Jurnal Inovasi Teknologi dan Komputer

Volume 02 | Number 01 | 2024
E-ISSN : 3026-5916 | Homepage : https://doi.org/10.54209/jitko.v2i01.136

Analisis Kerja dan Keamanan Algoritma Enkripsi AES pada Protokol SSH di Debian Server

Erick Simanjuntak[1], Yebi Susani Rajagukguk[2], Vicky Andreas Nainggolan[3], Oloan R Simanjuntak[4]

[1,2,3,4]Teknik informatika, Universitas Katolik Santo Thomas, Medan, Sumatera Utara, Indonesia

Article Info

Keywords:

Analisis Kerja dan Keamanan Algoritma Enkripsi AES pada Protokol SSH di Debian Server

ABSTRACT

Penelitian ini bertujuan untuk menganalisis kinerja dan keamanan algoritma enkripsi Advanced Encryption Standard (AES) pada protokol Secure Shell (SSH) di server berbasis Debian. Metode yang digunakan adalah pendekatan kuantitatif eksperimental melalui pengujian langsung terhadap tiga varian AES, yaitu AES-128-CTR, AES-192-CTR, dan AES-256-CTR. Parameter yang diuji meliputi waktu koneksi, kecepatan transfer data, dan penggunaan CPU. Hasil penelitian menunjukkan bahwa AES-192-CTR memiliki waktu koneksi tercepat sebesar 1,908 detik, sedangkan AES-128-CTR menghasilkan kecepatan transfer tertinggi sebesar 130,2 MB/s dengan waktu transfer 42,242 detik. Di sisi lain, AES-256-CTR memiliki tingkat keamanan paling tinggi, namun membutuhkan sumber daya CPU terbesar hingga 51,7%. Dengan demikian, terdapat trade-off antara performa dan keamanan, di mana pemilihan algoritma harus disesuaikan dengan kebutuhan sistem.

Corresponding Author:
Erick Simanjuntak
Teknik informatika, Universitas Katolik Santo Thomas, Medan, Sumatera Utara, Indonesia
Email: eric juntak@gmail.com

PENDAHULUAN

Di perkembangan jaman sekarang ini, Keamanan data menjadi sangat penting di era digital. Dan dari sekian banyak nya solusi cara yang paling efektif untuk melindungi data yaitu dengan Enkripsi, adapun enkripsi ialah mengubah informasi menjadi kode yang tidak dapat dibaca tanpa kunci yang tepat. Adapun algoritma Enkripsi yang banyak digunakan banyak orang atau sebagai energi yang diigunakan karena keamanan nya yang tinggi dan sangat efesien yaitu algoritma Advanced Encryption Standard (AES).(Henry et al., 2016)

Secure Shell (SSH) Jaringan yang mengakses penggunaan dari jarak jauh dengan aman terkendali. SSH juga menggunakan Enksripsi untuk melindungi data yang ditransfer antara klien dan server. Dan penggunaan AES sebagai Enkripsi dalam SSH sangat penting untuk menjaga kerahasiaan data. Analisis berlanjut tentang bagaimana AES bekerja didalam SSH, serta kerentanannya didalam pengiriman data yang bersifat privasi dan juga pemahaman tentang cara mengamankan sistem pada debian.(Tohirin, 2020)(Firman et al., 2024)(R. Kristoforus JB, 2012)

Permasalahan utama dalam penelitian ini berangkat dari semakin meningkatnya kebutuhan akan keamanan data dalam komunikasi jaringan, khususnya pada akses

jarak jauh melalui protokol Secure Shell (SSH). Meskipun SSH telah mengimplementasikan enkripsi untuk menjaga kerahasiaan data, pemilihan algoritma enkripsi yang tepat masih menjadi tantangan, terutama dalam menyeimbangkan antara tingkat keamanan dan performa sistem. Algoritma Advanced Encryption Standard (AES) memiliki beberapa varian kunci, yaitu AES-128, AES-192, dan AES-256, yang masing-masing menawarkan tingkat keamanan dan kebutuhan sumber daya yang berbeda. Namun, belum terdapat pemahaman yang komprehensif mengenai bagaimana perbedaan varian AES tersebut mempengaruhi kinerja SSH pada server berbasis Debian, baik dari sisi waktu koneksi, kecepatan transfer data, maupun penggunaan sumber daya sistem. Oleh karena itu, diperlukan analisis yang mendalam untuk mengidentifikasi varian AES yang paling optimal dalam konteks implementasi SSH, sehingga dapat memberikan rekomendasi yang tepat sesuai kebutuhan antara keamanan dan efisiensi sistem.

Penelitian ini memberikan kontribusi penting dalam bidang keamanan jaringan, khususnya pada implementasi algoritma enkripsi Advanced Encryption Standard (AES) dalam protokol Secure Shell (SSH) pada server berbasis Debian. Kontribusi utama penelitian ini adalah menyajikan analisis komprehensif terhadap kinerja dan tingkat keamanan dari tiga varian AES, yaitu AES-128, AES-192, dan AES-256, berdasarkan parameter waktu koneksi, kecepatan transfer data, serta penggunaan sumber daya CPU. Selain itu, penelitian ini juga memberikan perbandingan empiris yang diperoleh melalui pengujian langsung di lingkungan server, sehingga menghasilkan data yang lebih akurat dan relevan terhadap kondisi nyata. Hasil dari penelitian ini diharapkan dapat menjadi acuan praktis bagi administrator sistem dan peneliti dalam menentukan algoritma enkripsi yang paling sesuai dengan kebutuhan, baik yang berorientasi pada performa maupun pada tingkat keamanan yang tinggi. Dengan demikian, penelitian ini tidak hanya memperkaya kajian ilmiah terkait kriptografi jaringan, tetapi juga memberikan rekomendasi implementatif dalam pengamanan komunikasi data pada sistem berbasis Linux Debian.

METODE

Penelitian yang gunakan yaitu penelitan kuntitatif atau lebih tepatnya dengan metode pendekatan yaitu dengan lansung melakukan uji coba untuk menganalisis penggunaan algoritma AES (Advanced Encrytion Standard) terhadap kinerja dari protokol SSH pada sebuah server yang berbasis debian. Tujuannya antaralain untuk melakukan perbandingan dari tiga varian algoritma AES antarain yaitu AES(AES-128,AES-192, dan AES-256) untuk mengetahui seberapa efektif enkripsi yang digunakan dan seberapa baik performa dari algoritma tersebut.(Yuniati et al., 2011)(Syafaat & Finandhita, 2022)

Pendekatan Penelitian

Melalui penelitian yang menggunakan penelitan kuantitatif dengan experimentalnya, peneliti melakukan pengujian secara langsung pada server debian yang sudah di konfigurasi terlebih dahulu dengan protokol SSH dan algoritma AES. Hasil yang sudah di uji di catat dalam bentuk data numerik dan log sistemnya, setelah itu dilakukan analisis secara statistik-deskriptif.

Objek Penelitian

Objek yang di jadikan bahan penelitan adalah protokol SSHyang terdapat pada Debuian Server 10, dengan fokusnya pada implementasi algoritma AES sebagai kunci enkripsinya. Peneliti melakukan penelitian pada tiga varian algoritma AES yaitu, :

1. AES-192-CTR
2. AES-256-CTR
3. AES-128-CTR

Lingkungan Pengujian

Penelitian ini dilakukan di lingkungan yang telah dikonfigurasi atau lingkungan yang telah dipilih secara khusus untuk mendukung pengujian yang ingin dilakukan. Sistem yang digunakan adalah debian server(buster 10) yang memiliki peran sebagai server SSH.(Al Rivan et al., 2021). Perangkat yang digunakan yaitu open server SSH dan open SSH client untuk komunikasi SSHnya, ipertf untuk melakukan pengujian jaringan, htop untuk memantau sumberdaya yang akan digunakan, serta time untuk mencatat waktu yang digunakan dalam proses pengujian. (Tambunan & Neyman, 2024). Pengujian dijalankan di perangkat keras yaitu virtualBox dengan spesifikasi 2 core CPU , dengan RAM 2 GB dan penyimpanan 20 GB. Pengujian jaringan dilakukan pada koneksi internet lokal yang tersedia menggunaka LAN atau BRIGED NETWORK untuk hasil yang maksimal.(Pratama et al., 2020)

HASIL DAN PEMBAHASAN

Penelitian ini dilakukan untuk menganalisis kinerja dan keamanan tiga varian algoritma enkripsi AES (, AES-192, dan AES-256) yang digunakan dalam protokol SSH pada sistem operasi Debian Server. Pengujian dilakukan terhadap beberapa parameter: waktu koneksi, penggunaan CPU dan memori, kecepatan transfer data, dan keamanan transmisi data. Masing-masing pengujian dilakukan secara berulang untuk menjamin validitas data.(May Sarah Sianturi et al., 2020)

Pengujian Kinerja SSH

Waktu Koneksi SSH

Pengujian ini dilakukan untuk mengetahui seberapa cepat klien dapat membangun koneksi SSH ke server menggunakan masing-masing algoritma enkripsi. Pengujian dilakukan dengan mencatat waktu dari perintah dieksekusi hingga berhasil masuk ke server. Berikut adalah hasil dan tabel pengujian yang sudah diuji.

Tabel 1. Waktu Koneksi

NO	CHIPHER	PANJANG KUNCI	MODE	WAKTU KONEKSI
1	AES-128-CTR	128- BIT	CTR	4.732 DETIK
2	AES-192-CTR	192- BIT	CTR	1.908 DETIK
3	AES-256-CTR	256- BIT	CTR	2.121 DETIK

```
root@debian:~# time ssh -c aes256-ctr root@192.168.50.2 "exit"
root@192.168.50.2's password:

real    0m4.732s
```

Gambar 1. Hasil pengujian pada AES256-CTR

```
root@debian:~# time ssh -c aes128-ctr root@192.168.50.2 "exit"
root@192.168.50.2's password:

real    0m1.908s
```

Gambar 2. Hasil pengujian pada AES128-CTR

```
root@debian:~# time ssh -c aes192-ctr root@192.168.50.2 "exit"
root@192.168.50.2's password:

real    0m2.121s
```

Gambar 3. Hasil pengujian pada AES192-CTR

Dari hasil pengujian diata disitu menunjukkan bahwa AES192 Lebih cepat terkoneksi dari pada AES yang lainnya maka dari itu dapat diambil kesimpulan bahwa kinerja AES192 Lebih cepat dari pada AES128 Dan AES256.

Kecepatan Transfer file

Waktu transfer file diukur menggunakan perintah time yang dikombinasikan dengan scp, yaitu dengan format time scp -c [cipher] file user@ip:/tujuan. Nilai yang digunakan adalah waktu real, yang menunjukkan lamanya proses transfer file dari awal hingga selesai. Pengukuran ini penting untuk melihat seberapa besar pengaruh algoritma enkripsi terhadap kecepatan pengiriman data melalui protokol SSH.dan berikut adalah hasil gambar dan tabel hasil pengujian yang lakukan.

ALGORITMA AES	UKURAN FILE	LAMA TRANSFER(REAL)	KECEPATAN(MB/S
AES-128-CTR	5 GB	42.242 DETIK	130.2 MB/S
AES-192-CTR	5 GB	46.818 DETIK	115.1 MB/S
AES-256-CTR	5 GB	51.358 DETIK	106.9 MB/S

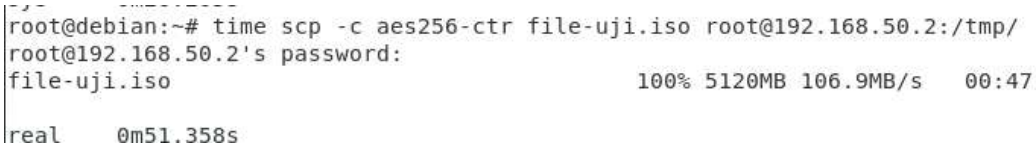
Berikut adalah gambar hasil pengujian transfer file Yang lakukan

```
root@debian:~# time scp -c aes128-ctr file-uji.iso root@192.168.50.2:/tmp/
root@192.168.50.2's password:
file-uji.iso                                  100% 5120MB 130.2MB/s   00:39

real    0m42.242s
```

Gambar 4. Hasil pengujian trasfer filepada AES128-CTR

```
root@debian:~# time scp -c aes192-ctr file-uji.iso root@192.168.50.2:/tmp/
root@192.168.50.2's password:
file-uji.iso                                  100% 5120MB 115.1MB/s   00:44

real    0m46.818s
```

Gambar 5. Hasil pengujian trasfer filepada AES192-CTR



Gambar 6. Hasil pengujian trasfer filepada AES256-CTR

Hasil pengujian menunjukkan bahwa semakin panjang kunci AES (misalnya dari AES-128 ke AES-256), maka tingkat keamanan meningkat karena ruang kunci yang lebih besar membuat cipher lebih tahan terhadap brute-force attack. Namun, peningkatan panjang kunci ini juga membawa konsekuensi, yaitu waktu transfer menjadi sedikit lebih lama, karena proses enkripsi dan dekripsi memerlukan lebih banyak siklus CPU. Selain itu, penggunaan CPU juga meningkat seiring dengan kompleksitas pengolahan cipher yang lebih kuat.

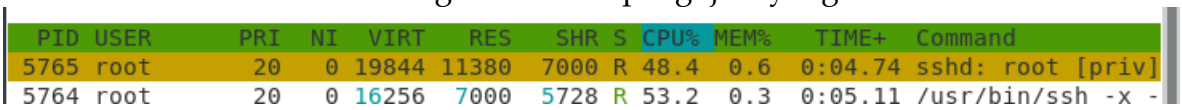
Dengan kata lain, ada trade-off antara keamanan dan performa. AES-128-CTR menawarkan kecepatan transfer dan efisiensi CPU terbaik, tetapi dengan kekuatan kriptografi yang lebih rendah. Sebaliknya, AES-256-CTR memberikan keamanan maksimal, namun lebih membebani sistem dari segi waktu dan sumber daya. Oleh karena itu, pemilihan cipher perlu disesuaikan dengan kebutuhan: apakah lebih menekankan pada performa atau pada tingkat keamanan data.

Pemakaian cpu saat transfer data

Tabel hasil pengamatan menunjukkan perbandingan penggunaan CPU dan waktu transfer file saat menggunakan tiga varian cipher AES, yaitu AES-128-CTR, AES-192-CTR, dan AES-256-CTR. Proses transfer dilakukan melalui perintah scp, dan pengamatan penggunaan CPU dilakukan secara langsung menggunakan alat bantu htop pada saat proses berlangsung.

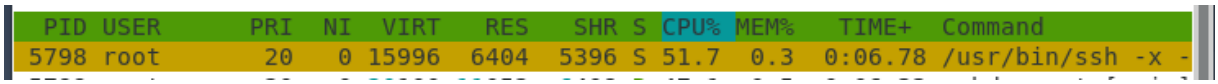
NO	CIPHER	PANJANG KUNCI	WAKTU TRANSFER	PENGGUNAAN CPU	KETERANGAN
1	AES-128-CTR	128 BIT	42.242 DETIK	48.2%	Penggunaan CPU cukup efisien
2	AES-192-CTR	192-BIT	46.818 DETIK	48.4%	CPU meningkat, performa tetap stabil
3	AES-256-CTR	256- BIT	51.358 DETIK	51.7%	CPU tinggi, proses enkripsi lebih berat

Berikut adalah gambar hasil pengujian yang lakukan



Gambar 7. Hasil pengujian pada AES 128

Gambar 8. Hasil pengujian pada AES 192



Gambar 9. Hasil pengujian pada AES 256

Dari data yang ditampilkan, dapat disimpulkan bahwa semakin panjang kunci cipher AES yang digunakan, maka penggunaan CPU juga meningkat. Pada saat menggunakan AES-128-CTR, proses enkripsi berlangsung cukup ringan, ditunjukkan dengan penggunaan CPU sebesar 48.2% dan waktu transfer selama 42 detik. Ketika beralih ke AES-192-CTR, terjadi peningkatan penggunaan CPU menjadi 48.4%, dengan waktu transfer juga sedikit lebih lama, yaitu 46 detik. Sedangkan saat menggunakan AES-256-CTR, penggunaan CPU mencapai 51.7, dan waktu transfer menjadi yang paling lambat, yakni 51 detik. Hal ini menunjukkan bahwa cipher AES dengan panjang kunci yang lebih besar membutuhkan lebih banyak sumber daya CPU untuk melakukan proses enkripsi dan dekripsi data. AES-256 menawarkan tingkat keamanan yang lebih tinggi secara teoritis, namun memberikan beban yang lebih besar terhadap sistem. Sebaliknya, AES-128 cukup efisien dan cepat, meskipun tingkat keamanannya lebih rendah dibandingkan AES-256. Dengan demikian, pemilihan cipher perlu mempertimbangkan keseimbangan antara kebutuhan keamanan dan performa sistem. Jika server memiliki spesifikasi CPU rendah atau transfer file dilakukan secara masif dan berkelanjutan, penggunaan AES-128 dapat lebih menguntungkan dari sisi performa. Namun, jika keamanan menjadi prioritas utama dan sistem mendukung beban CPU yang tinggi, maka AES-256 adalah pilihan yang tepat.

KESIMPULAN

Berdasarkan hasil penilitian dan yang telah diuji,dapat disimpulkan bahwa penerapan algoritma enkripsi Advance(AES) pada protocol Secure shell(SSH) di server Debian 10 telah terbukti mampu menjaga keamanan dan kerahasiaan data dalam komunikasi jaringan.Dari hasil pengujian ini ,terlihat bahwa ada perbedaan kinerja di setiap varian AES yang digunakan.AES-128-CTR menunjukkan bahwa kinerja ini bagus dalam hal transfer data,sedangkan AES-192-CTR bagus dalam keepatan koneksi dari varian AES lainnya.sedangkan AES-256-CTR lebih aman dari varian lainnya meskipun harus membutuhkan daya sistem yang lebih besar. Oleh karena itu, Keputusan untuk memilih algoritma AES yang akan diterapkan dalam SSH harus bergantung pada kebutuhan atau ketahanan sistem.Jadi jika sistem harus membutuhkan atau bergantung pada kinerja dan sumber daya dan ketahanan sitem, maka AES-128-CTR direkomendasikan untuk sistem tersebut. Di sisi lain, jika sistem bergantung pada keamanan data,maka AES-256-CTR direkomendasikan meskipun membutuhkan lebih banyak sumber daya.

DAFTAR PUSTAKA

Al Rivan, M. E., Arman, M., & Irsyad, H. (2021). Pelatihan Troubleshooting Instalasi Linux Debian Di SMK Negeri 5 Palembang. Fordicate, 1(1), 25–33.

Az Zahra, D. R., Ilham, F. P., Ramdhani, H. N., & Setiawan, A. (2024). Penerapan dan Pengujian Keamanan SSH Pada Server Linux menggunakan Hydra. Journal of Internet and Software Engineering, 1(3), 10. https://doi.org/10.47134/pjise.v1i3.2627

Firman, F., Astuti, A. D., & Matahari, M. (2024). Pengembangan Modul Praktikum Adminsitrasi Server Menggunakan Linux Debian 10 Pada Kelas 11 Tkj Development of Server Administration Practicum Module. Bitnet: Jurnal Pendidikan Teknologi Informasi, 9(1), 47–57. https://doi.org/10.33084/bitnet.v9i1.6326

Henry, Kridalaksana, A. H., & Arifin, Z. (2016). Kriptografi Aes Mode Cbc Pada Citra Digital Berbasis Android. Seminar Ilmu Komputer Dan Teknologi Informasi, 1(1), 45–52.

May Sarah Sianturi, N., Budi Nugroho, N., & Rista Maya, W. (2020). Implementasi Kriptografi Untuk Pengamanan Data Aset Perusahaan Pada PT.PLN (Persero) Dengan Menggunakan Metode Algoritma AES 192. Jurnal CyberTech, x. No.x(x).

Pratama, R., Orisa, M., & Ariwibisono, F. (2020). Aplikasi Monitoring Dan Controlling Server Menggunakan Protocol Icmp (Internet Control Message Protocol) Dan Ssh (Secure Shell) Berbasis Website. JATI (Jurnal Mahasiswa Teknik Informatika), 4(1), 397–403. https://doi.org/10.36040/jati.v4i1.2310

Putra, Y., Yuhandri, Y., & Sumijan, S. (2021). Meningkatkan Keamanan Web Menggunakan Algoritma Advanced Encryption Standard (AES) terhadap Seragan Cross Site Scripting. Jurnal Sistim Informasi Dan Teknologi, 56–63. https://doi.org/10.37034/jsisfotek.v3i2.44

R. Kristoforus JB, S. A. B. (2012). Implementasi Algoritma Rijndael untuk Enkripsi dan Dekripsi pada Citra Digital. Seminar Nasional Aplikasi Teknologi Informasi 2012, 2012(Snati), 15–16.

Syafaat, F., & Finandhita, A. (2022). Implementasi Kriptografi Aes-128 Pada Unmanned Aerial Vechile Dan Ground Control System.

Tambunan, M. R. H., & Neyman, S. N. (2024). Implementasi Firewall pada Linux untuk Pencegahan Dari Serangan DoS. Journal of Technology and System Information, 1(4), 10. https://doi.org/10.47134/jtsi.v1i4.2648

Tohirin, T. (2020). Penerapan Keamanan Remote Server Melalui Ssh Dengan Kombinasi Kriptografi Asimetris Dan Autentikasi Dua Langkah. Jurnal Teknologi Informasi, 4(1), 133–138. https://doi.org/10.36294/jurti.v4i1.1262

Yuniati, V., Indriyanta, G., & Rachmat C., A. (2011). Enkripsi Dan Dekripsi Dengan Algoritma Aes 256 Untuk Semua Jenis File. Jurnal Informatika, 5(1). https://doi.org/10.21460/inf.2009.51.69

Santria, U. & Arsoetar, N. (2017). Penggunaan Enkripsi End-to-End dalam Pengamanan Pesan dan Video Call pada Whatsapp.

Rodríguez, J., Sánchez, P., & García, M. (2021). Testing encryption algorithms: A focus on black-box testing methodologies. Software Testing, Verification & Reliability, 31(8), 1485–1498. https://doi.org/10.1002/stvr.1867.

Heiter, C. (2009). American Boarding Schools: The American Boarding School Experience. ThingsAsian Press.