak yang berhak untuk mendekripsikan pesan yang terenkripsi. Algoritma yang menggunakan kunci umum dan publik ini antara lain *Digital Signature Algorithm* (DSA), *RivestShamir-Adleman* (RSA), *Diffie-Hellman* (DH), dan sebegainya.

C. *Algoritma DES (Data Encryption Standard)*

Algoritma enkripsi yang paling banyak digunakan di dunia adalah DES (*Data Encryption Standard*) yang diadopsi oleh NIST (*National Institute of Standard and Technology*) sebagai standard pengolahan informasi Federal AS [7]. DES merupakan keamanan dasar yang dipublikasikan sejak 15 Januari 1977 dan sering digunakan dimana-mana, oleh karena itu ada kemungkinan DES akan tetap dilanjutkan penelitiannya sehingga menjadi suatu sistem enkripsi yang kuat dari segi keamanan data, sistem akses *control* dan *password*. Gambar 1 dibawah adalah gambar dari konsep dasar metode DES. Data dienkrip dalam blok-blok 64 bit menggunakan kunci 56 bit. DES mentransformasikan input 64 bit dalam beberapa tahap enkripsi ke dalam *output* 64 bit. Dengan tahapan dan kunci yang sama, DES digunakan untuk membalik enkripsi yang biasa disebut dengan proses dekripsi.



Gambar. 1. Flowchart Proses Enkripsi dan Dekripsi Pada Metode DES.

D. *Algoritma AES (Advanced Encryption Standard)*

Algoritma AES pertama kali diperkenalkan oleh NIST (*National Institute of Standard and Technology*), tepatnya pada tahun 2001. Dimana algoritman ini digunakan sebagai pengganti algoritma DES yang semakin lama semakin mudah untuk dipecahkan kuncinya [5].

Algoritma AES merupakan algoritma simetri yaitu mengunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma AES memiliki tiga pilihan kunci yaitu tipe: AES-128, AES-192 dan AES-256 [8]. Masing-masing tipe menggunakan kunci internal yang berbeda yaitu *round key* untuk setiap proses putaran. Proses putaran enkripsi AES-128 dikerjakan sebanyak 10 kali.

- *Addroundkey*
- Melakukan putaran dengan jumlah *a*-1, dengan proses *SubBytes*,

- *ShiftRows, MixColumns*, dan *AddRoundKey*. *Final round* merupakan putaran akhir dengan proses *SubBytes, ShiftRows*, dan *AddRoundKey*.

Sedangkan pada proses dekripsi AES-128, proses putaran juga dikerjakan sebanyak 10 kali (a=10), yaitu sebagai berikut :

- *AddRoundKey*.
- Putaran sebanyak a-1 kali, dimana pada setiap putaran dilakukan proses: I*nverseShiftRows, InverseSubBytes, AddRoundKey,* dan *InverseMixColumns*.
- *Final round*, adalah proses untuk putaran terakhir yang meliputi *InverseShiftRows, InverseSubBytes,* dan *AddRoundKey*.

Pada enkripsi dan dekripsi AES-192 proses putaran dikerjakan 12 kali (a=12), sedangkan untuk AES-256 proses putaran dikerjakan sebanyak 14 kali (a=14).

III. ANALISIS DAN PENGUJIAN SISTEM

Pada tahap analisis dan perancangan sistem enkripsi dan deskripsi *backup* data pengadaan yang diimplementasikan pada LPSE Universitas Udayana tentunya terdapat beberapa tahapan yang membuat nantinya sistem tersebut dapat berjalan sesuai dengan harapan yang direncanakan. Adapun tahapan-tahapan pada bagian analisis dan perancangan sistem adalah sebagai berikut :

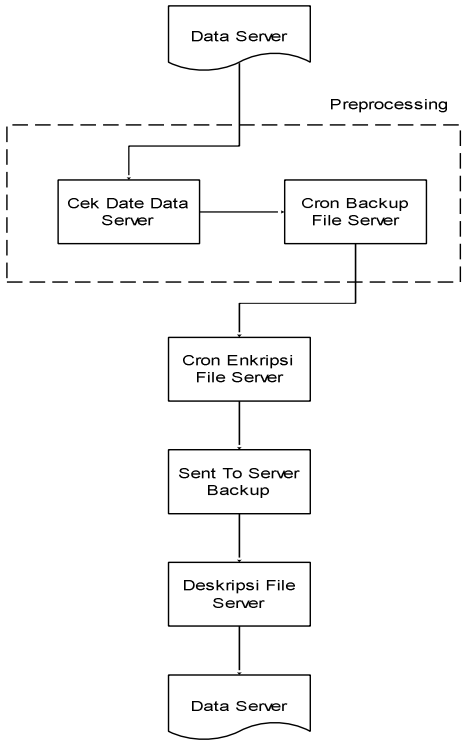
A. Analisis Kebutuhan

Untuk mewujudkan sistem palayanan berbasis *web* yang memiliki nilai *avaibility* tinggi, data yang ada pada *server* utama tentunya perlu direplikasi secara berkala pada *server backup*, dengan tentunya mengutamakan keamanan data saat terjadinya proses *backup* melalui jaringan LAN. Untuk mewujudkan hal tersebut tentunya diperlukan suatu proses analisis pendahulu, sehingga nantinya mekanisme tersebut dapat diterapkan dengan baik pada sistem informasi yang sudah ada sebelumnya. Dimana proses analisi ini akan dibagi menjadi dua bagian yaitu *baselining* dan *needs analysis*.

Dari sisi *baselining* layanan *web* LPSE sudah memiliki sistem *backup*. Dimana sistem *backup* tersebut merupakan layanan cadangan yang disiapkan untuk *server* utama LPSE jika sewaktu-waktu terjadi masalah terhadap layanan utama LPSE. Pada eksistensinya untuk melakukan pengamanan data pengadaan yang barang dan jasa yang berlangsung telah dilakukan mekanisme *backup* ataupun replikasi secara berkala sistem utama LPSE. Sehingga mekanisme tersebut akan dapat meningkatkan *avaibility* serta kesetersediaan data layanan LPSE. Dari sisi *needs analysis* mekanisme *backup* ataupun replikasi tersebut menggunakan jaringan LAN yang secara tidak langsung data yang sedang berjalan dapat disadap ataupun dimanipulasi oleh orang-orang yang tidak berkepentingan. Untuk mengamankan mekanisme tersebut makan sebelum dilakukan proses *backup* ataupun repilkasi data-data tersebut akan dienkripsi terlebih dahulu sehingga hal-hal yang berupa kejahatan dalam jaringan LAN dapat diminimalisir.

B. Mekanisme Pengamanan Backup File LPSE

Kriptografi merupakan ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Dalam proses enkripsi file *backup* LPSE ini akan menggunakan algoritma DES dan AES. Berikut adalah arsitektur dari sistem pengamanan *backup* file LPSE yang diimplementasikan pada penelitian ini.



Gambar. 2. Block Diagram Sistem Pengamanan File Backup LPSE.

Gambar 2 merupakan gambaran umum dari sistem yang dibangun, dimana secara garis besar proses pengamanan file *backup* LPSE akan dibagi menjadi beberapa sub bagian. Proses utama yang terjadi dalam mekanisme ini adalah data pada *server* utama LPSE akan dilakukan proses *backup* otomatis menggunakan mekanisme *cron* berdasarkan *date* dari file LPSE. Proses *backup* ini hanya berlangsung pada *server* utama LPSE, ketika data tersebut telah berhasil dilakukan proses *cron backup* pada *server* utama, maka data tersebut akan di enkripsi untuk meningkatkan keamanan data. Setelah terenkripsi lalu data tersebut akan di transfer menuju ke *server backup* melalui jaringan LAN. Ketika data sudah berhasi sampai pada *server backup*,kemudian data tersebut akan di deskripsi untuk mendapatkan data yang dapat dibaca atau data yang tidak terenkripsi. Setelah semua proses tersebut berjalan dengan baik maka semua proses pengamanan file *backup* LPSE telah berhasil dilakukan.

C. Implementasi Sistem Pengamanan

Untuk membangun sistem pengamanan file *backup* LPSE dibutuhkan beberapa komponen utama. Agar sistem *backup*

dan pengamanan baik enkripsi maupun deskripsi file berjalan secara otomatis, maka diperlukan suatu mekanisme *cron* yang ditanamkan pada *server* utama maupun *server backup*. Diamana sistem *cron* tersebut akan membangun penjadwalan perintah agar *server* utama melakukan proses *backup*, enkripsi file dan mentransfer data hasil enkripsi menuju ke *server backup* secara berkala. Pada *server backup* tentunya perlu juga ditanamkan sistem *cron*, dimana sistem tersebut nantinya akan membuat penjadwalan untuk melakukan deskripsi file yang diterima dari *server* utama. *Service cron* tersebut sebenarnya sudah terdapat pada sistem operasi linux pada *server* itu sendiri. Disini tinggal membuat penjadwalan terhadap pekerjaan-pekerjaan yang harus dikerjakan oleh sistem.

Ketika skenario penjadwalan sudah disiapkan, maka langkah selanjutnya adalah meyiapkan aplikasi enkripsi dan deskripsi yang diimplementasikan menggunakan metode DES dan AES-256. Dalam implementasinya sistem pengamanan ini akan dikembangkan menggunakan bahasa C++. Bahasa ini digunakan karena bahasa ini sangat kompatibel dengan perintah-perintah pada terminal linux dan karena berjalan berbasis terminal, aplikasi ini tentunya tidak akan memberatkan kinerja dari sistem pelayanan LPSE berbasis *web*. Karena pada intinya *server* yang digunakan akan berfokus pada penyediaan layanan, bukan melakukan operasi-operasi lain yang dapat membebani kinerja *server*. Untuk aplikasi enkripsi akan ditanamkan pada *server* utama, karena pada server utama akan berlangsung proses penyamaran data sebelum dikirimkan menuju *server backup*. Sedangkan aplikasi deskripsi akan ditanamkan pada *server backup*, karena *server* tersebut akan bertugas menerima data yang dikirim dalam bentuk yang tidak bisa terbaca. Untuk dapat membaca file yang dikirim maka pada *server backup* tersebut akan dilakukan proses deskripsi sehingga data yang diterima dapat dibaca untuk menampilkan info layanan pengadaan.

D. Pengujian Sistem

Dalam penelitan ini terdapat empat jenis pengujian yang dilakukan, dimana jenis–jenis pengujian tersebut adalah pengujian *black box*, pengujian waktu enkripsi dan deskripsi serta pengujian waktu pengiriman file. Untuk lebih jelasnya mengenai jenis–jenis desain pengujian tersebut akan dibahas lebih lengkap pada pembahasan di bawah :

- Pengujian *black box* yang digunakan dalam penelitian ini adalah pengujian *input* dan *output* dari sistem pengamanan. Proses pengujian *input* dilakukan dengan memasukkan *key* berupa susunan teks untuk melakukan proses deskripsi dan enkripsi file. Selanjutnya akan dilihat apakah *key* yang dimasukkan tersebut telah mampu melakukan proses enkripsi dan deskripsi file. Sedangkan pengujian *output* dilakukan dengan melihat apakah file terenkripsi sudah tidak dapat terbaca dan file yang dideskripsi sudah dapat dibaca sesuai dengan file sebelum dienkripsi.
- Pengujian ukuran file setelah terenkripsi digunakan untuk mengetahui berapa besar perbedaan ukuran file saat setelah terenkripsi dan sebelum terenkripsi baik menggunakan metode DES maupun AES.
- Pengujian *waktu* proses enkripsi dan deskripsi yang merupakan pengujian yang dilakukan untuk mengetahui waktu yang dibutuhkan oleh metode pengamanan file untuk melakukan proses enkripsi maupun deskripsi file.

Pengujian waktu proses *send file* merupakan proses yang berguna untuk melihat atau mengetahui waktu yang diperlukan oleh file terenkripsi untuk sampai pada *server* tujuan. Dimana waktu tempuh tersebut akan dibandingkan dengan waktu tempuh file tanpa enkripsi

IV. HASIL PENGUJIAN

Hasil dari setiap jenis pengujian sistem ini tentunya akan menghasilkan sebuah informasi yang sangat dibutuhkan untuk mengevaluasi mekanisme pengamanan file tersebut. Adapun hasil dari setiap jenis pengujian yang telah dilakukan adalah :

A. Pengujian Black Box

Dari hasil pengujian *black box* yang telah dilakukan dalam penelitian ini sistem pengamanan file *backup* LPSE memenuhi harapan *output* yang diharapkan pada saat melakukan pengujian. Dimana ketika dilakukan proses enkripsi dengan metode yang telah ditentukan, file yang dienkripsi tidak lagi dapat dibaca ataupun dibuka. Sehingga hal ini sangat sesuai dengan konsep awal tujuan dikembangkannya sistem pengamanan file *backup* LPSE. Dimana dengan file yang tidak dapat dibaca ataupun dibuka tersebut, tentunya akan membuat mekanisme transfer file dari *server* utama menuju ke *server backup* akan menjadi lebih aman atau dengan kata lain file tersebut tidak akan dapat dimanipulasi ataupun disadap oleh orang-orang yang tidak berkepentingan. Ketika file terenkripsi tersebut telah sampai pada *server backup*, maka akan dilakukan pengujian *black box* lagi dengan melakukan proses deskripsi file dengan menggunakan *key* yang sudah didefinisikan pada pengujian *input*. Dari hasil pengujian setelah dilakukan proses deskripsi file yang pada awalnya tidak dapat dibaca telah dapat dibaca dan dibuka.

B. Pengujian Ukuran File Hasil Enkripsi

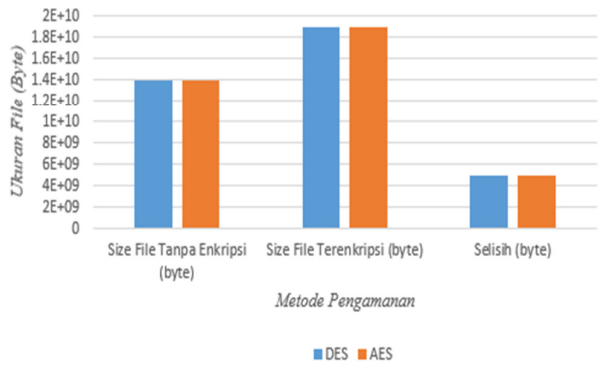
Dalam pengujian ini akan dilihat perbedaan ukuran file *backup* sebelum dan sesudah dienkripsi. Pada tahap ini pengujian akan dibagi menjadi dua sesi, dimana sesi pertama file *backup* akan dienkripsi menggunakan algoritma DES, nantinya akan dicari selisih antara ukuran file yang telah terenkripsi dan file *backup* yang belum terenkripsi. Pada sesi kedua proses enkripsi akan dilakukan menggunakan algoritma AES, dimana sama seperti sesi pertama hasil file terenkripsi akan dicari selisihnya terhadap file *backup* yang belum terenkripsi. Hasil dari pengujian dengan menggunakan kedua algoritma tersebut akan disajikan penulis pada tabel 1 :

TABEL I. UKURAN FILE TERENKRIPSI

Metode	***Ukuran File Tanpa Enkripsi (byte)***	***Ukuran File Terenkripsi (byte)***	***Selisih (byte)***

Metode	*Ukuran File Tanpa Enkripsi (byte)*	*Ukuran File Terenkripsi (byte)*	*Selisih (byte)*
DES	14.012.883.780	18.975.780.148	4.962.896.368
AES	14.012.883.780	18.975.780.160	4.962.896.380

Sesuai dengan tabel 1, terdapat perbedaan ukuran file hasil enkripsi oleh masing-masing metode, baik menggunakan metode DES maupun metode AES. Gambar 3 di bawah merupakan representasi perbandingan perbedaan ukuran file dari penggunaan masing-masing metode :



Gambar. 3.Grafik Perbandingan Ukuran Size File Enkripsi

Dari hasil pengujian yang telah dilakukan oleh penulis, dengan menggunakan algoritma DES ukuran file *backup* yang awalnya sebesar 14.012.883.780 *byte* bertambah menjadi 18.975.780.148 *byte*, atau terdapat perbedaan sebesar 4.962.896.368 *byte* antara file yang terenkripsi dan file yang belum terenkripsi. Sedangkan dengan menggunakan algoritma AES file hasil enkripsi juga mengalami peningkatan volume sebesar 4.962.896.380 *byte* sehingga file *backup* menjadi 18.975.780.160 *byte*.

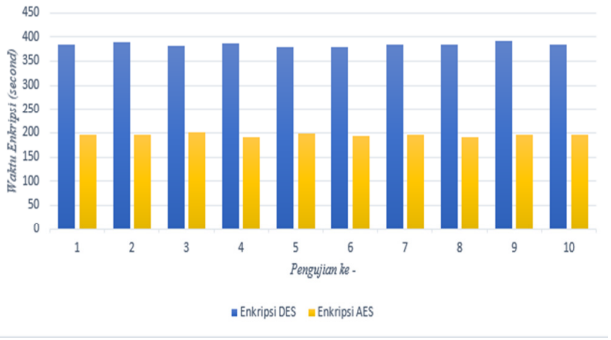
C. Pengujian Waktu Proses Enkripsi Dan Deskripsi

Dalam pengujian ini akan dihitung waktu yang dibutuhkan oleh masing metode pengamanan file dalam melakukan proses enkripsi dan deskripsi. Dimana pada pengujian pertama akan dilakukan pengujian waktu yang dibutuhkan oleh metode DES dan AES untuk melakukan proses enkripsi dan seskripsi file *backup* LPSE. Tabel 2 adalah hasil pengujian waktu yang dibutuhkan oleh masing-masing metode dalam melakukan enkripsi dan deskripsi file :

TABEL II. WAKTU PROSES ENKRIPSI & DESKRIPSI FILE

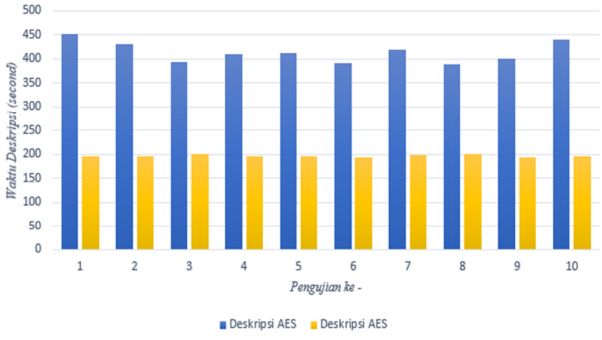
Pengujian ke-	*DES*		*AES*	
	Enkripsi (second)	*Deskripsi (second)*	*Enkripsi (second)*	*Deskripsi (second)*
1	384	452	197	195
2	390	430	195	197
3	382	394	200	201
4	388	410	190	195
5	380	412	198	196
6	378	392	194	194
7	384	420	195	198
8	384	390	191	200
9	391	401	197	194
10	384	441	197	195
Rata - Rata	384,5	414,2	195,4	196,5

Sesuai dengan tabel 2, terdapat perbedaan waktu yang digunakan oleh masing-masing metode dalam melakukan enkripsi dan deskripsi file *backup* LPSE. Gambar 4 adalah hasil pengujian waktu enkripsi file dari masing-masing metode :



Gambar. 4.Grafik Pengujian Waktu Proses Enkripsi

Berdasarkan grafik pada gambar 4, terlihat bahwa penggunaan metode AES membutuhkan waktu enkripsi yang lebih rendah dibandingan metode DES dengan studi kasus besar file yang sama. Dimana jika dirata-ratakan waktu yang diperlukan oleh metode AES untuk melakukan proses enkripsi adalah sebesar 195,4 detik, sedangkan metode DES membutuhkan waktu sebesar 384,5 detik. Dimana terdapat selisih sebesar 189,1 detik untuk melakukan proses enkripsi antara ketuda metode tersebut samapai file tersebut terenkripsi.



Gambar. 5.Grafik Pengujian Waktu Proses Deskripsi

Seperti terlihat pada gambar 5, penggunaan metode AES membutuhkan waktu enkripsi yang lebih rendah dibandingan metode DES dengan studi kasus besar file yang sama. Dimana jika dirata-ratakan waktu yang diperlukan oleh metode AES untuk melakukan proses deskripsi adalah sebesar 196,5 detik, sedangkan metode DES membutuhkan waktu sebesar 414,2 detik. Dimana terdapat selisih sebesar 217,7 detik untuk melakukan proses deskripsi antara ketuda metode tersebut samapai file tersebut dapat dibaca kembali.

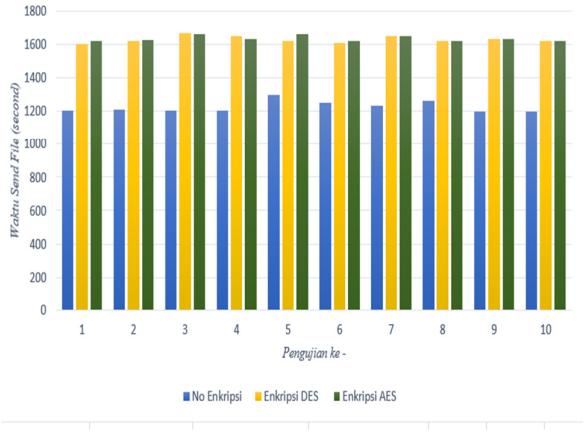
D. Pengujian Waktu Send File

Pada pengujian ini dilakukan untuk mengetahui berapa lama waktu yang dibutuhkan dalam proses *backup* file LPSE. Dimana dalam pengujian ini proses pengiriman file akan dilakukan menggunakan jaringan LAN. Pada proses akan dilihat bagaimana perbedaan waktu yang dibutuhkan dalam proses transfer file antara file tanpa enkripsi, file dengan enkripsi DES dan file dengan enkripsi AES. Tabel 3 merupakan hasil pengujian dari proses transfer file tersebut :

TABEL III. WAKTU SEND FILE

Pengujian ke-	***Waktu Send File (second)***		
	No Enkripsi	***Enkripsi DES***	***Enkripsi AES***
1	1203	1601	1622
2	1210	1622	1627
3	1205	1667	1660
4	1203	1650	1635
5	1300	1624	1660
6	1250	1609	1619
7	1232	1650	1652
8	1261	1619	1620
9	1201	1630	1630
10	1200	1620	1622
Rata - Rata	1226,5	1629,2	1634,7

Sesuai dengan tabel 3 di atas tentunya waktu yang dibutuhkan dalam melakukan pengiriman file yang terenkripsi dengan menggunakan metode DES, AES dan tanpa enkripsi akan menimbulkan ambang waktu yang berbeda. Dimana jika dilihat secara rata-rata pengiriman file tanpa proses enkripsi akan membutuhkan waktu yang paling minimum dengan 1226,5 detik disusul oleh penggunaan metode DES sebesar 1629,2 detik dan metode AES sebesar 1634,7 detik. Untuk mempermudah pengamatan hasil pengujian tersebut, gambar 6 adalah grafik pengujian waktu pengiriman file :



Gambar. 6.Grafik Waktu Pengiriman FIle

Berdasarkan grafik pada gambar 6 dapat dilihat bahwa waktu yang dibutuhkan oleh algoritma DES dan AES dalam melakukan pengiriman file tidak memiliki perbedaan waktu yang signifikan. Hal ini dikarenakan karena file hasil enkripsi yang dihasilkan dari kedua metode tersebut juga tidak memiliki *size* yang jauh berbeda. Dalam pengujian ini waktu yang diperoleh tersebut juga akan sangat mungkin berubah sesuai dengan penggunaan jaringan secara keseluruhan. Untuk meminimalisir hal tersebut, proses pengujian ini dilakukan pada dini hari disaat pengunaan jaringan pada ambang batas minimum dengan amsumsi untuk mendapatkan hasil pengujian yang stabil.

E. Analisa Keseluruhan

Dalam penelitian ini, sistem pengamanan file *backup* LPSE telah berhasil diimplementasikan sehingga file yang melewati jaringan LAN tidak dapat lagi dibaca oleh orang yang tidak berkepentingan. Hal ini tentunya akan sangat berguna untuk menjaga keamanan data layanan pengadaan barang dan jasa yang sedang maupun yang telah berlangsung. Ketika berbicara performansi, tentunya banyak hal yang harus dipertimbangkan baik dari keamanan data maupun efisisensi dan efektifitas dari penerapan mekanisme tersebut. Hasil dari penerapan mekanisme ini haruslah membuat data yang melewati jaringan LAN bersifat aman namun proses pengaman yang dilakukan tidak akan membebani kinerja perangkat yang ada, karena ketika seseorang ingin mengamankan data, layanan utama yang disediakan dalam hal ini layanan pengadaan barang dan jasa berbasis *web* tidak boleh terganggu kinerjanya. Dengan pertimbangan tersebut pengujian penggunaan kedua metode tersebut tentunya dapat digunakan referensi metode apa yang tepat digunakan dalam kasus ini. Dalam melakukan pengujian sistem berbasis *black box,* algoritma DES dan AES telah mampu melakukan pengamanan file LPSE. Selain itu masih dari pengujian *black box* sistem yang dikembangan dengan algoritma DES dan AES juga telah mampu mengembalikan file tersebut ke bentuk semula melaui proses deskripsi. Hasil file yang dienkripsi menggunakan kedua metode tersebut tidak memiliki perbedaan yang signifikan yaitu ketika menggunakan algoritma DES file yang dienkripsi menjadi sebesar 18.975.780.148 *byte* dan ketika menggunakan algoritma AES file yang dienkripsi menjadi sebesar 18.975.780.160 *byte,*

hanya berselisih 12 *byte* dari penggunaan kedua metode tersebut.

Ketika berbicara waktu yang diperlukan oleh algoritma DES dan AES untuk melakukan enkripsi dan deskripsi tentunya secara garis besar algoritma AES memiliki rentang waktu yang lebih cepat dibandingka metode DES dalam melakukan kedua proses tersebut dengan ukuran file sumber yang sama. Dimana metode AES hanya memerlukan waktu rata-rata sekitar 195,4 detik untuk melakukan proses enkripsi dan sekitar 196,5 detik untuk melakukan proses deskripsi. Sedangkan algoritma DES membutuhkan waktu yang lebih lama atau rata-rata sekitar 384,5 detik untuk melakukan proses enkripsi dan sekitar 414,2 detik untuk melakukan proses deskripsi. Hal ini dikarenakan proses pendeskripsian file menggunakan metode DES memerlukan proses yang lebih komplek daripada metode AES.

Pada proses pengiriman file hasil enkripsi dari *server* utama menuju *server backup* atara kedua metode yang diterapkan tidak memiliki perbedaan waktu yang signifikan, hal ini dikarenakan ukuran file enkripsi yang dihasilkan oleh algoritma DES dan AES tidak memiliki perbedaan yang besar. Selain itu waktu pengiriman file sangat dipengaruhi oleh kepadatan jaringan saat proses tersebut. Dalam pengujian ini untuk mendapatkan hasil yang konstan, proses pengiriman dilakukan dini hari dengan asumsi kepadatan jaringan yang rendah. Dimana hasil pengujian tersebut untuk file enkripsi dengan algoritma DES membutuhkan waktu rata-rata sebesar 1629,2 detik dan AES membutuhkan waktu rata-rata sebesar 1634,7 detik.

V. KESIMPULAN

Berdasarkan pada pengujian yang telah dilakukan maka dapat diambil kesimpulan bahwa mekanisme pengamanan yang dilakukan menggunakan algoritma DES dan AES telah mampu memberikan keamanan terhadap file *backup* LPSE yang melewati jaringan LAN. Perbedaannya adalah pada performansi penerapan kedua metode tersebut, metode AES lebih tepat diterapkan karena membutuhkan waktu enkripsi dan deskripsi *file* yang lebih rendah dari motode DES dengan selisih rata-rara waktu enkripsi sebesar 189,1 detik dan 217,7 detik untuk proses deskripsi. Hal lain yang mendukung penerapan algoritma AES dalam kasus ini adalah file enkripsi yang dihasilkan tidak jauh berbeda dengan algoritma DES, sehingga secara tidak langsung waktu yang dibutuhkan dalam proses *backup* juga *relative* sama.

UCAPAN TERIMA KASIH

Karya ini didukung oleh LPSE Universitas Udayana sebagai penyedia data dan perangkat dalam melakukan penelitian.

REFERENSI

[1] "LPSE LKPP." [Online]. Available: https://lpse.lkpp.go.id/eproc/tentangkami. [Accessed: 10-May-2016].

[2] K. Ashadi, M. Yuliana, and M. Z. S. Hadi, "Analisa Dan Implementasi Sistem Keamanan Data Dengan Menggunakan Metode Enkripsi Algoritma Rc-5," *PENS-ITS*, 2011.

[3] A. Zelvina, S. Effendi, and D. Arisandi, "Perancangan Aplikasi Pembelajaran Kriptografi Kunci Publik ElGamal Untuk Mahasiswa," *Dunia Teknol. Inf.-J. Online*, vol. 1, no. 1, 2012.

[4] A. R. Alvianto and D. Darmaji, "Pengaman Pengiriman Pesan Via SMS dengan Algoritma RSA Berbasis Android," *J. Sains Dan Seni ITS*, vol. 4, no. 1, pp. A1–A6, 2015.

[5] C. H. Kim, "Differential Fault Analysis against AES-192 and AES-256 with Minimal Faults," in *2010 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, 2010, pp. 3–9.

[6] A. K. Wijaya and M. Martinus, "Rancang Bangun Aplikasi Enkripsi dan Dekripsi Berbasis Android dengan Menggunakan Algoritma Hybrid DES dan Elgamal," 2013.

[7] I. P. Herryawan, "Analisa Dan Penerapan Algoritma Des Untuk Pengamanan Data Gambar Dan Video," *J. Ilmu Komput.*, vol. 4, no. 1, 2011.

[8] V. Lusiana, "Implementasi Kriptografi pada File Dokumen Menggunakan Algoritma AES-128," *J. Din. Inform.*, vol. 3, no. 2, 2011.