MOTIVECTION
Journal of Mechanical Electrical and Industrial Engineering

Volume : 6, Number : 1, 2024
ISSN : 2655 – 7215 [printed] ; 2685-2098 [online]
DOI : 10.46574/motivection.v6i1.314

Implementation of Web-Based File Sharing Security System

Implementasi Sistem Keamanan Berbagi File Berbasis Website

Mike Yuliana[1*], Nuril Hidayah[1], Amang Sudarsono[1]

Abstract

File-sharing activities become a bridge for communication in the form of data between one party and another party. File sharing allows users to share data with other users, by uploading data to the server computer and other users can download data from the server computer. A document security system is indispensable to keep document data safe until its destination. File Web Sharing will transmit data with cryptographic methodologies. The algorithm used is Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Blowfish. This study aims to compare the performance of AES, DES, and Blowfish algorithms when implemented to secure file sharing. Performance research results show that the DES algorithm is on average 8.35% faster than AES and the Blowfish algorithm is 7.11% faster than AES. Memory usage capacity testing shows that the AES algorithm requires 4.82% greater memory capacity than Blowfish, and the DES requires 2.41% greater memory capacity than the Blowfish algorithm.

Keywords
File sharing, AES, DES, Blowfish

Abstrak

Kegiatan *file sharing* menjadi jembatan komunikasi data antara satu pihak dengan pihak lainnya. *File sharing* memberikan pengguna kemampuan untuk berbagi data dengan pengguna lain, dengan cara mengunggah data ke komputer server dan pengguna lain dapat mengunduh data dari komputer server. Sistem keamanan terhadap dokumen sangat diperlukan untuk menjaga data dokumen tetap aman sampai tujuannya. Web *File Sharing* akan mengirimkan data dengan metodologi kriptografi. Algoritma yang digunakan adalah Advanced Encryption Standard (AES), Data Encryption Standard (DES), dan Blowfish. Penelitian ini bertujuan untuk membandingkan kinerja algoritma AES, DES dan Blowfish saat diimplementasikan untuk mengamankan *file sharing*. Hasil pengujian kinerja menunjukkan bahwa algoritma DES rata-rata 8,35% lebih cepat dibandingkan AES sedangkan Blowfish 7,11% lebih cepat dibandingkan AES. Berdasarkan pengujian kapasitas penggunaan memori terlihat bahwa AES membutuhkan kapasitas memori 4,82% lebih besar dibandingkan Blowfish dan DES membutuhkan kapasitas memori 2,41% lebih besar dari Blowfish.

Kata Kunci
File sharing, AES, DES, Blowfish

[1] *Departemen Teknik Elektro, Politeknik Elektronika Negeri Surabaya*
Jln. Raya IT, Keputih, Sukolilo, Surabaya, Jawa Timur, Indonesia
* mieke@pens.ac.id

Submitted :January 20, 2024. Accepted : February 27, 2024. Published : February 29, 2024.

This is an open access article distributed under the Creative Commons 4.0 Attribution License

PENDAHULUAN

Aktivitas *file sharing* atau kegiatan berbagi dokumen sudah sering dilakukan. Kegiatan ini digunakan untuk komunikasi pengiriman data yang dilakukan antara satu pihak dengan pihak lainnya. *File sharing* atau berbagi berkas adalah aktivitas membagi atau menyediakan akses data ke media digital di internet kepada orang lain [1]. Untuk bisa saling berbagi, penyedia berkas harus melakukan *upload* berkas ke server terlebih dahulu, agar bisa diunduh oleh pengguna lain. Untuk mengatasi kebocoran data dari layanan server, dapat digunakan pendekatan enkripsi dan dekripsi dari sisi klien [2].

Berbagi dokumen melalui *website* sering dilakukan mengingat semua kegiatan dilakukan secara daring. Sistem keamanan untuk dokumen sangat diperlukan untuk menjaga agar data dokumen tetap aman sampai tujuan [3]. Keamanan komputer berhubungan dengan pencegahan dan deteksi terhadap tindakan penganggu yang tidak dikenali dalam sistem komputer. Kriptografi dapat mengubah dan melakukan format ulang data antar komputer agar lebih aman [4].

AES, DES, dan Blowfish merupakan algoritma yang menggunakan teknik kriptografi kunci simetris untuk penelitian ini [5]. Tujuannya adalah untuk melakukan perbandingan analisis performansi dan kapasitas memori yang dibutuhkan dari ketiga algoritma tersebut. Penelitian *file web sharing* ini menggunakan *Secure Socket Layer* (SSL) sebagai teknologi standar dan terdaftar untuk keamanan komunikasi antara *web server* dan *browser Internet* atau server email dan klien email [17]. Sistem *website* dibuat untuk membantu pengguna agar dapat mengakses dengan mudah secara daring.

Advanced Encryption Standard (AES)

Algoritma AES atau sering disebut sebagai algoritma Rijndael adalah cipher blok simetris dengan ukuran blok 128 bit dan ukuran kunci sepanjang 128, 192, atau 256 bit. AES bekerja pada matriks berukuran 4x4 di mana tiap-tiap sel matriks terdiri atas 1 byte (8 bit). Block cipher diasumsikan sebagai sebuah kotak. Setiap plainteks akan dikonversikan terlebih dahulu ke dalam blok-blok dalam bentuk *hexadecimal*, kemudian dilanjutkan pemrosesan dengan metode AES [6].

Metode ini dimulai dari teks biasa yang dienkripsi dan kemudian dikonversi ke teks cipher menggunakan algoritma enkripsi dan kunci. Ketika sudah mencapai penerima teks, maka cipher teks akan dikonversi menggunakan kunci yang sama yang diterapkan untuk enkripsi menggunakan algoritma dekripsi [7].

Data Encryption Standard (DES)

Algoritma DES menggunakan pendekatan enkripsi simetris dan Teknik subtitusi dan permutasi. Algoritma DES menggunakan ukuran blok 64 bit dan ukuran kunci 56 bit. Algoritma ini menggunakan algoritma yang sama untuk proses enkripsi dan dekripsi [8].

Proses dekripsi terhadap cipherteks merupakan kebalikan dari proses enkripsi. Jika proses enkripsi urutan kunci internal yang digunakan adalah K1, K2, …,K16, maka proses dekripsi urutan kunci yang digunakan adalah K16, K15, …,K1,

Setiap putaran 16,15,…,1 adalah keluaran setiap putaran deciphering yang dalam hal ini (R16, L16) diperoleh dengan mempermutasikan cipherteks dengan matriks permutasi IP-1. Pra-keluaran dari deciphering adalah (L0, R0) dengan permutasi awal IP akan didapatkan kembali blok plainteks semula [9].

Blowfish

Blowfish dikembangkan untuk memenuhi kriteria desain yang cepat dalam implementasinya dimana pada keadaan optimal dapat mencapai 26 *clock cycle* per *byte*, kompak dimana dapat berjalan pada memori kurang dari 5 KB dan keamanan variable. Panjang kunci bervariasi mulai dari 32 bit dengan maksimum 448 bit [10].

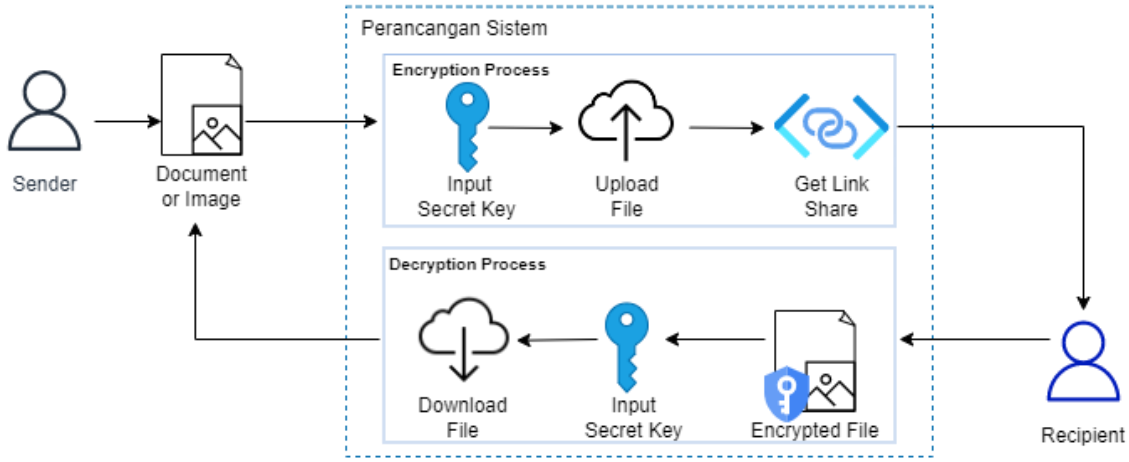
Ketika waktu komputasi enkripsi dan dekripsi, algoritma Blowfish memberikan performansi yang lebih baik dari pada algoritma kriptografi simetrik, seperti DES, TripleDES, Twofish, dan Threefish [11].

METODE PENELITIAN

Penelitian ini menggunakan metode eksperimen. Tahapan yang dilalui mulai dari studi literatur, perancangan sistem, implementasi sistem, pengujian hingga analisa dan kesimpulan. Perancangan *file web sharing* diperlukan untuk sistem yang akan di implementasikan pada penelitian ini. Sistem *file sharing* memiliki berbagai istilah, seperti situs *crowd sourcing*, *study aid*, dan platform *peer-to-peer* [14]. Penelitian ini menggunakan platform website secara *peer-to-peer* dengan user sebagai pengirim akan memilih *file* berupa dokumen atau gambar. Untuk memberikan keamanan pada *file* yang akan dikirimkan, pengirim melakukan input *secret key* yang akan melakukan proses enkripsi dari file berupa teks original atau *plain text* untuk dilakukan enkripsi menjadi *cipher text*. Setelah itu, pengirim dapat melakukan *upload file* dan menerima *link* yang dapat dikirimkan ke penerima.

Sisi penerima menerima link yang dapat dibuka langsung untuk melakukan proses dekripsi file. Proses ini dilakukan untuk mengubah *cipher text* menjadi *plain text* kembali menggunakan secret key yang sama karena bersifat simetris [12]. Selanjutnya, pengirim dapat melakukan download *file* untuk mendapatkan *file* seperti semula.

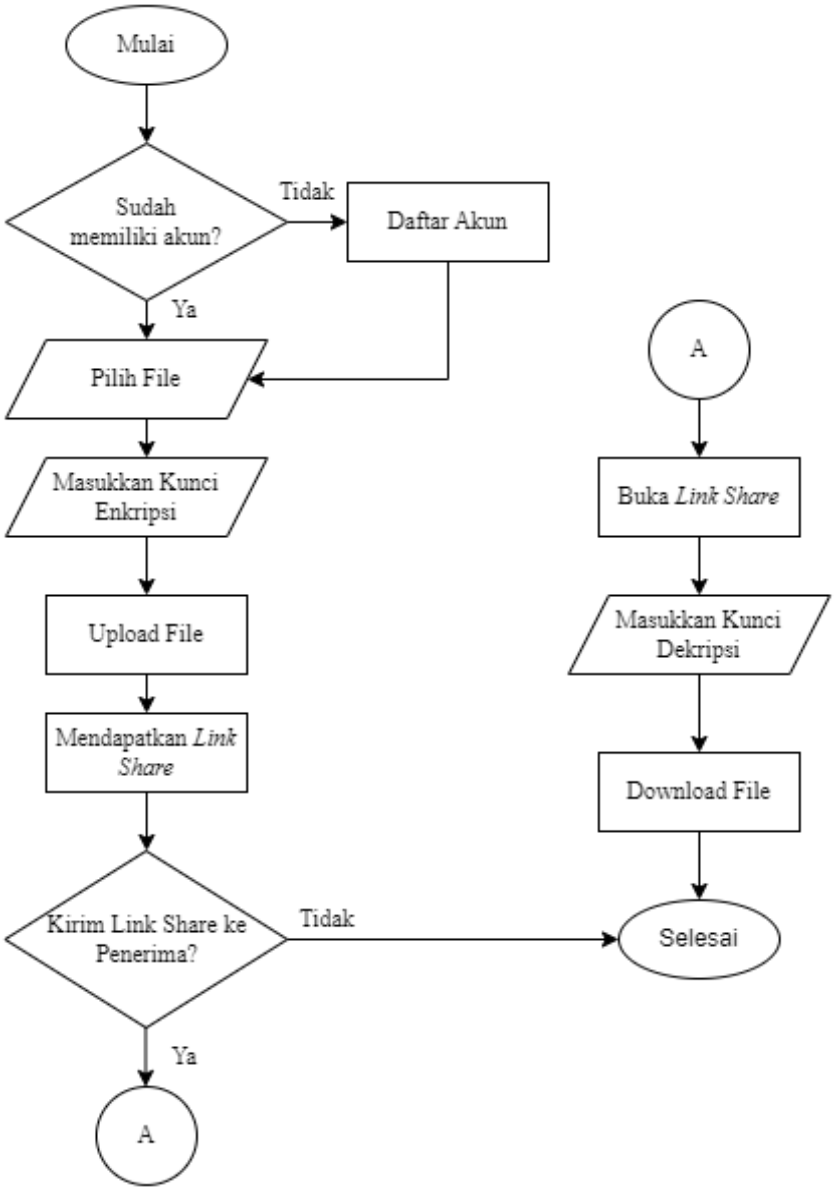
Proses enkripsi dan dekripsi suatu data dengan algoritma AES, DES, dan Blowfish sesuai dengan pemilihan kuncinya dan urutan proses yang dipilih. Enkripsi data adalah algoritma kriptografi yang lebih efisien secara matematis dan elegan, tetapi kekuatan utamanya terletak pada opsi untuk berbagai panjang kunci yang digunakan [16]. Berikut blok merupakan blok diagram diagram yang digunakan untuk implementasi keamanan berbagi file berbasis website seperti yang terlihat pada Gambar 1.



Gambar 1. Blok Diagram Perancangan File Web Sharing

Flowchart

Diagram alir penelitian pada Gambar 2 menggambarkan implementasi sistem dalam penelitian ini.



Gambar 2. Flowchart Implementasi Sistem

Pengujian Sistem

Pengujian komputasi performansi untuk algoritma AES, DES, dan Blowfish agar *user* dapat mengetahui performa kecepatan dari masing-masing algoritma. Pengujian ini untuk menilai waktu enkripsi ketika proses upload dan dekripsi ketika proses download agar mengetahui performansi algoritma [13]. Berikut rencana pengujian perfomansi menggunakan komputasi pada Tabel 1.

Tabel 1. Pengujian komputasi performansi

Parameter	Cara Pengujian	Hasil
Pengujian Perfomansi Komputasi	User melakukan proses upload dan download dengan memilih file pdf atau doc. Ketika berhasil, maka akan muncul nilai komputasi di bagian atas website.	Nilai komputasi akan muncul di page upload dan download dalam detik.

Pengujian kapasitas memori dilakukan agar user dapat mengetahui seberapa besar penggunaan memori untuk algoritma AES, DES, dan Blowfish. Penggunaan memori dari *library* python sebagai kompleksitas ruang klasifikasi kerangka kerja dengan algoritma enkripsi [15]. Penyimpanan data di platform *multicloud* menghilangkan masalah krusial terkait vendor *lock-in* dengan satu platform *cloud* [18]. Berikut rencana pengujian penggunaan kapasitas memori menggunakan FileZilla pada Tabel 2.

Tabel 2. Pengujian kapasitas memori

Parameter	Cara Pengujian	Hasil
Pengujian Kapasitas Memori	Ketika proses enkripsi, file akan masuk ke server. Untuk melihat seberapa besar memori yang diperlukan untuk masing-masing file, user menghubungkan FileZilla dengan folder uploads dari vps server.	Dapat dilihat di FileZilla untuk masing-masing file yang diupload.

HASIL DAN PEMBAHASAN

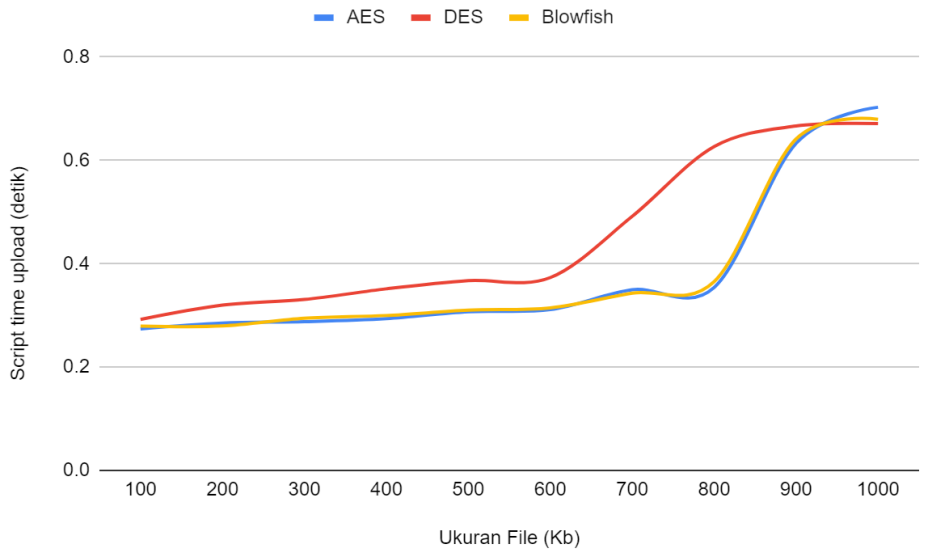
Hasil Pengujian Komputasi

Pengujian dilakukan dengan pengambilan beberapa sampel. Pada pengujian ini dilakukan komputasi data yang mana menghitung waktu *untuk script code* melakukan proses upload maupun download. Pengujian dilakukan dengan penambahan *code* pada file *code* upload dan download. Berikut hasil pengujian *script time upload* untuk format dokumen pdf seperti pada Tabel 3. Pada Tabel 3 dijelaskan bahwa pengujian dilakukan sebanyak 10 sampel dengan berbagai ukuran file dokumen. Pengujian ini menggunakan dokumen dengan format pdf mulai dari ukuran terkecil 100 kb hingga ukuran terbesar 1000 kb.

Tabel 3. Hasil Pengujian Script Time Upload Format PDF

Ukuran File (Kb)	*Script time upload* (detik)		
	AES 128	DES 64	Blowfish 64
100	0.2739369869	0.2921268940	0.2793810368
200	0.2851538658	0.3198108673	0.2795140743
300	0.2878301144	0.3307828903	0.2945878506
400	0.2935838699	0.3514640331	0.2998068333
500	0.3071911335	0.3673350811	0.3100819588
600	0.3111569881	0.3731999397	0.3145909309
700	0.3496680260	0.4916930199	0.3429939747
800	0.3539998531	0.6268210411	0.3654351234
900	0.6329941750	0.6665618420	0.6416199207
1000	0.7028641701	0.6712620258	0.6794369221

Berdasarkan data grafik Gambar 3, terdapat hasil script time untuk masing-masing algoritma dari AES, DES, dan blowfish. Hasil yang didapatkan dari rata-rata *execution time* menunjukkan bahwa DES lebih cepat 8,35% dari AES, sementara blowfish lebih cepat 7,11% dari AES.



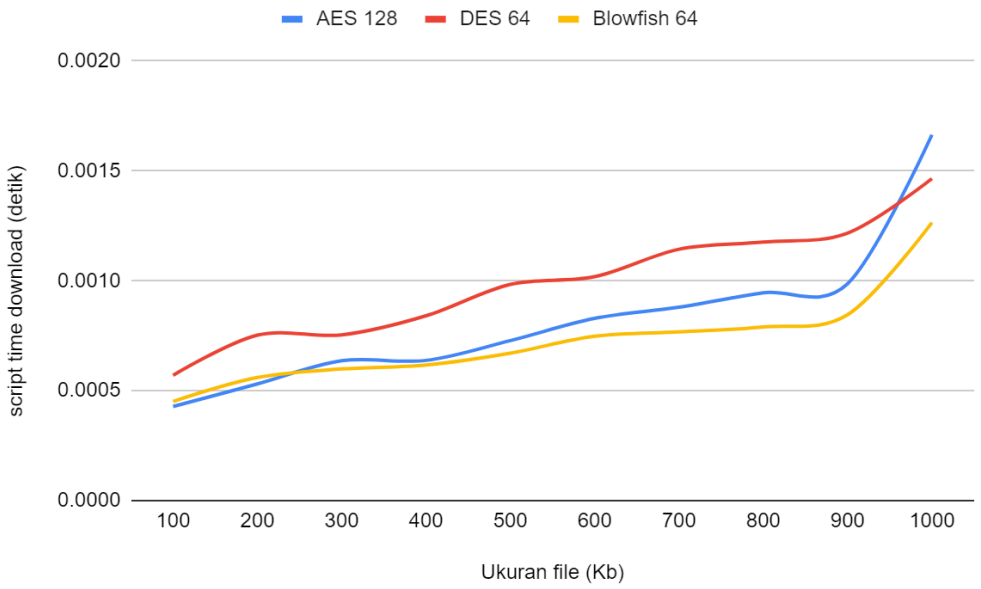
Gambar 3. Grafik Pengujian Komputasi Upload Dokumen PDF

Pada Tabel 4 dapat dijelaskan bahwa pengujian dilakukan sebanyak 10 sampel dengan berbagai ukuran file dokumen. Pengujian ini menggunakan dokumen dengan format pdf mulai dari ukuran terkecil 100 kb hingga ukuran terbesar 1000 kb.

Berdasarkan data grafik Gambar 4 , terdapat hasil script time untuk masing-masing algoritma dari AES, DES, dan blowfish. Hasil yang didapatkan dari rata-rata execution time menunjukkan bahwa DES lebih cepat 9,1% dari AES, sementara blowfish lebih cepat 6,11% dari AES.

Tabel 4. Hasil Pengujian Script Time Download Format PDF

Ukuran File (Kb)	***Script time download* (detik)**		
	AES 128	**DES 64**	**Blowfish 64**
100	0.0004279613495	0.0005700588226	0.0004510879517
200	0.0005309581757	0.0007529258728	0.0005600452423
300	0.0006361007690	0.0007541179657	0.0005989074707
400	0.0006380081177	0.0008409023285	0.0006170272827
500	0.0007281303406	0.0009839534760	0.0006709098816
600	0.0008289813995	0.0010190010070	0.0007479190826
700	0.0008800029755	0.0011439323430	0.0007679462433
800	0.0009460449219	0.0011761188510	0.0007898807526
900	0.0009870529175	0.0012176118850	0.0008459091187
1000	0.0016648769380	0.0014650821690	0.0012650489810



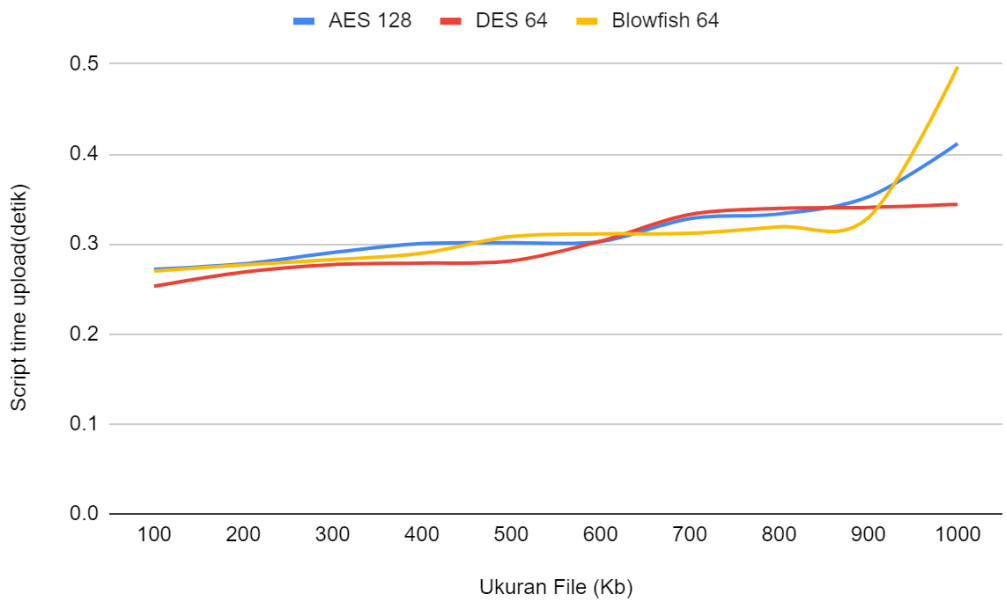
Gambar 4. Grafik Pengujian Komputasi Download Dokumen PDF

Pada Tabel 5 dapat dijelaskan bahwa pengujian dilakukan sebanyak 10 sampel dengan berbagai ukuran file dokumen. Pengujian ini menggunakan dokumen dengan format doc mulai dari ukuran terkecil 100 kb hingga ukuran terbesar 1000 kb.

Berdasarkan data grafik Gambar 5, terdapat hasil script time untuk masing-masing algoritma dari AES, DES, dan blowfish. Hasil yang didapatkan dari rata-rata execution time menunjukkan bahwa DES lebih cepat 2,45% dari AES, sementara blowfish lebih cepat 0,39% dari AES.

Tabel 5. Hasil Pengujian Script Time Upload Format DOC

Ukuran File (Kb)	***Script Time Upload* (detik)**		
	AES 128	**DES 64**	**Blowfish 64**
100	0.2718911171	0.2529981136	0.270005941
200	0.2778971195	0.2687661648	0.276720047
300	0.2905249596	0.2771060467	0.282588005
400	0.3004610538	0.2787759304	0.289713144
500	0.3014550209	0.2810847759	0.308234930
600	0.3027567863	0.3031919003	0.311305999
700	0.3282139301	0.3328199387	0.311882019
800	0.3334078789	0.3395690918	0.319122076
900	0.352380991	0.3406980038	0.329326868
1000	0.4117250443	0.3439581394	0.496940136



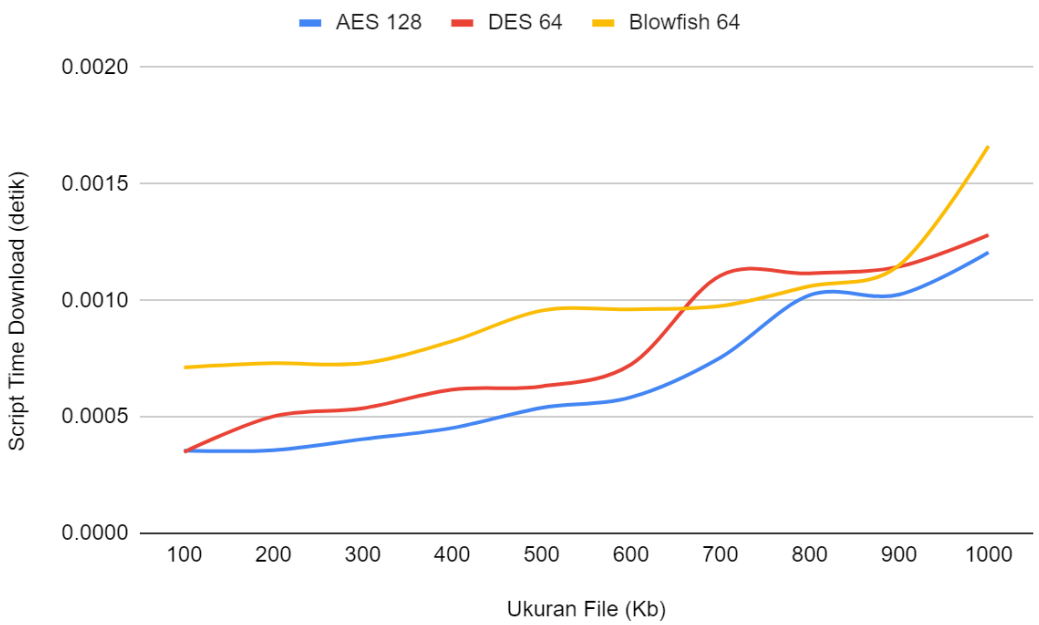
Gambar 5. Grafik Pengujian Komputasi Upload Dokumen DOC

Pada Tabel 6 dapat dijelaskan bahwa pengujian dilakukan sebanyak 10 sampel dengan berbagai ukuran file dokumen. Pengujian ini menggunakan dokumen dengan format doc mulai dari ukuran terkecil 100 kb hingga ukuran terbesar 1000 kb.

Tabel 6. Hasil Pengujian Script Time Download Format DOC

Ukuran File (Kb)	***Script Time Download* (detik)**		
	AES 128	**DES 64**	**Blowfish 64**
100	0.0003550052643	0.0003490447998	0.0007121562958
200	0.0003571510315	0.0005021095276	0.0007300376892
300	0.0004041194916	0.0005369186401	0.0007300376892
400	0.0004520416260	0.0006170272827	0.0008249282837
500	0.0005388259888	0.0006308555603	0.0009560585022
600	0.0005841255188	0.0007247924805	0.0009617805481
700	0.0007541179657	0.0011060237880	0.0009758472443
800	0.0010221004490	0.0011160373690	0.0010609626770
900	0.0010249614720	0.0011448860171	0.0011508464810
1000	0.0012059211730	0.0012810230260	0.0016629001621

Berdasarkan data grafik Gambar 6, terdapat hasil script time untuk masing-masing algoritma dari AES, DES, dan blowfish. Hasil yang didapatkan dari rata-rata execution time menunjukkan bahwa DES lebih cepat 8,9% dari AES, sementara blowfish lebih cepat 18,6% dari AES.



Gambar 6. Grafik Pengujian Komputasi Download Dokumen DOC

Hasil Pengujian Kapasitas Memori

Penggunaan kapasitas *memory* ketika proses enkripsi yang berada di sisi server perlu juga diperhatikan agar sesuai dengan RAM yang disediakan oleh layanan VPS server. Pada penelitian ini, menggunakan bantuan software FileZilla untuk melihat kapasitas *memory* ketika berada di sisi server.

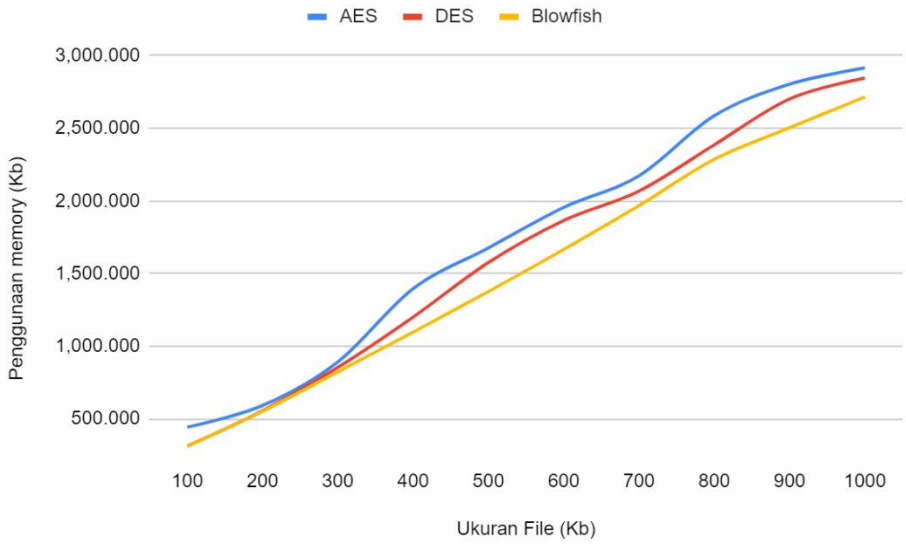
Berikut hasil penggunaan kapasitas memori untuk enkripsi dengan format file document (doc) pada Tabel 7.

Tabel 7. Hasil Pengunaan Memory Format DOC

Ukuran File (Kb)	Penggunaan Memory (Kb)		
	AES 128 (Kb)	DES 64 (Kb)	Blowfish 64 (Kb)
100	442.471	312.238	311.328
200	591.972	555.532	551.632
300	891.289	853.871	823.328
400	1396.235	1200.471	1096.400
500	1676.288	1576.288	1376.288
600	1955.244	1865.144	1665.744
700	2172.432	2067.725	1967.472
800	2586.562	2386.372	2286.472
900	2804.021	2702.059	2504.048
1000	2915.125	2845.275	2715.680

Pengujian kapasitas penggunaan memori dilakukan agar dapat mengetahui seberapa besar memori yang dibutuhkan selama proses enkripsi yang terjadi di server. Pengujian ini menggunakan 10 sampel file dengan format .doc mulai dari ukuran file 100 kb sampai 1000 kb.

Berdasarkan data Tabel 7, terdapat hasil kapasitas penggunaan memori untuk masing-masing algoritma dari AES, DES, dan blowfish. Hasil yang didapatkan dari rata-rata kapasitas memori menunjukkan bahwa AES membutuhkan kapasitas memori 4.34% lebih besar daripada Blowfish, sementara DES membutuhkan kapasitas memori 2,17% daripada Blowfish. Gambar 7 menunjukkan grafik perbandingannya.



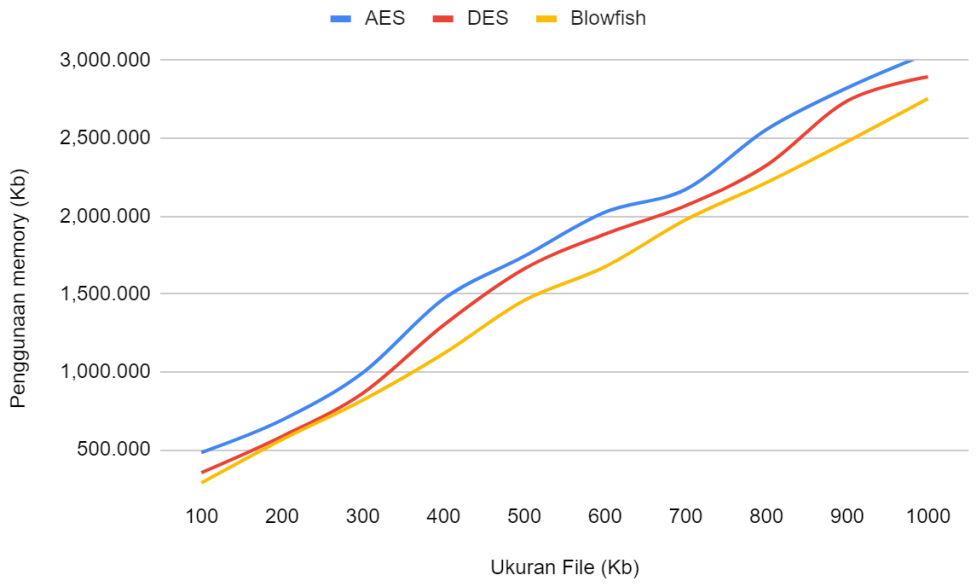
Gambar 7. Grafik Pengujian Kapasitas Memori Format DOC

Pengujian kapasitas penggunaan memori dilakukan agar dapat mengetahui seberapa besar memori yang dibutuhkan selama proses enkripsi yang terjadi di server. Pengujian ini menggunakan 10 sampel file dengan format .doc mulai dari ukuran file 100 kb sampai 1000 kb.

Berdasarkan data Tabel 8 , terdapat hasil kapasitas penggunaan memori untuk masing-masing algoritma dari AES, DES, dan blowfish. Hasil yang didapatkan dari rata-rata kapasitas memori menunjukkan bahwa AES membutuhkan kapasitas memori 5.30% lebih besar daripada Blowfish, sementara DES membutuhkan kapasitas memori 2,65% daripada Blowfish. Gambar 8 menunjukkan grafik perbandingannya.

Tabel 8. Hasil Pengunaan Memory Format PDF

Ukuran File (Kb)	Penggunaan Memory (Kb)		
	AES 128 (Kb)	DES 64 (Kb)	Blowfish 64 (Kb)
100	482.471	352.702	287.312
200	691.045	585.784	565.168
300	994.882	863.138	818.832
400	1468.538	1300.316	1116.944
500	1742.865	1662.054	1459.024
600	2025.478	1885.135	1675.232
700	2172.432	2067.725	1977.136
800	2556.623	2326.324	2215.568
900	2824.148	2740.594	2479.328
1000	3045.172	2895.265	2755.088



Gambar 8. Grafik Pengujian Kapasitas Memori Format PDF

Secara umum terlihat bahwa dari segi performansi DES lebih cepat dibandingan AES dan Blowfish, hal ini terjadi karena size Algoritma DES menggunakan ukuran blok 64 bit dan ukuran kunci 56 bit yang lebih rendah jika dibandingkan dengan kunci AES yang menggunakan ukuran blok 128 bit dan ukuran kunci 128 bit sedangkan Blowfish menggunakan ukuran blok 64 bit dan ukuran kunci 32 bit hingga 448 bit. Dari segi kebutuhan kapasitas memori, Blowfish membutuhkan kapasitas memori yang lebih tinggi jika dibandingkan dengan AES, namun perbedaan tersebut tidak terlalu signifikan jika dibandingkan dengan DES. Hal ini terjadi karena ukuran blok yang digunakan untuk pemrosesan data sama sama 64 bit antara Blowfish dan AES.

SIMPULAN DAN SARAN

Simpulan

Algoritma AES, DES dan Blowfish sudah berhasil diterapkan untuk proses enkripsi dan dekripsi file dari format doc dan pdf. Berdasarkan hasil pengujian perfomansi menunjukkan bahwa algoritma DES rata-rata 8.35% lebih cepat daripada AES dan perfomansi algoritma Blowfish lebih cepat 7.11% daripada algoritma AES. Hasil performansi DES lebih cepat dari AES karena pengaruh dari bit algoritma. Berdasarkan hasil pengujian kapasitas penggunaan *memory* menunjukkan bahwa algoritma AES membutuhkan kapasitas memori 4.82% lebih besar daripada Blowfish dan algoritma DES membutuhkan kapasitas memori 2.41% lebih besar daripada algoritma Blowfish. Algoritma DES dapat menjadi opsi terbaik untuk enkripsi dan dekripsi dari sisi performansi dibandingkan dengan AES dan Blowfish. Sementara itu, kebutuhan kapasitas memori disarankan menggunakan Blowfish daripada AES maupun DES.

Saran

Penelitian ini masih belum membutuhkan pengembangan sistem lebih lanjut. Oleh karena itu, diharapkan penelitian selanjutnya dapat mengembangkan ukuran kapasistas file lebih dari 1000 kilobytes dan variasi jenis file yang digunakan, seperti gambar, video, dan lainnya.

DAFTAR RUJUKAN

[1] M. Khairul and R. Jefril, "Analysis and Design of File Security System AES (Advanced Encryption Standard) Cryptography Based," *JAETS (Journal of Applied Engineering and Technological Science)*., vol. 1, no. 2, pp. 113-123, 2020.

[2] S. Shuzhou, M. Hui, S. Zishuai, Z. Rui, "WebCloud: Web-Based Cloud Storage for Secure Data Sharing across Platforms," *IEEE Transactions on Dependable and Secure Computing.,* pp. 1545-5971, 2020.

[3] Sheeja, Bibin, Priya, and Nishanth, "Secure File Sharing System in Cloud Using AES and Time Stamping Algorithms," *IOP Conf. Ser.*, pp. 906, 2020, doi: 10.1088/1757-899X/906/1/012023.

[4] Esther, Prasad, and Kumar, "Analysis of Cryptography Encryption for Network Security," *IOP Conf. Ser.,* pp. 981, 2020, doi: 10.1088/1757-899X/981/2/022028.

[5] P. Kuntal, "Performance analysis of AES, DES, and Blowfish cryptographic algorithms on small and large data files," *Int. J.Inf. Technol*., 2020, doi: 10.1007/s41870-018-0271-4

[6] G. Archisman, "Comparison of Encryption Algorithms: AES, Blowfish and Twofish for Security of Wireless Networks," *IRJET*., vol. 7, no. 6, pp. 4656-4659, 2020.

[7] H. Taufik and M. Rahutomo, "A Systematic Literature Review Method on AES Algorithm Data Sharing Encryption On Cloud Computing," *International Journal Of Artificial Intelegence Research*., vol. 4, no. 1, pp. 49-57, 2020.

[8] V. Akshitha, R. Sai, N. Shaik, and Ravindra, "An Efficient Optimization and Secured Triple Data Encryption Standard Using Enhanced Key Scheduling Algorithm," *Elsevier B.V*., 2020, doi: 10.1016/j.procs.2020.04.113.

[9] Y. Wang and Y. Li, "Improved Design of DES Algorithm Based on Symmetric Encryption Algorithm," *IEEE*., 2021, doi: 10.1109/ICPECA51329.2021.9362619.

[10] D.G Jatin, K.S. Adarsh, and P.S. Nipun, "Comparative Study on Different Encryption and Decryption Algorithm," *ICACITE*., 2021, doi: 10.1109/ICACITE51222.2021.9404734.

[11] A. Haneen and Alenezi, "Performance Evaluation of Cryptographic Algorithms: DES, 3DES, Blowfish, Twofish, and Threefish," *IJCNIS*., vol. 14, no. 1, 2022.

[12] P. Pooja and B. Rajesh, "Performance Evaluation of Hybrid Cryptography Algorithm for Secure Sharing of Text and Images," *IRJET*., vol. 7, pp. 3773-3778, 2020.

[13] Logunleko, Adeniji and A. Logunleko, "A Comparative Study of Symmetric Cryptography Mechanism on DES, AES and EB64 for Information Security," *IJSRCSE*., vol. 8, pp. 45-51, 2020.

[14] L. Thomas and C. Codrin, "Contract cheating by STEM students through a file sharing website: a Covid-19 pandemic perspective," *International Journal for Educational Integrity*., 2021, doi: 10.1007/s40979-021-00070-0.

[15] C. Daniel, G.K. Selorm and D.G. James, "Performance comparison of 3DES, AES, Blowfish and RSA for Dataset Classification and Encryption in Cloud Data Storage," *IJCA*., vol. 177, no. 40, 2020.

[16] R. Lavanya and M. Karpagam, "Enhancing the security of AES through small scale confusion operations for data communication," *Elsevier B.V*., 2020, doi: 0.1016/j.micpro.2020.103041.

[17] D. Roza and S. Mohsen, "Secure Socket Layer in the Network and Web Security," *International Journal of Computer and Information Engineering*., vol. 14, no. 10, 2020.

[18] S. Bijeta, D. Surjeet, J. Vivek, L. Dac-Nhuong, M. Senthilkumar and S. Gautam, "Integrating encryption techniques for secure data storage in the cloud," *Trans Emerging Tel Tech.*, 2020, doi: 10.1002/ett.4108.