PENDEKATAN KEAMANAN SERTA KECEPATAN AKSES DATA PADA *CLOUD* DENGAN ALGORITMA *HUFFMAN* DAN AES

Wahyu Eko Susanto
Program Studi Manajemen Informatika
AMIK BSI Yogyakarta
Jl Ringroad Barat, Ambarketawang, Gamping , Sleman, Yogyakarta
(0274)4342536
e-mail :wahyu.wes@bsi.ac.id

ABSTRAK

Dalam semua sistem informasi, lalulintas data menjadi faktor penting.Sehingga dibutuhkan upaya bagaimana menjaga data agar dapat dijamin keamanannya sehingga kita mampu mendapatkan *Confidentiality, Authorization, Authentication, Accountability, Integrity* dari data tersebut. Dan apabila kita menggunakan *cloud* maka tidak hanya keamanan data saja namun juga bagaimana kita dapat mengkomunikasikan data ini dengan cepat dan ringan tanpa harus membebani *bandwidth* secara signifikan, keadaan ini berbanding urus dengan besar kecilnya data dan intensitas komunikasi data itu sendiri. Dalam Makalah ini metode yang penulis menggunakan metode penelitian *development research.* Dari masalah yang diatas, maka diperlukan perpaduan yang pas antara bagaimana kita mengkombinasikan algoritma-algoritma kompresi untuk memperkecil data yang akan di transmisikan dan algoritma enkripsi sebagai pelindung data agar dapat terjamin keamanannya baik ketika di transmisikan maupun ketika di simpan di *cloud storage*. Salah satu diantara algoritma-algoritma tersebut yang mempunyai kinerja terbaik menurut makalah ini adalah algoritma kompresi *Huffman* dan algoritma enkripsi AES dimana kedua algoritma ini apabila kita kombinasikan diharapkan dapat menghasilkan data dengan *byte* yang lebih kecil serta lebih aman ketika ditransfer ke *cloud* maupun ketika berada di *cloude storage*.

Keywords *:Cloud, Algoritma AES, Algoritma Huffman*

I. Pendahuluan

Pembangunan sebuah sistem yang terkomputerisasi menjadi sebuah kebutuhan yang peting bagi eksistensi sebuah perusahaan namun pembangunan sistem yang terkomputerisasi membutuhkan dana dan sumber daya yang tidak sedikit baik untuk pembangunan infrastrukturnya, pengelolaannya maupun SDM yang harus menanganinya sehingga mengakibatkan perusahaan harus berkonsentrasi pada pengembangan sistemnya selain harus berkonsentrasi pula dalam pengembangan bisnisnya.

Namun semua itu dapat di atasi dengan hadirnya *Cloud Computing*, *Cloud Computing* memberikan sebuah solusi bagi perusahaan yang ingin mengembangkan atau membangun sistem yang terkomputerisasi tanpa harus memikirkan bagaimana membangun dan mengelola sistem itu sehingga perusahaan dapat lebih berkonsentrasi pada bisnisnya. Dengan menggunakan *cloud* pengeluaran untuk membangun sistem juga menjadi lebih murah karena *cloud user* tidak perlu menyediakan semua infrastruktur untuk membangun sistem tersebut karena telah di sediakan oleh *cloud vendor*.

Walaupun penggunaan *cloud computing* dalam pembangunan sebuah sistem yang terkomputerisasi menjadi lebih murah namun pada kenyataannya tidak seperti itu karena *cloud user* harus membangun infrastruktur untuk koneksi dengan *cloud* yang baik agar sistem *cloud* dapat berjalan dengan baik, dalam hal ini besaran *bandwidth*akan sangat berpengaruh terhadap kinerja sistem. Semakin besar atau semakin banyak data yang di transfer maka akan semakin besar pula *bandwidth* yang diperlukan. Ironisnya di Indonesia menurut survey dilakukan oleh ESCAP (*Economic and Social Commission for Asia and the Pacific*)pada bulan Agustus 2013menunjukkan bahwa Indonesia dalam infrastruktur *bandwidth*nya masih rendah di bandignkan dengan negara ASEAN lainnya.

Selain masalah besarnya *bandwidth* yang diperlukan masalah keamanan juga menjadi isu utama dalam penggunaan *cloud computing*, Dengan adanya hal ini dirasa perlu untuk membuat sebuah solusi agar data yang dikirim menjadi lebih kecil sehingga tidak membutuhkan *bandwidth* yang terlalu besar namun data tetap aman. Dengan demikian biaya untuk menyediakan *bandwidth* dapat diminimalkan.

Masalah keamanan *cloud computing* masih menjadi kendala dalam upaya membangun kepercayaan agar *user* mau menggunakna *cloud*selain

itu kebutuhan *bandwidth* juga menjadi kendala untuk penerapan *cloud* dalam sistem. Oleh karena itu pada tesis ini di lakukan pengabungan antara kompresi file dan enkripsi file yang berbasis teks untuk tetap menjaga keamanan data saat di transfer maupun saat berada di *storage* sekaligus mengecilkan ukuran file sehingga dapat meminimalisir penggunaan *bandwidth* ketika di transfer dan menghemat ruang penyimpanan pada *cloud storage*.

Pada makalah ini akan di buat kombinasi antara kompresi file menggunakan algoritma *Huffman* dan enkripsi file menggunakan algoritma AES, agar enkripsi lebih cepat dilakukan dan file yang dikirim menjadi lebih ringan sehingga meminimalkan penggunaan ruang pada *cloud storage* dan mengurangi kebutuhan *bandwidth* untuk transfer data.

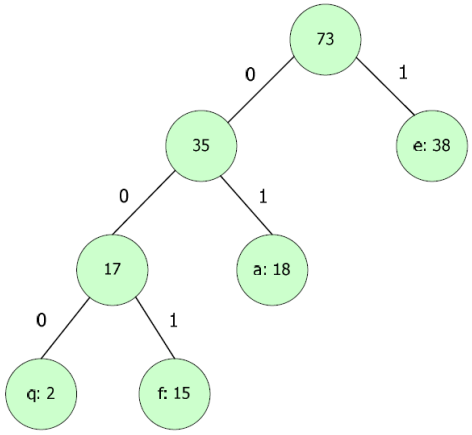
II. Tinjauan pustaka

2.1. Algoritma *Huffman.*

Algoritma *Huffman*, yang dibuat oleh seorang mahasiswa MIT bernama David *Huffman*, merupakan salah satu metode paling lama dan paling terkenal dalam kompresi teks.

Huffman encoding adalah sebuah teknik kompresi dokumen yang menggunakan jumlah kemunculan relatif simbol-simbol karakter pada dokumen teks untuk menghasilkan representasi biner dengan panjang tertentu untuk tiap karakter.Representasi biner ini menjadi kode *Huffman*untuk sebuah karakter. Proses *encoding* memiliki karakteristik bahwa tidak ada kode untuk sebuah karakter yang diawali oleh kode karakter lain. Pada umumnya, kode *Huffman*direpresentasikan dalam bentuk pohon biner *Huffman*(“0” merepsentasikan cabang kiri, dan “1” merepresentasikan cabang kanan).

Berikut ini contoh gambar algoritma *huffman*



Sumber :(Agung, 2013)

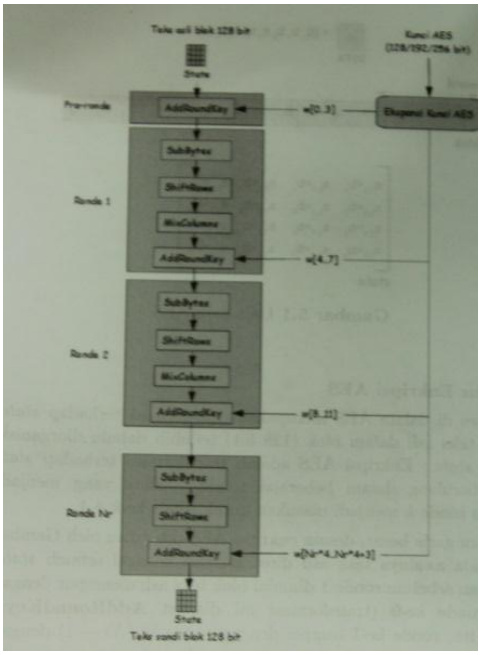
Gambar 1. Contoh Pohon *Huffman*

2.2. Algoritma AES

Algoritma AES (*Advanced Encritpion Standard*) dipublikasikan oleh NIST (*National Institute of Standard and Technology*) pada tahun 2000 yang digunakan untuk menggantikan algoritma DES yang semakin lama semakin mudah untuk membobol kuncinya. NIST memberikan spesifikasi AES yaitu harus memiliki panjang blok 128 bit dan mampu mendukung panjang kunci 128, 192 dan 256. Dari beberapa algoritma yang di seleksi NIST memilih Sistem Penyandian Rijndael yang di kembangkan oleh Joan Daemen dan Vincent sebagai penyandian AES yang di dasarkan pada kriteria(Sadikin, 2013, p. 151):

1. Keamanan
   Tahan terhadap serangan *brute force*
2. Biaya
   Memiliki biaya komputasi dan memori yang efisien agar dapat diimplementasikan pada perangkat keras maupun lunak
3. Karakteristik algoritma dan implementasi
   System penyandian harus bersifat terbuka, fleksibel, dan sederhana.

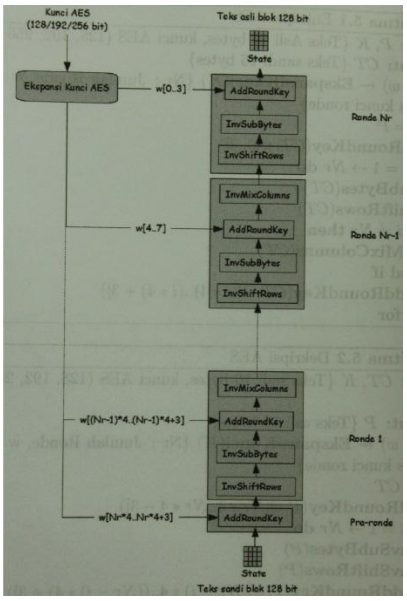
Adapun susunan struktur enkripsi dan dekripsi yang dimiliki oleh AES sebagai berikut



Sumber: (Sadikin, 2013, p. 154)

Gambar 2. Struktur enkripsi AES

Adapun susunan dekripsi dari Algoritma AES ini adalah Sebagai berikut.



Sumber :(Sadikin, 2013, p. 156)

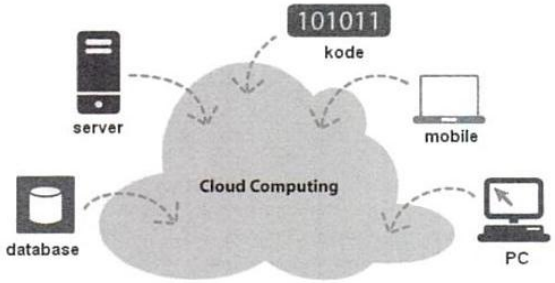
Gambar 3. Struktur enkripsi AES

2.3. *Cloud*

Dalam makalah ini *Cloud* di artikan sebagai *Internet.Cloud computing* menurut (Enterprise, 2010, p. 1)adalah " suatu bentuk evolusi lanjutan dari Internet yang menggabungkan pemanfaatan teknologi komputer dan pengembangan berbasis internet". Merujuk dari pernyataan menurut Jubilee Enterprice diatas dapat kita simpulkan bahwa *cloud computing* ini memanfaatkan sumberdaya komputer dimana layanannya tersedia secara *online*.Beberapa komponen untuk dapat menggunakan *Cloud computing* antara lain (Enterprise, 2010) :

1. *Cloud Client.*
2. *Cloud Services.*
3. *Cloud Application.*
4. *Cloud Platform.*
5. *Cloud Storage.*
6. *Cloud Infrastructure*.

Dari ke enam komponen diatas yang masih menjadi kendala utama bagi *user* untuk menggunakan *cloud computing* ialah pada *cloud storage*. "*Cloud storage is a model of networked online storage where data is stored on multiple virtual servers, generally hosted by third parties, rather than being hosted on dedicated servers"*(Balbudhe & Balbudhe, 2013, p. 83). adalah model penyimpanan *online* jaringan dimana data disimpan pada beberapa *server* virtual, umumnya diselenggarakan oleh pihak ketiga, bukannya *host* di *dedicated server*.Karena pada sisi ini data dari pemilik ada pada pihak ke tiga sehingga di perlukan enkripsi data untuk dapat menjamin bahwa data tersebut tidak dilihat oleh penyedia *cloud storage*.



Sumber: (Enterprise, 2010, p. 2)

Gambar 4. Ilustrasi *Cloud Computing*

Cloud computing dapat dikategorikan ke dalam tiga model layanan (Leena, 2012, p. 544)

1. *Software as a Service (SaaS)*. Pengguna hanya dapat mengakses aplikasi yang berjalan di *cloud*. Aplikasi ini dapat diakses melalui berbagai antarmuka klien seperti web browser. Dalam layanan ini pengguna tidak memiliki akses kontrol manajemen untuk dapat mengelola atau mengendalikan infrastruktur dasar seperti jaringan, server, sistem operasi, penyimpanan atau kemampuan lainnya. Pengguna memiliki beberapa konfigurasipengguna tertentu untuk pengaturan terhadap aplikasi.
2. *Platform as a Service (PaaS)*. Salah satu fasilitas yang diberikan kepada pengguna adalah untuk menempatkan salah satu aplikasi pada infrastruktur yang akan dibuat dengan menggunakan bahasa pemrograman dan alat yang didukung oleh pengguna. Dalam hal ini pengguna tidak dapat mengelola atau mengendalikan infrastruktur dasar seperti jaringan, server sistem operasi, penyimpanan tetapi pada saat yang sama memiliki kontrol atas aplikasi yang digunakan dan memungkinkan melakukan konfigurasi aplikasi.
3. *Infrastructure as a Service (IaaS)*. Dalam satu fungsi ini yang diberikan kepada pengguna yaitu penyimpanan, jaringan dan sumber daya komputasi penting lainnya dimana pengguna dapat memasang dan menjalankan perangkat lunak secara acak yang dapat digunakan oleh

beberapa aplikasi atau sistem operasi. Dalam hal ini pengguna memiliki kontrol atas sistem operasi, aplikasi yang digunakan, penyimpanan dan kontrol yang dimilikinya terbatas pada komponen jaringan seperti *firewall* dll.

III. Tinjauan Studi

Shashi Mehrotra Seth dan Rajan Mishra melakukan penelitian dalam jurnalnya "*Comparative Analysis Of Encryption Algorithms For Data Communication"*untuk mengkomparasikan algoritma DES, AES dan RSA agar diketahui algoritma Mana yang paling efektif dari 3 algoritma yang di bandingkan.Tujuan dari dilakukannya komparasi ketiga algoritma ini karena penggunaan Algoritma enkripsi ternyata memakan sumber daya yang ada komputer yang cukup signifikan seperti waktu pemrosesan, memori, dan penggunaan daya.Alasan inilah yang mendasari Shashi Mehrotra Seth dan Rajan Mishra melakukan penelitian dengan melakukan Perbandingan antara DES, AES dan RSA dengan pertimbangan waktu pemrosesan, penggunaan memori dan *byte* keluaran.

Pemilihan penggunaan enkripsi dalam menjaga keamanan data yang terbaik dengan mempertimbangkan faktor waktu pemrosesan, memori, dan kinerja CPU untuk mendapatkan algotirma terbaik.Dari Percobaan yang telah di lakukan pada enkripsi file teks dengan 4 file size yang berbeda menunjukkan hasil waktupemrosesan pada Algoritma DES paling cepat kemudian AES dan RSA yang paling lama, perbedaan waktu antara DES dan AES ± 0,2 sec sedangkan DES dengan RSA ± 8 sec. Sedangkan pengujian untuk penggunaan memori, Algoritma AES paling sedikit, kemudian algoritma DES yang paling banyak RSA, dimana perbedaan antara AES dan DES ±4 KB, sedangkan dengan RSA ±10 KB. Dan hasil akhir byte Keluaran Algoritma RSA paling kecil pada angka 63,536 byte ,sedang DES dan AES sama yaitu 131,072 byte. (Seth & Mishra, 2011)

Anurag Porwal, dkk. dalam jurnalnya "*An Approach For Secure Data Transmission In Private Cloude*" menemukan sebuah permasalahan untuk komunikasi data pada *cloud*, hal initimbul Karena adanya komunikasi data dari *server* ke klien dan sebaliknya sehingga perlu untuk melindungi data yang di komunikasikan namun tanpa mempengaruhi network layerdan melindungi dari orang yang tidak mempunyai otorisasi untuk memasukkan data ke server. Dari pembahasan jurnal ini mengungkapkanTeknis pokok yang mendukung infrastruktur dan layanan *cloud computing* termasuk virtualisasi, perangkat lunak yang berorientasi layanan, teknologi jaringan komputer, pengelolaan fasilitas yang besar, dan efisiensi daya.Memberikan metode pendekatan untuk melindungi transmisi data yang aman pada cloud.Dari jurnal ini dapat kita simpulkan dengan menggunakan algoritma enkripsi *d*ata akan terlindungi di dalam *server* sesuai dengan pilihan metode pengamanan, sehingga data dapat di berikan tingkat prioritas keamanan.Pendekatan yang di ajukan dalam peper in adalah dengam memberikan enkripsi dengan tanpa menggunakan *SSL* maupun *IPsecurity*. Pendekatan ini efektif karena tidak mengubah implementasi dari IP layer dan dapat melindungi data sejak sebelum proses komunikasi data dilakukan, Serta menambah keamanan data pada saat penyimpanan sehingga user dapat lebih yakin atas keamanan datanya.(Porwal, Maheshwari, Pal, & Kakhani, 2012)

Pradnyes Bhisikardan Prof. Amit Sahu dalam jurnalnya*"Security In Data Storage And Transmission In Cloud Computing"*mengemukakan bahwa ada masalahmengenai menjaga agar data *user* tetap aman pada cloud. Karena data *user*ditransfer dari *Client* ke *server* atau sebaliknya dan ketika data user di bagi dengan pihak ketiga, yaitu penyedia layanan *Cloud*ketika disimpan di *cloudstorage*.Konsep pada jurnal ini lebih menekankan pada bagaiman Menjaga keamanan data saat di transmisikan dan ketika di simpan di *cloud* tanpa mempengaruhi *network layer*.Jaminan keamanan data saat di transmisikan dan ketika disimpan menjadi aspek utama dari kalitas layanan.Meskipun *cloud database* berbasis *online* yang menyediakan ruang penyimpanan yang besar dan sumberdaya yang dapat di sesuaikan dengan kebutuhan namun *user* akan kehilangan kewenagannya terkait integritas data dan ketersediaan datanya .sehingga diperlukan penggunaan teknik pengamanan data baru karena dianggap fasilitas yang sudah ada tidak dapat di pakai dengan alasan ketika itu tetap di gunakan *user* tidak akan mempunyai kontrol atas datanya yang berada di *cloud*. Salah satu caranya dengan meggunakan teknik dengan mengenkripsi data di atas layer transport.Yaitu dengan menerapkan algoritma AES, triple DES dan DES sebelum data di transmisikan.Skema ini efisien terhadap kegagalan Byzantine, serangan untuk memodifikasi data dan bahkan serangan terhadap server secara bersama-sama.(Bhisikar & Sahu, 2013)

Miss A.Kakoli raoLeena, Dalam jurnalnyayang berjudul "*Centralized Database Security In Cloud*" yang membahas mengenai keamanan data pada cloud adapun Latar belakang masalah jurnal membahas Mencari solusi masalah keamanan data dan acses kontrol agar *user* yakin ketika melakukan pengolahan data pribadi dan data rahasia mereka. Dan juga permasalahan kunci keamanan dan pertukarannya.Hipotesis yang akan di uji dalam jurnal ini adlah untuk Memastikan

pertukaran kunci data tetap aman dengan*RSA key Exchange Protocol*.Dari hasil refiew terhadap jurnal ini dapat di tarik kesimpulan bahwa Tujuan dari jurnal ini adalah Agar *user* yakin ketika pengolahan data pribadi dan data rahasia mereka. Sedangkan temuan utamadari jurnal ini yaitu dengan menggunakan protokol *RSA key exchange* antara penyedia layanan cloud dengan user untuk pertukaran kunci yang aman dengan sebuah kunci simetris sebagai jalan keluar dari masalah pendistribusian kunci dan management.Dari pembahasan yang di lakukan yang bias kita dapatkan dari jurnal ini adalah bahwa Fleksibel dan mudah tersedia yang ada dilayanan *cloud* menyimpan masalah mengenai keamanan data untuk dapat berbagi data secara aman, untuk mengatasi ini kita dapat menggunakan pendekatan bebasis otentik daripada menggunakan pendekatan berbasis komunikasi.Dari jurnal ini dapat di tarik kesimpulan bahwa Penggunaan TORDES, RSA dapat meningkatkan keamanan data dengan biaya yang minimal dan usaha yang sedikit.Yang telah di ujiakn Pada pengujian akses data sederhana. (Leena, 2012)

IV. METODE PENELITIAN

Metode pengumpulan data yangdi gunakan dalam penelitian ini adalah melakukan studi literatur dengan pengumpulan data-data dari internet, jurnal dan karya-karya ilmiah lainnya. Metode penelitian pada karya ilmiah.*Development research*atau penelitian pengembangan menjadi metode penelitian dalam makalah ini yang merupakan penelitian berorientasi pada pemecehan masalah praktis.permasalahan yang akan di pecahkan dalam penelitian pengembangan ini adalah bagaimana kita dapat menjamin keamanan data pada *cloud* pada saat di kirimkan maupun ketika berada di *storage* dengan mempertimbangkan ukuran data dankecepatan proses enkripsi. Karya tulis ini terbatas pada gagasan proses pemecahan masalah tidak membahas mengenai implementasi lebih lanjut.

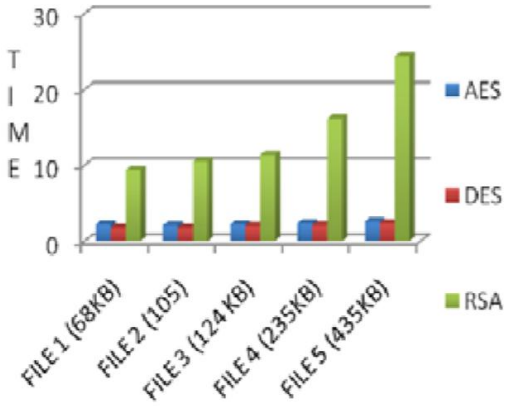
V. HASIL PENELITIAN DAN PEMBAHASAN

5.1. Analisa Komparasi Hasil

5.1.1. Komparasi Algoritma Enkripsi AES, DES dan RSA.

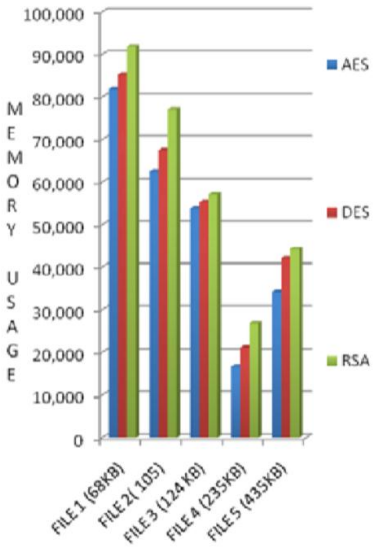
Data yang di transmisikan pada *cloud* haruslah dapat di jamin kemanannya selain dari sisi keamanan size data yang di transmisikan juga haruslah menjadi perhatian penting karena ini berbanding lurus dengan besar *bandwidth* yang akan di gunakan, semakin besar dan semakin sering data tersebut di taransmisikan makan *bandwidth* yang di pakai juga semakin besar.

Ada beberapa pilihan algoritma yang dapat kita gunakan untuk mengamankan data yang kita trnsmisikan ke *cloud* bebrapa diantaranya dengan menggukanan algoritma enkripsi beberap algoritma itu adalah Algoritma AES, DES dan RSA. Namun bebrapa algoritma ter sebut mempunyai bebrapa kelebihan dan kekurangan dalam proses enkripsinya, ini menjadi bahan pertimbangan dalam menggunakan model enkripsi yang tepat utnuk di gunakan. Dari hasil ujicoba yang di lakukan oleh Shashi Mehrotra Seth dan Rajan Mishra, mengenai hasil komparasi dari bererapa algoritma tersebut di tinjau dari waktu pemrosesan, memori yang di gunakan dan byte yang di hasilkan. Berikuti ini data ujicoba komparasi yang di hasilakn dari ketiga algoritma enkripsi tersebut.



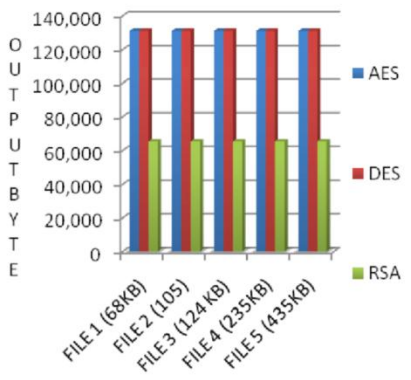
Sumber : (Seth & Mishra, 2011, p. 293)

Gambar 5. Perbandingan waktu komputasi antara AES, DES dan RSA



Sumber : (Seth & Mishra, 2011, p. 293)

Gambar 6. Perbandingan penggunaan memori antara AES, DES dan RSA



Sumber : (Seth & Mishra, 2011, p. 294)

Gambar 7. Perbandingan byte keluaran antara AES, DES dan RSA

Percobaan pada enkripsi file teks dengan 5 file size yang berbeda menghasilkan

a) Waktu pemrosesan : Algoritma DES paling cepat kemudian AES dan RSA yang paling lama, perbedaan waktu antara DES dan AES ± 0,2 sec sedangkan dengan RSA ± 8 sec.
b) Memori : Algoritma AES paling sedikit, kemudian algoritma DES yang paling banyak RSA, dimana perbedaan antara AES dan DES ±4 KB, sedangkan dengan RSA ±10 KB.
c) Byte Keluaran : Algoritma RSA paling kecil (63,536 byte) ,sedang DES dan AES saama(131,072 byte)

Dari hasil pengujian diatas dapat di ambil kesimpulan bahwa algoritma AES mempunyai keunggulan pada sisi waktu pemrosesan dan alokasi memori yang lebih sedikit namun byte yang di hasilkan lebih besar di bandingkan dengan algoritma yang lainnya. Oleh karena intu di perlukan sebuah algoritma kompresi yang dapat menutupi kekurangan dari algoritma enkripsi AES ini.

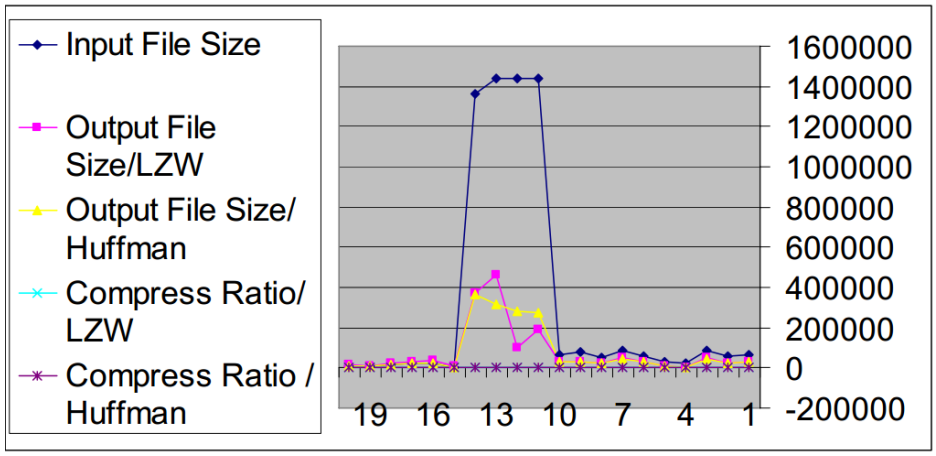
5.1.2. **Komparasi Algoritma Kompresi *Huffman***

Ada beberapa alternatif yang dapat di gunakan untuk melakukan kompresi data sebagai usaha untuk meminimalisir *space* yang di gunakan untuk menyimpan data ataupun untuk meminimalisir penggunaan *bandwidth* untuk mentransmisikan data tersebut. Namun dari hasil ujicoba yang di lakukan oleh Mohammed Al-laham dan Ibrahiem M. M. El Emary menunjukkan algoritma *Huffman* mempunyai efektifitas yang paling tinggi di bandingkan dengan algoritma *Run Length Encoding Technique, Arithmetic Coding Technique, LZ-77 Encoding Technique, LZW Coding Technique*.Berikut ini hasil pengujian yang telah di lakukan algoritma LZW dan Huffman.

Tabel 1. Perbandingan Algoritma LZW dan Huffman

File Name	Input File Size	Output File Size/LZW	Output File Size/ Huffman	Compress Ratio/ LZW	Compress Ratio / Huffman
Example1. doc	68096	30580	29433	55%	57%
Example2. doc	58880	23814	23640	60%	66%
Example3. doc	83968	48984	46876	42%	45%
Example4. doc	20480	2530	4836	88%	76%
Example5. doc	27648	8222	10921	70%	60%
Example6. doc	57856	30993	27163	46%	53%
Example7. doc	87552	54229	47101	38%	46%
Example8. doc	48128	23631	20600	51%	55%
Example9. doc	79360	30363	32416	62%	59%
Example10. doc	68096	30581	29433	55%	57%
Pict3.bmp	1440054	193888	276506	87%	81%
Pict4.bmp	1440054	100338	282824	93%	80%
Pict5.bmp	1440054	461637	318178	68%	78%
Pict6.bmp	1365318	371601	366830	73%	73%
Inprise. gif	4654	6634	5073	-43%	-9%
Baby. jpg	26183	35367	26487	-35%	-1%
Cake. Jpg	23036	32457	23479	-41%	-2%
Candles. jpg	17639	23230	17885	-32%	-1%
Class. jpg	5851	6764	6035	-16%	-3%
Earth. jpg	9370	12955	9811	-38%	-5%

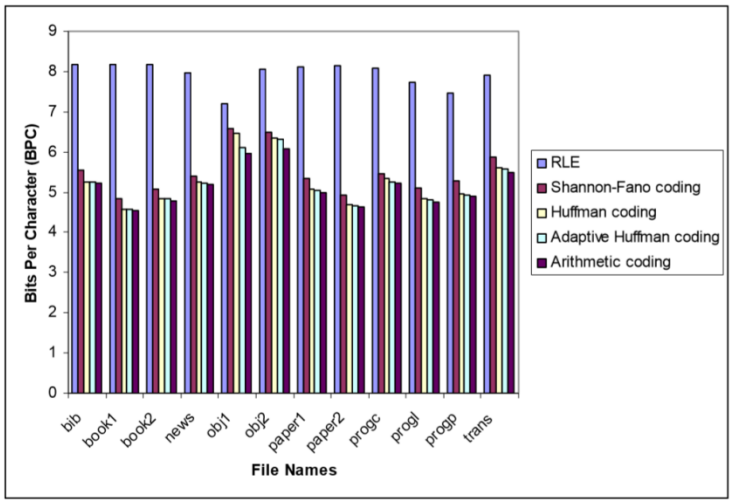
Sumber :(Al-laham & El Emary, 2007)



Sumber :(Al-laham & El Emary, 2007)

Gambar 8. Perbandingan Algoritma LZW dan Huffman

Selain dari hasil penelitian yang di lakukan oleh Mohammed Al-laham dan Ibrahiem M. M. El Emary, Hasil serupa juga di dapatkan dari ujicoba yang di lakukan oleh Irwan Wardoyo , dkk kita dapat lihat bahwa dengan menggunakan kode ASCII untuk meng-encoding teks tersebut membutuhkan 800.000 bit, sedangkan dengan menggunakan 3-bit kode dibutuhkan 300.000 bit dan dengan menggunakan kode *Huffman* hanya membutuhkan 224.000. Dengan menggunakan data tersebut maka dapat kita lihat bahwa dengan menggunakan algoritma *Huffman* dapat mengompres teks sebesar 70% dibandingkan kita menggunakan kode ASCII dan sebesar 25,3% dibandingkan kita menggunakan 3-bit kode.Pada pengujianPerbandingan Kinerja Algoritma Kompresiyang di lakukan oleh SenthilShanmugasundaram dan Robert Lourdusamy menunjukkan hasil Dalam teknik kompresi statistik, *Arithmetic coding* melebihi yang lainnya dengan peningkatan sebesar 1,15% dibandingkan *Adaptive Huffman coding*, 2.28% lebih dari *Huffman coding*, 6.36% lebih dari*Shannon-Fano coding* dan 35.06% lebih dariteknik*Run Length Encoding.*



Sumber :(Shanmugasundaram & Lourdusamy, 2011, p. 73)

Gambar 9.Perbandingan Kinerja Algoritma Kompresi

Dari bebrapa penelitian mengenai kompresi teks diatas Huffman coding menjadi salah satu alternative terbaik sebagai solusi melakukan kompresi data dengan berbagai pertimbangan dari byte keluaran yang di hasilkan, kinerja kompresi, waktu pemrosesan dan penggunaan memori yang di perlukan.

Kesimpulan Dan Saran

Karena pada *cloud* membutuhkan kecepatan transfer data yang baik maka dengan menggunakan algoritma hufman dapat menjadi salah satu pilihan untuk membuat data yang di kirim menjadi lebih kecil sehinga membutuhkan *bandwidth* tidak terlalu besar untuk transfer datanya sehingga memungkinkan bagi user yang hanya memiliki *bandwidth* keciltetap dapat menikmati *cloud* akses data yang cepat. Kemudin pada sisi keamanan datanya kita dapat menggabungkan algoritma *Huffman* ini dengan algoritma enkripsi dari hasil ujicoba beberapa penelitian ilmiah diatas dan salah satunya yang di lakukan oleh Shashi Mehrotra Sethdan Rajan Mishra dapat kita simpulkan bahwa algoritma AES mempunyai waktu pemrosesan dan penggunaan memori yang lebih sedikit di banding dengan algoritma DES dan RSA. Namun algoritma AES mempunyai kekurangan dalam byte keluaran yang relative lebih besar di bandingkan dengan algoritma yang lainnya.Oleh karenanya enkripsi AES ini dapat kita sandingkan dengan algoritma *Huffman* untuk dapat menghasilkan data dengan *byte* yang lebih kecil serta lebih aman ketika ditransfer ke *cloud*e maupun ketika berada di *cloude storage.*

Ada Beberapa hal yang belum terselesaikan di peneletian ini dan di harapkan dapat di selesaikan pada penelitian selanjutnya adapun saran bagi peneliti selanjutnya dari yang belum terselesaikan di peneletian ini antara lain :

1. Pada tulisan selanjutnya di harapkan kedua algoritma ini sudah dapat di aplikasikan secara real sehingga dapat secara nyata bermanfaat bagi pengguna *cloud*.
2. Penggunaan algoritma *Huffman* hanya akan optimal bila di gunakan untuk komresi teks, untuk penelitian selanjutnya di harapkan dapat menemukan kombinasi yang pas untuk melakukan kompresi pada semua bentuk dokumen tidak semata pada teks namun juga pada gambar, video maupun yang berbentuk suara.
3. Penggunaan desain infrastruktur jaringan yang tepat juga berdampak pada transfer data, pada penelitian selanjutnya diharapkan dapat menunjukkan perpaduan desain infrastruktur yang tepat untuk di gabungkan dengan algoritma ini sehingga menjadi lebih optimal.

VIII. DAFTAR PUSTAKA

Balbudhe, P., & Balbudhe, P. (2013). Cloud Storage Reference Model for Cloud Computing. *International Journal of IT, Engineering and Applied Sciences Research (IJIEASR)*, 81-85.

Enterprise, J. (2010). *Trik Mengoperasikan PC Tanpa Software.* Jakarta: PT Elex Media Komputindo.

Agung, M. (2013). *Implementasi Huffman Encoding Berorientasi Objek pada Bahasa Pemrograman Java.* Bandung: Institut Teknologi Bandung.

Al-laham, M., & El Emary, I. (2007). Comparative Study Between Various Algorithms of Data Compression Techniques. *The World Congress on Engineering and Computer Science.* San Francisco.

Bhisikar, P., & Sahu, P. (2013). Security in Data Storage and Transmission in Cloud Computing. *International Journal of Advanced Research in Computer Science and Software Engineering*, 410-415.

Huffman, D. A. (1952). A Method for the Construction of Minimum-Redundancy Codes. *I.R.E* (hal. 1098-1101). Proceedinges Of The I.R.E.

Leena, M. r. (2012). Centralized Database Security in Cloud. *International Journal of Advanced Research in Computer and Communication Engineering*, 544-549.

Nigoti, R., Jhuria, M., & Shailendra, S. (2013). A Survey of Cryptographic Algorithms for Cloud Computing. *International Journal of Emerging Technologies in Computational and Applied Sciences* , 141-146.

Porwal, A., Maheshwari, R., Pal, B., & Kakhani, G. (2012). An Approach for Secure Data Transmission in Private Cloud. *International Journal of Soft Computing and Engineering*, 151-155.

Ruddy, M., & Ozdemir, E. (2013). *An In-Depth Study of Broadband Infrastructure in the ASEAN Region August 2013.* Bangkok: Economic and Social Commission for Asia and the Pacific .

Sadikin, R. (2013). *Kriptografi Untuk Keamanan Jaringan.* Yogyajarta: ANDI Yogyakarta.

Seth, S. M., & Mishra, R. (2011). Comparative Analysis Of Encryption Algorithms For Data Communication. *International Journal of Computer Science and technology*, 292-294.

Shanmugasundaram, S., & Lourdusamy, R. (2011). A Comparative Study Of Text Compression Algorithms. *International Journal of Wisdom Based Computing,*, 68-76.