ANALISIS PERFORMA ALGORITMA ENKRIPSI AES, DES, DAN 3DES PADA PENGIRIMAN DATA MENGGUNAKAN UFTP

Anita Kusumawardani[1)], Mahendra Data, S.Kom., M.Kom[2)], Eko Sakti P., S.Kom., M.Kom[3)]
Informatika, Fakultas Ilmu Komputer, Universitas Brawijaya
Jl. Veteran No. 8 Malang 65145, Indonesia
Email: wardanita18@gmail.com[1)], mahendra.data@ub.ac.id[2)], ekosakti@ub.ac.id[3)]

Abstrak

UFTP merupakan protokol sekaligus aplikasi end-user yang menyediakan layanan reliable multicast dan memiliki fitur enkripsi untuk mengamankan data. UFTP ditujukan untuk pengiriman file berukuran besar. Algoritma enkripsi yang tersedia di aplikasi UFTP adalah AES, DES, dan 3DES yang merupakan block-cipher encryption dengan kunci simetris. Masing-masing algoritma memiliki performa yang berbeda yang akan mempengaruhi proses pengiriman file. Penelitian ini berawal dari keingintahuan penulis terhadap performa enkripsi AES, DES, dan 3DES dalam aplikasi UFTP. Dalam penelitian ini, lima file dengan ukuran yang berbeda digunakan untuk pengiriman tanpa enkripsi, pengiriman menggunakan enkripsi AES, pengiriman menggunakan enkripsi DES, dan pengiriman menggunakan enkripsi 3DES. Kelima file tersebut memiliki ukuran dalam rentang 200 MB hingga 1000 MB. Pengujian dilakukan dalam dua tahap. Tahap pertama menggunakan sebuah server dan sebuah klien yang dihubungkan dengan server proxy UFTP yang berjalan di komputer server. Lingkungan pengujian yang digunakan adalah jaringan komputer Fakultas Ilmu Komputer Universitas Brawijaya dengan server diletakkan di Laboratorium KCV dan klien diletakkan di Laboratorium Jaringan Komputer. Pengiriman file dilakukan menggunakan jaringan kabel yang menghubungkan kedua laboratorium. Pengujian kedua dilakukan menggunakan empat klien yang terhubung dengan sebuah server melalui emulator. Hasil pengujian menggunakan aplikasi UFTP menunjukkan bahwa performa algoritma AES sedikit lebih baik dibanding algoritma DES. Sementara itu, algoritma 3DES menghasilkan performa terburuk dengan kecepatan proses enkripsi-dekripsi dua kali lebih besar dibanding algoritma AES dan algoritma DES..

Kata kunci : *performa, UFTP, aes, des, 3des*

Abstract

UFTP is a protocol at the same end-user applications that provide reliable multicast services and features secure data encryption. UFTP intended for delivery of large files. Encryption algorithms available in the UFTP application are AES, DES, and 3DES which are block-cipher encryption with a symmetric key. Each algorithm has a different performance that will affect the process of files transmissions. This study came from my curiosity about AES, DES, 3DES encryption performances in UFTP application. In this study, five files of different sizes used for different scenario of transmissions which are transmission without encryption, transmission using AES encryption, transmission using DES encryption, and transmission using 3DES encryption. All file used for transmission has the size in the range of 200 MB to 1000 MB. There are two test that has been done on this study. First test is done using a server and a client associated with UFTP proxy server running on the server computer. The test environment used is the computer network of Faculty of Computer Science of Brawijaya University with a server is placed at the Laboratory of KCV and the client is placed in the Laboratory of Computer Network. File transmission is done using the network cable that connects the two laboratories. The second test is done using four client that connect to a server using an emulator as a bridge or router. The test results indicate that the use of AES algorithm performance using UFTP applications is slightly better than the DES

algorithm. Meanwhile, the 3DES algorithm produces the worst performance with a speed of encryption and decryption process two times greater than the algorithms AES and DES algorithms.

***Keywords**: performance, UFTP, aes, des, 3des*

1. PENDAHULUAN

1.1 Latar Belakang

UFTP merupakan program pengiriman file secara multicast yang berguna untuk pengiriman file berukuran besar dan memiliki fitur enkripsi. Atmojo (2016) meneliti tentang perbandingan performansi metode file sharing dalam penelitiannya yang berjudul "Analisis Perbandingan Performansi Metode File Sharing Berbasis Multicast dengan Peer-to-Peer dalam Proses Distribusi Konten Data". Penelitian tersebut menggunakan UFTP sebagai aplikasi multicast dan BiTorrent Sync sebagai aplikasi peer-to-peer, dengan kesimpulan bahwa UFTP dengan mekanisme TMCC menghasilkan performansi yang lebih baik dibanding BiTorrent Sync untuk pengiriman konten data tanpa menggunakan enkripsi.

Penambahan fitur enkripsi pada pengiriman file akan mempengaruhi lamanya waktu pengiriman. Belum diketahui seberapa besar pengaruh penggunaan enkripsi terhadap pengiriman file menggunakan aplikasi UFTP. Untuk itu perlu adanya penelitian yang mengevaluasi performa algoritma enkripsi pada aplikasi UFTP sehingga dapat diketahui pengaruh penggunaan algoritma enkripsi terhadap proses pengiriman file. Algoritma enkripsi yang tersedia pada aplikasi UFTP adalah AES, DES, 3DES yang merupakan algoritma block cipher dengan kunci simetris.

Penelitian yang telah dilakukan oleh Al Tamimi (2006) terhadap performa algoritma AES, DES, dan 3DES menyimpulkan bahwa AES memiliki performa terburuk karena proses komputasi yang lebih rumit. Penelitian tersebut mengevaluasi performa algoritma AES, DES, 3DES, dan Blowfish dengan panjang kunci yang berbeda. Penelitian lain yang dilakukan oleh Agrawal dan Sharma (2010) melakukan implementasi dan analysis algoritma dengan kunci simetris yaitu AES, 3DES, Blowfish, dan RC4. Hasilnya adalah algoritma Blowfish merupakan algoritma yang kuat dibandingkan algoritma lain, sementara 3DES memerlukan waktu komputasi yang paling lama. Penelitian ini juga menyebutkan bahwa DES adalah enkripsi yang paling banyak digunakan terutama pada aplikasi finansial dan AES ideal digunakan untuk aplikasi chat atau aplikasi yang berhubungan dengan transaksi keuangan.

Penelitian milik Al Tamimi serta Agrawal & Sharma memberikan hasil yang berbeda terkait performa algoritma AES, DES, dan 3DES. Menurut Singhal & Raina (2011), kompleksitas proses enkripsi tergantung pada algoritma enkripsi, perangkat lunak yang digunakan, serta kunci untuk proses enkripsi dan dekripsi data pada suatu algoritma. Oleh karena itu, penulis ingin meneliti tentang performa algoritma AES, DES, dan 3DES pada aplikasi UFTP sekaligus untuk mengetahui pengaruh penggunaan enkripsi terhadap pengiriman file. Judul yang digunakan pada penelitian ini adalah "Analisis Performa Algoritma Enkripsi AES, DES, dan 3DES pada Pengiriman Data Menggunakan UFTP". Pengujian dilakukan dalam dua tahap yaitu pengujian menggunakan satu klien di jaringan komputer lokal Fakultas Ilmu Komputer Universitas Brawijaya dan pengujian menggunakan 4 klien yang dijalankan dengan virtual machine. Diharapkan penelitian ini dapat berguna untuk memberikan gambaran performa algoritma enkripsi AES, DES, dan 3DES pada aplikasi UFTP yang merupakan aplikasi multicast.

1.2 Rumusan Masalah

Rumusan masalah penelitian ini adalah:

1. Bagaimana performa pengiriman konten data melalui UFTP tanpa menggunakan enkripsi?
2. Bagaimana performa pengiriman konten data melalui UFTP menggunakan algoritma enkripsi AES, DES dan 3DES?

1.3 Tujuan

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengetahui performa pengiriman file melalui aplikasi UFTP tanpa menggunakan enkripsi.
2. 2. Mengetahui performa pengiriman file menggunakan algoritma enkripsi AES, DES, dan 3DES pada aplikasi UFTP.

.

1.4 Manfaat

Manfaat dari penelitian ini adalah:

1. Mendapatkan hasil uji dan analisis performa algoritma enkripsi pada proses pengiriman konten data menggunakan aplikasi UFTP.
2. Memberikan acuan penggunaan enkripsi yang efisien dalam proses pengiriman konten data melalui UFTP.

1.5 Batasan Masalah

Batasan masalah dalam penelitian ini diantaranya adalah:

1. Penelitian ini dibatasi pada pembahasan mengenai performa algoritma enkripsi pada pengiriman konten data melalui UFTP dan tidak membahas kekuatan algoritma enkripsi dalam pengamanan data.
2. Panjang kunci yang digunakan pada algoritma AES adalah 128 bits dengan mode operasi CBC.

2. DASAR TEORI

2.1 Multicast

Dalam jaringan komputer, alamat IPv4 terbagi kedalam tiga tipe fundamental yaitu unicast, broadcast, dan multicast. Sebuah alamat unicast merupakan alamat yang didesain untuk transmisi sebuah paket ke satu tujuan. Alamat broadcast digunakan untuk mengirim datagram ke seluruh host dalam suatu jaringan. Alamat multicast didesain dengan kemampuan untuk mengirim datagram ke sejumlah host yang terkonfigurasi sebagai anggota dari sebuah grup multicast, baik dalam satu jaringan maupun di jaringan komputer yang berbeda. Sebuah datagram pada multicast dikirim ke anggota grup tujuan yang memiliki "best effort" reability yang sama. Hal tersebut berarti bahwa multicast tidak menjamin bahwa datagram yang ditransmisikan akan sampai ke seluruh anggota grup yang menjadi tujuan. Multicast juga tidak menjamin bahwa paket yang diterima oleh host tujuan memiliki urutan yang sama dengan paket yang dikirim.

Perbedaan IP multicast dan IP unicast yaitu adanya alamat grup di Destination Address field pada IP header. Pada unicast, alamat IP yang digunakan adalah alamat IP class A, class B, atau class C. Multicast menggunakan alamat IP class D yang berbeda dengan unicast yaitu 224.0.0.0 hingga 239.255.255.255. Sebuah alamat multicast ditujukan kepada sejumlah penerima yang mendefinisikan grup multicast. Pengirim menggunakan alamat multicast sebagai alamat IP tujuan dari paket yang nantinya ditransmisikan ke seluruh anggota grup multicast. Alamat IP pada class D diawali dengan empat angka biner yaitu "1110" yang diikuti oleh 28 bit ID grup multicast.

Alamat IP grup multicast telah ditetapkan oleh The Internet Assigned Numbers Authority (IANA). Alamat IP 224.0..0..0 digunakan sebagai base address dan tidak dapat diterapkan pada grup multicast lain. Alamat multicast dalam rentang 224.0.0.1 hingga 224.0.0.255 telah digunakan dalam sejumlah routing protocols. Router multicast tidak diijinkan mengirim datagram multicast dengan alamat tujuan dalam rentang ini.

Multicast tidak membatasi lokasi fisik sebuah host maupun jumlah anggota dalam sebuah grup. Host individu dapat bergabung ke dalam grup atau keluar dari grup multicast secara bebas. Sebuah host dapat menjadi anggota di satu atau lebih grup multicast dan tidak harus menjadi anggota sebuah grup untuk dapat mengirim pesan ke anggota grup multicast. (Semeria dan Maufer, 1996)

2.2 UFTP

UFTP merupakan reliable multicast protocol sekaligus aplikasi end-user yang koresponden. UFTP dapat disebut sebagai penerus dari Starburst Multicast FTP (MFTP) yang diusulkan pada tahun 2004 dan menawarkan layanan reliable multicast file transfer menggunakan UDP (Bakharev dan Siemens, 2013). Aplikasi ini dapat digunakan untuk pengiriman file berukuran besar ke sejumlah penerima dan dapat melakukan pengiriman melalui satellite link dengan komunikasi dua arah. Dalam hal pengiriman file melalui satellite link, aplikasi yang menggunakan TCP cenderung tidak efisien karena adanya delay yang tinggi.

Satu session dalam UFTP terdiri atas tiga fase yaitu fase Announce/Register, fase File Transfer, dan fase Completion. Fase *Announce/Register* adalah fase dimana UFTP mengatur *session* untuk file transfer sekaligus melakukan negosiasi seluruh parameter enkripsi. Fase *File Transfer* terbagi menjadi 2 subfase yaitu fase *File Info* dan fase *Data Transfer* untuk setiap file yang dikirim. Sub fase *File Info* yaitu server mengirim pesan yang mendeskripsikan file yang akan dikirim,

sedangkan *Data Transfer* adalah proses saat file dikirim ke penerima. Fase terakhir adalah fase *Completion* atau *Confirmation* yang mengindikasikan akhir dari *session*.

2.2 AES

AES atau *Advanced Encryption Standard* merupakan standar enkripsi yang dipublikasin oleh *National Institute of Standard and Technology*. AES dikembangkan untuk menggantikan DES yang dianggap kurang aman. Algoritma AES menggunakan kunci dengan panjang 128 bits, 192 bits, dan 256 bits.

2.3 DES

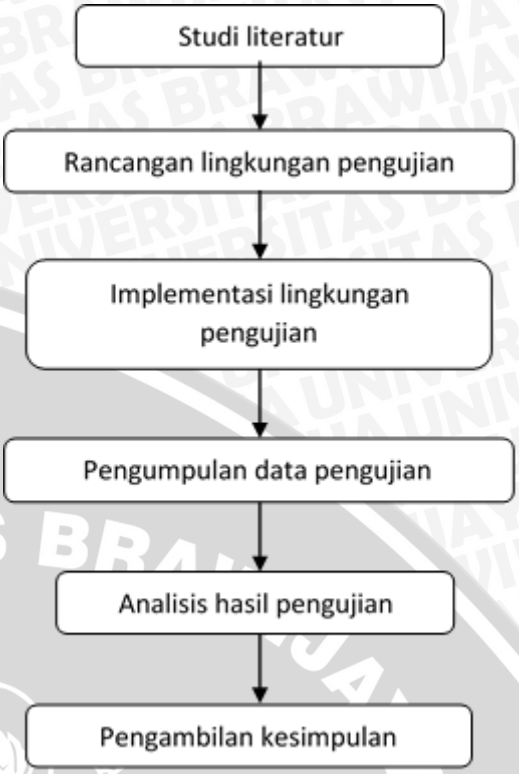
DES atau *Data Encryption Standard* merupakan standar enkripsi yang digunakan dalam banyak aplikasi. Proses enkripsi pada DES lebih sederhana debanding proses enkripsi AES. Panjang kunci yang digunakan algoritma DES adalah 64 bits.

2.4 3DES

3DES merupakan pengembangan dari algoritma DES. Pada dasarnya 3DES adalah enkripsi DES yang dijalankan dalam 3 proses yaitu proses encrypt-decrypt-encrypt dalam algoritmanya. Proses tersebut menghasilkan kunci dengan panjang 168 bit, tiga kali lipat dari panjang kunci DES. 3DES menggunakan proses EDE dengan kunci enkripsi dan dekripsi yang berbeda untuk satu proses 3DES. Hal ini untuk menghindari loop yang panjang karena adanya penggunaan kunci yang sama secara berulang.

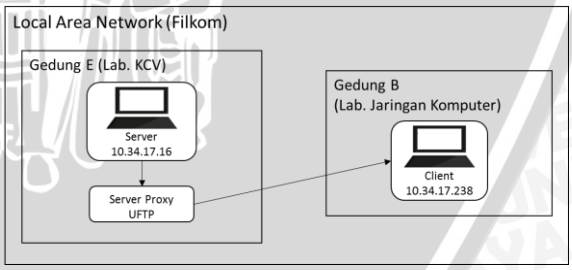
3. METODOLOGI

Alur metode penelitian dapat dilihat pada Gambar 3.1.



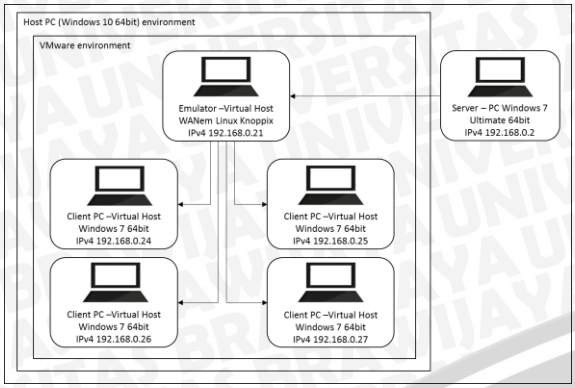
Gambar 3.1 Alur metode penelitian

Penelitian ini dilakukan dalam dua pengujian yaitu pengujian yang dilakukan di lingkungan jaringan komputer FILKOM Universitas Brawijaya dimana server dan klien diletakkan pada gedung yang berbeda serta pengujian dengan empat klien menggunakan emulator. Lingkungan pengujian penelitian ini terlihat pada Gambar 3.2 dan Gambar 3.3.



Gambar 3.2 Lingkungan pengujian I

..



Gambar 3.3 Lingkungan pengujian II

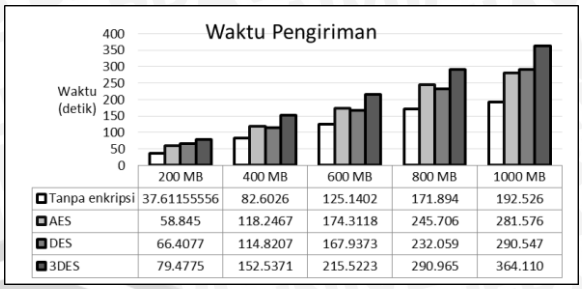
Terdapat 20 skenario pengujian yang dilakukan pada penelitian ini. Skenario pengujian tersebut dapat dilihat pada Tabel 3.1

Tabel 3.1 Skenario Pengujian

Skenario	Ukuran File (MB)	Enkripsi-Dekripsi
1	200	Tanpa Enkripsi
2		AES
3		DES
4		3DES
5	400	Tanpa Enkripsi
6		AES
7		DES
8		3DES
9	600	Tanpa Enkripsi
10		AES
11		DES
12		3DES
13	800	Tanpa Enkripsi
14		AES
15		DES
16		3DES
17	1000	Tanpa Enkripsi
18		AES
19		DES
20		3DES

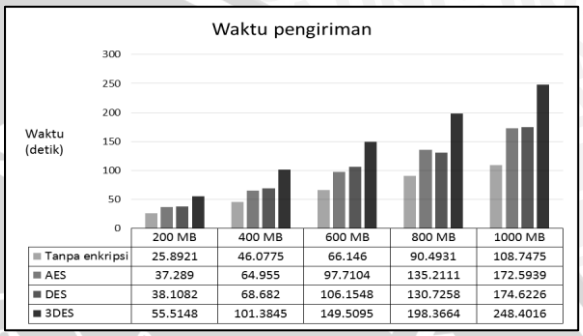
4. HASIL DAN ANALISIS

Hasil pengujian penelitian ini dapat dilihat pada gambar di bawah ini. Gambar 4.1 dan Gambar 4.2 menampilkan hasil pengujian dengan parameter waktu pengiriman, Gambar 4.3 dan Gambar 4.4 menampilkan nilai *throughput*, dan Gambar 4.5 menampilkan kecepatan proses enkripsi-dekripsi untuk tiap algoritma.pada pengujian pertama dan engujian kedua.



	200 MB	400 MB	600 MB	800 MB	1000 MB
Tanpa enkripsi	37.61155556	82.6026	125.1402	171.894	192.526
AES	58.845	118.2467	174.3118	245.706	281.576
DES	66.4077	114.8207	167.9373	232.059	290.547
3DES	79.4775	152.5371	215.5223	290.965	364.110

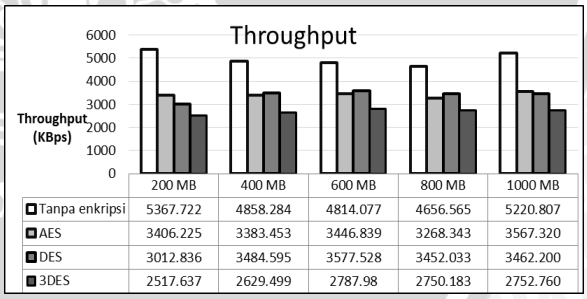
Gambar 4.1 Waktu Pengiriman pengujian I



	200 MB	400 MB	600 MB	800 MB	1000 MB
Tanpa enkripsi	25.8921	46.0775	66.146	90.4931	108.7475
AES	37.289	64.955	97.7104	135.2111	172.5939
DES	38.1082	68.682	106.1548	130.7258	174.6226
3DES	55.5148	101.3845	149.5095	198.3664	248.4016

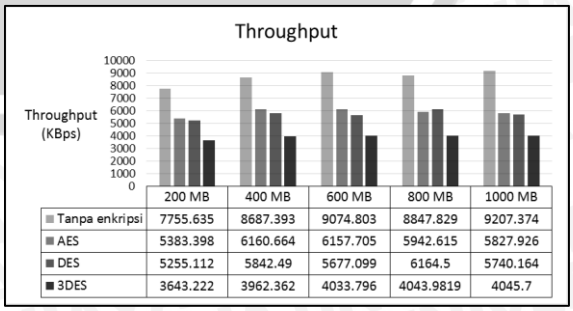
Gambar 4.2 Waktu Pengiriman pengujian II

Waktu pengiriman yang dihasilkan terus meningkat seiring bertambahnya ukuran file. Pengiriman menggunakan algoritma 3DES menunjukkan peningkatan waktu pengiriman yang lebih tinggi dibanding pengiriman tanpa menggunakan enkripsi maupun pengiriman menggunakan AES dan DES. Waktu pengiriman menggunakan algoritma AES dan DES saling mengungguli satu sama lain.



	200 MB	400 MB	600 MB	800 MB	1000 MB
Tanpa enkripsi	5367.722	4858.284	4814.077	4656.565	5220.807
AES	3406.225	3383.453	3446.839	3268.343	3567.320
DES	3012.836	3484.595	3577.528	3452.033	3462.200
3DES	2517.637	2629.499	2787.98	2750.183	2752.760

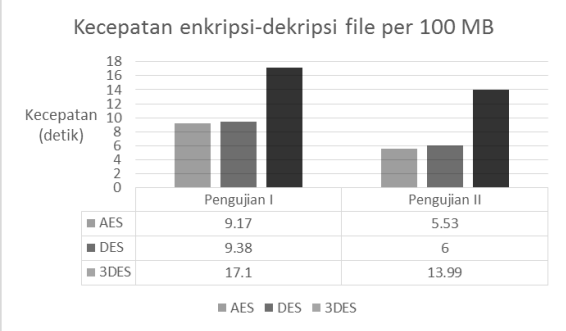
Gambar 4.3 Throughput pengujian 1



	200 MB	400 MB	600 MB	800 MB	1000 MB
Tanpa enkripsi	7755.635	8687.393	9074.803	8847.829	9207.374
AES	5383.398	6160.664	6157.705	5942.615	5827.926
DES	5255.112	5842.49	5677.099	6164.5	5740.164
3DES	3643.222	3962.362	4033.796	4043.9819	4045.7

Gambar 4.3 Throughput pengujian 1I

Throughput yang dihasilkan saat pengiriman tanpa menggunakan enkripsi lebih besar dibanding throughput yang dihasilkan pengiriman file menggunakan enkripsi. Di antara ketiga algoritma enkripsi, 3DES memiliki throughput terendah yaitu berkisar antara 2500 KBps hingga 2800 KBps pada pengujian pertama. Throughput yang dihasilkan pada pengiriman menggunakan AES dan DES berkisar antara 3000 KBps hingga 3500 KBps. Perbandingan nilai throughput pengujian pertama dan kedua adalah sebanding dengan hasil bahwa throughput 3DES lebih kecil dari AES dan DES karena proses enkripsi dan dekripsi yang lebih lama.



Gambar 4.5 Kecepatan enkripsi-dekripsi file

Rata-rata kecepatan proses enkripsi-dekripsi AES sedikit lebih baik dibanding DES. Sementara itu rata-rata kecepatan algoritma 3DES dua kali lebih besar disbanding algoritma DES dan AES.

5. PENUTUP

3.1 Kesimpulan

Berdasarkan pengujian yang telah dilakukan, dapat disimpulkan bahwa:

1. Pengujian performa pengiriman file melalui UFTP tanpa menggunakan enkripsi menghasilkan waktu pengiriman yang proporsional untuk setiap kenaikan ukuran file sebesar 200 MB dan menghasilkan rata-rata throughput dengan throughput yang cukup stabil.
2. Berdasarkan hasil pengujian dengan parameter waktu pengiriman, throughput, dan kecepatan enkripsi-dekripsi, diketahui bahwa AES memiliki performa yang lebih baik dibanding DES. Sementara itu, 3DES membutuhkan waktu dua kali lebih banyak dibanding AES dan DES untuk melakukan enkripsi-dekripsi file dengan throughput yang jauh lebih kecil dibanding pengujian dengan AES dan DES..

3.2 Saran

Saran yang dapat diberikan untuk pengembangan penelitian selanjutnya adalah:

1. Perlu adanya penelitian performa UFTP beserta fitur enkripsinya di lingkungan jaringan komputer FILKOM Universitas Brawijaya secara *wireless*.
2. Penelitian ini dilakukan tanpa memperhatikan kondisi trafik jaringan komputer. Untuk itu diperlukan penelitian yang membandingkan performa algoritma enkripsi pada aplikasi UFTP dalam kondisi trafik yang berbeda yaitu pada saat jaringan komputer ramai dan sepi.

DAFTAR PUSTAKA

Agrawal, H., Sharma, M., 2010. Implementation and Analysis of Various Symmetric Cryptosystems. Indian Journal of Sience and Technology, [e-journal] 3(12). Tersedia melalui: Indian Journal of Science and Technology <www.indjst.org> [Diakses 28 Desember 2015]

Al Tamimi, A.,n.d. Performance Analysis of Data Encryption Algorithms. Tersedia di: <http://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf/> [Diakses 16 Januari 2016]

Atmojo, D.D., 2016. Analisis Perbandingan Performansi Metode File Sharing Berbasis Muliticast dengan Peer-to-Peer dalam Proses Distribusi Konten Data. S1. Universitas Brawijaya.

Bakharev, A., Siemens, E., 2012. Actual Approaches For – Multicats-Based Reliable Data Transport and Their Deficiencies. International Conference on Networking and Services (9). Lisbon: International Academy Research and Industry Association.

Cisco® Visual Networking Index, 2015. The Zettabyte Era: Trends and Analysis.Cisco [online]. Tersedia di: <http://www.cisco.com > [Diakses 26 Januari 2016]

Dworkin, Morris, 2001. Recommendation for Block Cipher Modes of Operation: Methods

and Techniques. U.S: National Institute of Standards and Technology.

Semeria, C., Maufer, T., 1996. Introduction to IP Multicast Routing. U.S: Standford University. Tersedia di: <https://web.stanford.edu/class/files/> [Diakses 16 April 2016]

Singh, G., Supriyadi, 2013. Study of Encryption Algorithms (RSA, DES, 3DES, and AES) for Information Security. International Journal of Computer Applications, [e-journal] 67(0975 – 8887). Tersedia melalui: <http://citeseerx.ist.psu.edu/> [Diakses 5 Februari 2016]

Singhal, N., Raina, J.P.S., 1996. Comparative Analysis of AES and RC4 Algorithms for Better Utilization. U.S: North Carolina State University

Stallings, W., 2011. Cryptography and Network Security. 5th edition. New York: Prentice Hall.