Journal of Information Technology and Computer Science (INTECOMS)
Volume 7 Nomor 4, Tahun 2024
e-ISSN : 2614-1574
p-ISSN : 2621-3249

TEKNIK PENGAMANAN DATA MENGGUNAKAN ALGORITMA *ADVANCE ENCRYPTION STANDARD* DENGAN *COMMON EVENT FORMAT* UNTUK MENINGKATKAN KEAMANAN LOG JARINGAN

DATA SECURITY TECHNIQUES USING ADVANCE ENCRYPTION STANDARD ALGORITHM WITH COMMON EVENT FORMAT TO IMPROVE NETWORK LOG SECURITY

Moch. Dzikri Azhari Ali[1], Asep Id Hadiana[2], Melina[3]
[1, 2, 3]Program Studi Informatika, Fakultas Sains dan Informatika, Universitas Jenderal Achmad Yani
mochdzikriazhari20@if.unjani.ac.id

ABSTRACT

Rapid developments in information technology demand more protection of data security and data exchange in the digital world. Security threats on the network can occur from various sources so that techniques are needed to protect information that moves between interconnected computer networks. Network log security is a very important step to strengthen network security. Network logs are records or recordings of activities that occur within a computer network, including information such as unauthorized access attempts, user activity, and other important events. This research aims to evaluate how effective the use of the Advanced Encryption Standard (AES) algorithm is in securing network log data by using encryption and decryption methods with the application of the Common Event Format (CEF) to increase the security of network log data encrypted in CEF. The AES algorithm is a chiper to maintain data confidentiality and integrity. Meanwhile, CEF serves to simplify the process of recording security-related events and to combine various logs from various sources into one system. This research is to make an important contribution to the development of more effective security techniques on network log data.

Keywords: *AES, CEF, decryption, encryption, network logs*

ABSTRAK

Perkembangan pesat dalam teknologi informasi menuntut perlindungan yang lebih terhadap keamanan data dan pertukaran data dalam dunia digital. Ancaman keamanan pada jaringan dapat terjadi dari berbagai sumber sehingga perlu teknik untuk melindungi informasi yang berpindah antar jaringan komputer yang saling terhubung. Keamanan log jaringan menjadi langkah yang sangat penting untuk memperkuat keamanan jaringan tersebut. Log jaringan adalah catatan atau rekaman aktivitas yang terjadi di dalam jaringan komputer, mencakup informasi seperti percobaan akses tidak sah, aktivitas pengguna, dan peristiwa penting lainnya. Penelitian ini bertujuan untuk mengevaluasi seberapa efektif penggunaan algoritma *Advanced Encryption Standard* (AES) dalam mengamankan data log jaringan dengan menggunakan metode enkripsi dan dekripsi yang menerapkan *Common Event Format* (CEF) untuk meningkatkan keamanan data log jaringan yang dienkripsi pada CEF. Algoritma AES merupakan sebuah *chiper* untuk menjaga kerahasiaan dan integritas data. Sedangkan, CEF berfungsi untuk menyederhanakan proses pencatatan peristiwa yang terkait dengan keamanan serta untuk menggabungkan beragam log dari berbagai sumber ke dalam satu sistem. Penelitian ini dapat memberikan kontribusi penting dalam pengembangan teknik keamanan yang lebih efektif pada data log jaringan.

Kata Kunci: AES, CEF, dekripsi, enkripsi, log jaringan

PENDAHULUAN

Seiring dengan perkembangan teknologi informasi yang selalu berubah menyebabkan keamanan suatu informasi sangatlah penting, terutama pada jaringan yang terkoneksi dengan internet. Namun, adanya ketidakseimbangan antara perkembangan teknologi tetapi tidak diikuti dengan perkembangan pada sistem keamanan itu sendiri, menyebabkan cukup banyak sistem-sistem yang lemah dan harus ditingkatkan keamanannya(Akhriana & Irmayana, 2019). Lemahnya keamanan di internet dapat meningkatkan risiko pencurian data yang terdapat dalam sistem internet oleh pihak-pihak yang tidak bertanggung jawab. Pencurian data dalam suatu sistem di internet disebut sebagai kasus kejahatan komputer. *Cybercrime* adalah istilah untuk mendeskripsikan

kejahatan yang terjadi di internet(Nyoman Putri Purnama Santhi & Nengah Nuarta, 2023). Menurut Deep Instinct, terjadi peningkatan serangan siber menggunakan malware sebesar 358% pada tahun 2020 dibandingkan tahun 2019. Sementara, ransomware mengalami peningkatan sebanyak 435% pada tahun 2020 dibandingkan tahun sebelumnya(Budi et al., 2021). Fenomena ini juga tercermin di Indonesia, di mana sejak tahun 2019, Kementerian Komunikasi dan Informatika (Kominfo) mencatat sebanyak 29 lembaga dan perusahaan menjadi korban kejahatan siber berupa kebocoran data. Dari puluhan kasus tersebut, 21 di antaranya telah diselesaikan oleh Kominfo. Data Kominfo menunjukkan bahwa 29 kasus kebocoran data ini disebabkan oleh sistem keamanan yang rawan diretas (Samad & Persadha, 2022). Serangan siber dapat memberikan kerugian finansial besar, kehilangan data, dan merusak reputasi (Laksana & Mulyani, 2024). Meningkatnya frekuensi dan kompleksitas serangan siber, yang dapat terjadi kapan memerlukan sistem keamanan yang mampu mendeteksi serangan (Alamsyah et al., 2020). Keamanan log jaringan merupakan langkah yang sangat penting untuk memperkuat keamanan jaringan (Lantz, 2006).

Salah satu aspek penting dari sistem keamanan adalah log jaringan yang memiliki peran penting untuk memantau keamanan sistem informasi, namun seringkali diabaikan. Log jaringan adalah catatan atau rekaman aktivitas yang terjadi di dalam jaringan komputer, mencakup informasi seperti percobaan akses tidak sah, aktivitas pengguna, dan peristiwa penting lainnya. Log jaringan dapat mendeteksi dan merespons serangan, dan memantau kesehatan jaringan sehingga perlu adanya strategi yang cukup untuk melindungi data log jaringan (Ramli, 2023).

Teknik kriptografi, seperti enkripsi, merupakan salah satu metode untuk menjaga keamanan data dengan mengubah *plainteks* menjadi *cipherteks* yang tidak terbaca oleh pihak yang tidak berwenang (Putra et al., 2023). Kriptografi merupakan studi matematis yang bertujuan untuk melindungi sistem informasi dengan memastikan kerahasiaan, integritas data, autentikasi, dan mencegah penyangkalan (Ismadiah et al., 2020). Terdapat berbagai teknik kriptografi untuk menyandikan pesan atau data informasi, diantaranya adalah teknik subtitusi dan permutasi. Salah satu metode kriptografi yang memanfaatkan keduanya adalah algoritma *Advanced Encryption Standard* (AES) (Bhaudhayana, 2018).

Penerapan enkripsi pada log jaringan dapat memberikan tingkat perlindungan yang tinggi. Proses enkripsi membuat log jaringan sulit dibaca atau dimanipulasi oleh pihak yang tidak berwenang, sehingga seorang peretas akan kesulitan membaca atau melakukan perubahan signifikan pada log jaringan tanpa memiliki kunci enkripsi yang sesuai (Lantz, 2006). Selain itu, dalam konteks keamanan jaringan, *Common Event Format* (CEF) digunakan sebagai format pencatatan yang telah diakui dalam industri, yang memungkinkan data untuk diinterpretasikan dengan mudah dan dapat diimplementasikan oleh perangkat keamanan (More et al., 2020).

Beberapa penelitian terdahulu yang mengkaji tentang penerapan enkripsi yaitu penelitian (Lantz, 2006), yang menerapkan enkripsi pada log jaringan sehingga dapat memberikan tingkat perlindungan yang tinggi. Proses enkripsi membuat log jaringan sulit dibaca atau dimanipulasi oleh pihak yang tidak berwenang, sehingga seorang peretas akan kesulitan membaca atau melakukan perubahan signifikan pada log jaringan tanpa memiliki kunci enkripsi yang sesuai. Penelitian (Gabriel, 2022), menerapkan algoritma AES untuk mengamankan log file menjadi sorotan utama. Menurut penelitian ini, penggunaan algoritma AES pada log file dinilai sebagai isu yang signifikan dan semakin menjadi perhatian

bagi individu maupun organisasi. Oleh karena itu, algoritma AES dijadikan solusi untuk mengamankan log tersebut. Melalui penggunaan algoritma AES, data log dapat dienkripsi dengan kuat, memberikan jaminan terhadap kerahasiaan serta integritasnya. Algoritma AES yang digunakan dalam mengamankan log file memiliki peran penting dalam menjaga keamanan dan integritas data log. Selanjutnya penelitian (Manullang, 2023), yang menggunakan algoritma AES dengan mode *Cipher Block Chain* (CBC). Penyandian data dilakukan dengan menggunakan kunci 128 bit atau setara dengan 16 karakter. Hal ini menghasilkan *ciphertext*, hasil dari enkripsi yang terdiri dari karakter atau simbol-simbol unik, yang membuat pesan atau informasi sulit dibaca atau dipahami. Proses dekripsi diperlukan untuk mengembalikan pesan ke bentuk aslinya.

Berdasarkan penjelasan diatas, telah ada penelitian terdahulu yang mengkaji penerapan enkripsi pada log jaringan, seperti penelitian (Lantz, 2006), yang mengkaji enkripsi umum secara umum tetapi tidak ada pembahasan secara spesifik tentang integrasi enkripsi dengan format log yang terstandarisasi. Penelitian (Bhaudhayana, 2018), menggunakan algoritma AES tetapi tetapi tidak menjelaskan kebutuhan akan format log yang terstruktur dan terstandarisasi. Penelitian (More et al., 2020), telah menerapkan AES dengan mode *Cipher Block Chain* (CBC), namun belum mengintegrasikannya dengan format log yang terstruktur. Oleh karena itu, penelitian ini mengusulkan pendekatan baru dengan mengkombinasikan algoritma enkripsi AES dan CEF untuk melindungi log jaringan dan menyediakan format log yang terorganisir sebagai perlindungan tambahan dari serangan siber yang mau mencuri atau memanipulasi data log jaringan. Diharapkan hasil penelitian ini dapat memberikan kontribusi yang lebih efektif pada keamanan data log jaringan.

TINJAUAN PUSTAKA

Tinjauan Pustaka menguraikan mengenai pengertian dan definisi yang diambil dari penelitian terdahulu serta beberapa literatur review yang berhubungan dengan topik penelitian.

Kriptografi

Kriptografi adalah disiplin ilmu yang memfokuskan pada teknik-teknik penyandian tertentu yang digunakan untuk memastikan keamanan pesan atau data saat proses pengiriman, dengan tujuan untuk mencegah informasi dalam pesan atau data tersebut dari dimanipulasi oleh pihak yang tidak berwenang (Permana, 2018).

Algoritma *Advanced Encryption Standard* (AES)

Algoritma AES merupakan suatu *chiper* yang aman digunakan untuk melindungi data atau informasi yang bersifat rahasia. Algoritma ini menggunakan pendekatan simetris dengan penerapan kunci yang sama pada proses enkripsi maupun dekripsi. AES diperkenalkan oleh *National Institute of Standard and Technology* (NIST) pada tahun 2001 sebagai pengganti algoritma DES yang sudah berakhir masa penggunaannya dan dianggap sudah usang serta rentan terhadap serangan. Algoritma AES menggunakan input dan output berupa urutan data sebesar 128 bit, dikenal sebagai blok data atau *plaintext*. Blok data ini kemudian dienkripsi menjadi *chipertext* (Bhaudhayana, 2018).

Proses enkripsi dalam algoritma AES melibatkan empat jenis transformasi *bytes*, yaitu *SubBytes, ShiftRows, MixColumns,* dan *AddRoundKey* (Handoyo & Subakti, 2020).

Common Event Format (CEF)

CEF adalah standar pencatatan yang dikembangkan oleh ArcSight, perusahaan yang menyediakan solusi manajemen peristiwa dan keamanan informasi, yang dikenal sebagai *Security Information and Event Management* (SIEM). CEF berfungsi untuk menyederhanakan proses

pencatatan peristiwa yang terkait dengan keamanan serta untuk menggabungkan beragam log dari berbagai sumber ke dalam satu sistem. Penggunaan format data terstruktur oleh CEF memungkinkan pencatatan peristiwa dengan berbagai jenis dan tingkat keparahan. Kehadiran CEF sangat penting karena menciptakan format standar untuk mencatat peristiwa yang berkaitan dengan keamanan, memudahkan integrasi log dari berbagai sumber ke dalam satu sistem. CEF memberikan kemudahan dalam analisis, otomatisasi, serta identifikasi pola dan tren dalam data log dengan menggunakan format log yang terstandarisasi, yang membantu dalam pemecahan masalah dan analisis log (Watts, 2023).

Log File

Log file jaringan adalah salah satu alat yang efektif untuk mengamankan lalu lintas jaringan dari penyusupan. Log file dapat mencatat berbagai aspek lalu lintas jaringan, seperti alamat IP yang mencoba mengakses jaringan, port yang digunakan, waktu dan tanggal percobaan, dan informasi lainnya. Apabila digunakan dengan p tepat, log file dapat sangat membantu dalam menjaga keamanan dan integritas jaringan. Agar manfaatnya optimal, *logging* harus selalu diaktifkan dan log file harus diperiksa secara berkala sehingga dapat memberikan perlindungan yang efektif terhadap peretas.

METODE

Langkah-langkah penelitian yang dilakukan untuk melakukan pengamanan data pada log jaringan ditunjukkan pada Gambar 1.

Gambar 1. Metode Penelitian

Pengumpulan Data Log Jaringan:

Tahap pertama yang dilakukan adalah pengumpulan data log jaringan. Pada tahap ini, dibutuhkan contoh data log jaringan yang akan digunakan sebagai *input* dalam proses enkripsi dan dekripsi. Data log jaringan ini diperoleh dengan menggunakan aplikasi pihak ketiga yang bisa digunakan yaitu *wireshark*. Data yang dikumpulkan mencakup alamat IP sumber dan tujuan, port sumber dan tujuan dan lainnya. Pengumpulan data ini mencakup seluruh log jaringan yang dihasilkan oleh perangkat dalam suatu jaringan tertentu selama periode waktu tertentu, dengan menggunakan Wireshark.

Penerapan CEF:

Tahap selanjutnya adalah penerapan CEF yang merupakan kunci penting dalam membuat data log jaringan terstandarisasi dan terstruktur. Melalui penerapan CEF, format log jaringan dapat memberikan kemudahan dalam analisis sehingga dapat membantu dalam pemecahan masalah dan analisis log. Standarisasi format log ini tidak hanya meningkatkan efisiensi dalam membaca dan memahami data log, tetapi juga memfasilitasi pemecahan masalah dengan menyediakan kerangka kerja yang terstruktur. Penerapan CEF ini digunakan

untuk meningkatkan keamanan log jaringan secara keseluruhan.

Pada tahap ini, log yang dihasilkan dari file PCAP diubah ke dalam format CEF. Proses ini melibatkan ekstraksi informasi penting dari paket jaringan seperti IP sumber, IP tujuan, port sumber, dan port tujuan serta informasi lainnya. Hasil dari log yang dihasilkan dapat diubah ke dalam format CEF, sehingga ditampilkan dalam bentuk yang terstandarisasi dan terstruktur seperti yang terlihat pada contoh berikut:

CEF:0|MyCompany|MyProduct|1.0|200|UDP Traffic|3|src=74.125.200.95 dst=192.168.10.111 spt=443 dpt=63247 start=2024-06-02T14:54:32Z end=2024-06-02T14:54:32Z msg=UDP Traffic from 74.125.200.95 to 192.168.10.111 on ports 443->63247

Penjelasan untuk setiap bagian dalam format CEF diatas dapat dilihat pada Tabel 1.

Tabel 1. Penjelasan Label CEF

No	CEF Label	Deskripsi
1	CEF:0	Versi format CEF.
2	MyCompany	Nama vendor yang menghasilkan log.
3	MyProduct	Nama produk yang menghasilkan log.
4	1.0	Versi produk yang menghasilkan log.
5	200	ID tanda tangan acara.
6	UDP Traffic	Nama singkat atau deskripsi dari acara.
7	3	Tingkat keparahan acara.
8	src=74.125.200.95	Alamat IP sumber.
9	dst=192.168.10.111	Alamat IP tujuan.
10	spt=443	Port sumber.
11	dpt=63247	Port tujuan.
12	start=2024-06-02T14:54:32Z	Waktu mulai acara.
13	end=2024-06-02T14:54:32Z	Waktu berakhir acara.
14	msg=UDP Traffic from 74.125.200.95 to 192.168.10.111 on ports 443->63247	Pesan yang mendeskripsikan acara.

Penerapan CEF tidak hanya mempermudah analisis data log jaringan, tetapi juga mengoptimalkan keamanan informasi dengan menyediakan format yang terstruktur dan mudah dipahami.

Pemilihan Kunci Enkripsi:

Tahapan berikutnya adalah pemilihan kunci enkripsi yang merupakan tahap penting dalam proses keamanan data dengan menggunakan algoritma AES. Panjang kunci dalam AES bisa berbeda-beda, yaitu 128 bit, 192 bit, atau 256 bit. Variasi panjang kunci ini mempengaruhi jumlah putaran yang dilakukan dalam algoritma AES. Jumlah putaran dalam AES bervariasi tergantung pada panjang kunci yang digunakan, di mana setiap putaran membutuhkan kunci putaran dan input dari putaran sebelumnya. Algoritma ini memiliki tiga variasi jumlah putaran yang ditunjukkan dalam Tabel 2.

Tabel 2. Jumlah Putaran Kunci Pada AES

Tipe	Panjang Kunci	Jumlah Putaran
AES-128	128 bit	10
AES-192	192 bit	12
AES-256	256 bit	14

Dalam konteks ini, pemilihan kunci enkripsi harus memperhatikan panjang kunci yang sesuai dengan standar keamanan. Keberhasilan algoritma AES dalam memberikan tingkat keamanan yang tinggi sebagian besar bergantung pada kompleksitas kunci enkripsi yang digunakan. Pada tahap ini, panjang kunci yang optimal harus dipertimbangkan agar memberikan lapisan keamanan yang efektif terhadap potensi ancaman keamanan jaringan. Panjang kunci yang akan dipilih yaitu 16 karakter atau 128 bit dan kunci harus terdiri dari beberapa kombinasi seperti huruf besar, huruf kecil, angka, dan karakter khusus. Kombinasi ini memastikan tingkat kompleksitas yang tinggi, sehingga meningkatkan kesulitan

bagi pihak yang tidak berwenang untuk menebak atau memecahkan kunci tersebut. Penerapan panjang kunci dan kombinasi karakter dapat memberikan perlindungan yang lebih kuat terhadap ancaman keamanan jaringan.

Proses Enkripsi Data:

Tahap berikutnya adalah proses enkripsi data. Setelah kunci enkripsi dipilih dengan cermat, selanjutnya melibatkan implementasi algoritma AES untuk menjalankan proses enkripsi pada data log jaringan. Proses ini dilakukan dengan mengubah data log asli yang telah dilakukan penerapan format CEF (*plainteks*) menjadi bentuk terenkripsi (*cipherteks*) menggunakan kunci enkripsi yang telah ditentukan sebelumnya.

Proses enkripsi dalam algoritma AES melibatkan empat jenis transformasi *byte*: *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*. Pada awal enkripsi, input yang telah disalin ke dalam keadaan (*state*) akan mengalami transformasi *AddRoundKey* sebanyak Nr kali, sesuai dengan jumlah putaran dalam algoritma AES. Proses ini dikenal sebagai fungsi putaran (*round function*) dalam AES. Pada putaran terakhir, terdapat perbedaan di mana *state* tidak mengalami transformasi *MixColumns* (Handoyo & Subakti, 2020). Secara umum, enkripsi algoritma AES yang bekerja pada blok 128-bit dengan kunci 128-bit adalah sebagai berikut (Nurnaningsih & Permana, 2018):

1. *AddRoundKey*: Melakukan operasi XOR antara state awal (*plaintext*) dengan *cipher key*. Tahap ini disebut juga initial round.
2. Putaran sebanyak Nr-1 kali. Proses yang dilakukan pada setiap putaran adalah:
   a. *SubBytes*: Substitusi *byte* menggunakan tabel substitusi (*S-box*).
   b. ShiftRows: Pergeseran baris-baris *array state* secara *wrapping*.
   c. *MixColumns*: Mengacak data di kolom-kolom *array state*.
   d. *AddRoundKey*: Melakukan operasi XOR antara *state* dengan *round key*.
3. *Final round*: Proses untuk putaran terakhir, yang meliputi:
   a. Su*bBytes*
   b. *ShiftRows*
   c. *AddRoundKey*

Evaluasi dan Kesimpulan:

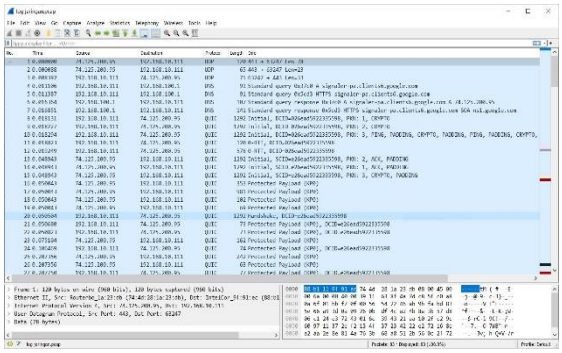
Tahap terakhir dari penelitian ini adalah evaluasi hasil dan penarikan kesimpulan berdasarkan proses enkripsi yang telah dilakukan. Selain itu, dilakukan juga pengujian pada penelitian ini yaitu dengan mengukur tingkat keamanan kunci yang digunakan dengan menggunakan *tool How Secure Is Your Password*. Diharapkan melalui metode penelitian ini dapat diperoleh pemahaman yang lebih mendalam mengenai seberapa efektifnya penggabungan algoritma AES dan format CEF dalam meningkatkan keamanan data log jaringan.

HASIL DAN PEMBAHASAN

Hasil dari penelitian ini berupa aplikasi web yang menunjukkan penerapan format CEF, enkripsi, dan dekripsi melalui langkah-langkah yang mudah digunakan. Proses ini meliputi pengunggahan file PCAP, konversi ke format CEF, enkripsi file, dekripsi file dan pengujian kunci dengan menggunakan *tool How Secure Is Your Password*.

Pengumpulan Data Log Jaringan

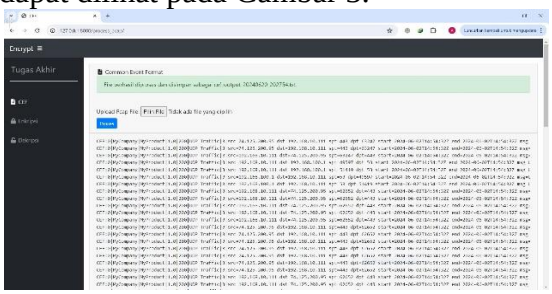
Proses pengumpulan data log jaringan dimulai dengan memilih antarmuka jaringan yang akan dipantau dan memulai penangkapan data. Semua paket data yang melewati antarmuka jaringan tersebut direkam, termasuk informasi penting seperti alamat IP sumber dan tujuan, port sumber dan tujuan, serta jenis protokol yang digunakan. Setelah periode pengumpulan data selesai, penangkapan dihentikan dan hasilnya disimpan dalam format PCAP (*Packet Capture*), yang dapat dilihat pada Gambar 2.



Gambar 2. Pengumpulan Log Jaringan

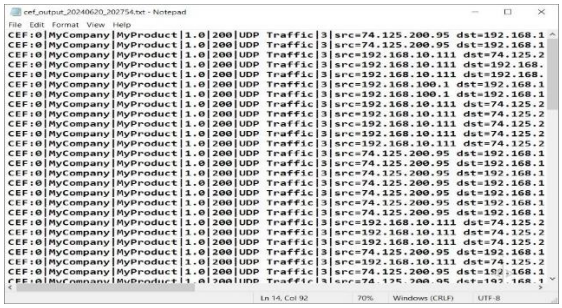
Penerapan Format CEF

Proses penerapan format CEF dimulai dengan mengunggah file PCAP yang berisi log jaringan. File tersebut kemudian dikonversi ke dalam format CEF, yang memungkinkan penyusunan data log jaringan menjadi terstruktur dan mudah dibaca. Setelah dikonversi, hasilnya disimpan sebagai file txt, yang dapat dilihat pada Gambar 3.



Gambar 3. Implementasi Input File Pcap

Setelah proses konversi ke format CEF, data dalam file log akan disusun dengan standar yang konsisten, memudahkan integrasi dengan sistem analisis keamanan lainnya. Berikut adalah contoh hasil data yang telah menerapkan format CEF yang ditunjukkan pada Gambar 4.



Gambar 4. Hasil Penerapan Format CEF

Proses Enkripsi

Proses enkripsi dimulai dengan mengunggah file txt dari log jaringan yang telah diformat dalam CEF dan memasukkan kunci enkripsi. Setelah itu, data tersebut dienkripsi menjadi *ciphertext* yang tidak dapat dibaca oleh pihak yang tidak memiliki akses. Hasil enkripsi kemudian disimpan sebagai file txt yang berisi data dalam bentuk terenkripsi, sehingga memastikan bahwa informasi sensitif terlindungi dengan baik, yang ditunjukkan pada Gambar 5.

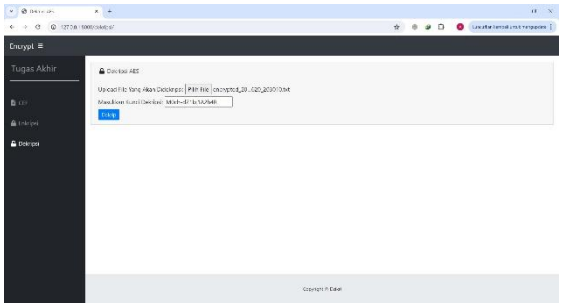
Gambar 5. Implementasi Input Enkripsi

Setelah melakukan proses enkripsi, data dalam file teks akan diubah menjadi pesan acak yang tidak bisa dibaca oleh pihak yang tidak memiliki kunci enkripsi. Berikut adalah contoh hasil dari data yang telah dienkripsi, dan ditunjukkan pada Gambar 6.

Gambar 6. Hasil Enkripsi

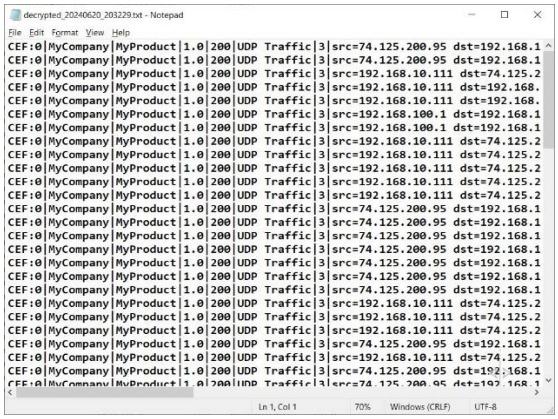
Proses Dekripsi

Proses dekripsi adalah langkah di mana file yang telah dienkripsi dapat kembali diakses atau dibaca. Proses ini dilakukan dengan mengunggah file hasil enkripsi dan memasukkan kunci yang sama saat melakukan proses enkripsi sebelumnya. Hasil dekripsi kemudian disimpan sebagai file txt yang berisi data asli yang telah dipulihkan dari bentuk terenkripsi, yang ditunjukkan pada Gambar 7.



Gambar 7. Implementasi Input Dekripsi

Setelah proses dekripsi, data yang semula tidak dapat dibaca akan dikembalikan ke bentuk aslinya. Berikut adalah contoh hasil data yang telah didekripsi, menunjukkan bahwa informasi asli dapat diakses kembali dengan kunci yang benar seperti yang ditunjukkan pada Gambar 8.



Gambar 8. Hasil Dekripsi

Pengujian Kunci

Dalam pengujian kunci, penulis menggunakan alat bernama *How Secure is Your Password* untuk mengukur tingkat keamanan dari kunci yang dipakai. Alat ini menyediakan tiga metode pengecekan kunci, mulai dari kunci yang lemah hingga yang kunci yang kuat. Kunci yang diuji adalah kunci yang telah melalui proses enkripsi pada program. Metode pengecekan kunci tersebut meliputi:

1. Panjang Kunci: Mengevaluasi apakah kata sandi memiliki panjang yang cukup, karena kata sandi yang lebih panjang cenderung lebih sulit dipecahkan.
2. Kompleksitas Karakter: Memeriksa apakah kata sandi mengandung kombinasi huruf besar, huruf kecil, angka, dan karakter khusus.
3. Pesan Peringatan: Menyediakan rekomendasi kepada pengguna mengenai tindakan yang dapat dilakukan untuk meningkatkan keamanan kata sandi mereka apabila kata sandi tersebut dinilai lemah.

Berdasarkan ketiga faktor ini, alat tersebut akan menghitung estimasi waktu yang diperlukan untuk menebak kunci yang digunakan. Berikut adalah tabel hasil pengujian kunci yang telah digunakan, yang ditunjukkan pada Tabel 3.

Tabel 3. Hasil Pengecekan Kunci

No	Kunci	Waktu
1	9876543210987654	1.2 detik
2	aAa98765432aAaab	3 hari
3	ZYXWVUTSRQPO1111	4.18 detik
4	9C8HgfBtikGe8Qhg	33 triliun tahun
5	BkFVqXE@R9PgJCfA	6 ribu triliun tahun

Berdasarkan Tabel 3, dapat disimpulkan bahwa untuk mencapai tingkat keamanan yang tinggi, kunci harus terdiri dari kombinasi huruf besar, huruf kecil, angka, dan karakter khusus. Semakin kompleks dan acak kombinasi karakter yang digunakan, semakin sulit dan memakan waktu bagi pihak yang tidak berwenang untuk memecahkan kunci tersebut

SIMPULAN

Dalam penelitian ini, implementasi enkripsi menggunakan algoritma AES yang dikombinasikan CEF untuk mengamankan log jaringan telah berhasil dilakukan. Proses enkripsi AES pada file log yang telah diformat dalam CEF menggunakan kunci 128-bit memastikan kerahasiaan dan integritas data. Kunci enkripsi yang dipilih dengan mengkombinasikan huruf besar, huruf kecil, angka, dan karakter khusus dapat memperkuat keamanan proses enkripsi dan dekripsi data log jaringan. Penggunaan format CEF juga mendukung analisis keamanan yang efektif terhadap aktivitas jaringan yang tercatat. Sebagai saran, untuk pengembangan selanjutnya, dapat dipertimbangkan untuk memperluas cakupan pengujian keamanan dengan

mempertimbangkan implementasi metode otentikasi tambahan atau penggunaan kunci dengan panjang yang lebih besar, seperti AES-192 atau AES-256, tergantung pada kebutuhan keamanan spesifik jaringan yang dihadapi. Keseluruhan, implementasi ini tidak hanya meningkatkan keamanan data log jaringan tetapi juga memastikan bahwa data sensitif dalam log dapat diakses dan dikelola secara aman dan efisien.

DAFTAR PUSTAKA

Akhriana, A., & Irmayana, A. (2019). Web app pendeteksi jenis serangan jaringan komputer dengan memanfaatkan Snort dan log honeypot. *CCIT*, 12(1), 87–98.

Alamsyah, H., -, R., & Al Akbar, A. (2020). Analisa keamanan jaringan menggunakan network intrusion detection and prevention system. *JOINTECS (Journal of Information Technology and Computer Science)*, 5(1), 17. https://doi.org/10.31328/jointecs.v5i1.1240

Bhaudhayana, I. M. W. G. (2018). Implementasi algoritma kriptografi AES 256 dan metode steganografi LSB pada gambar bitmap. *Angewandte Chemie International Edition*, 3(1), 10–27.

Budi, E., Wira, D., & Infantono, A. (2021). Strategi penguatan cyber security guna mewujudkan keamanan nasional di era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia*, 3(November), 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

Gabriel, A. J. (2022). Securing system logs in financial institutions using hybrid AES-ECC cryptography. *Journal of Internet Technology and Secured Transactions*, 10(1), 780–786. https://doi.org/10.20533/jitst.2046.3723.2022.0096

Handoyo, J., & Subakti, Y. M. (2020). Keamanan dokumen menggunakan algoritma Advanced Encryption Standard (AES). *Journal of SITECH (Sistem Informasi dan Teknologi)*, 3(2), 143–152. https://doi.org/10.24176/sitech.v3i2.5865

Ismadiah, R., Syahrizal, M., & Ramadhani, P. (2020). Kombinasi algoritma Cipher Block Chaining (CBC) dan Mars pada penyandian file PDF. *Journal of Computer Systems and Informatics*, 1(4), 337–345.

Laksana, T. G., & Mulyani, S. (2024). Pengetahuan dasar identifikasi dini deteksi serangan kejahatan siber untuk mencegah pembobolan data perusahaan. *Jurnal Ilmiah Multidisiplin*, 3(1), 109–122. https://doi.org/10.56127/jukim.v3i01.1143

Lantz, B. (2006). Locking down log files: Enhancing network security by protecting log files. *Issues in Information Systems*, 7(2), 43–47. https://doi.org/10.48009/2_iis_2006_43-47

Manullang, S. F. (2023). Pengamanan data file dokumen menggunakan algoritma Advanced Encryption Standard mode Cipher Block Chaining. *Jurnal Ilmiah Teknik Informatika*, 17(1), 53–67.

More, S., Jamadar, I., & Kazi, F. (2020). Security visualization and active querying for OT network. *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. https://doi.org/10.1109/ICCCNT49239.2020.9225275

Nurnaningsih, D., & Permana, A. A. (2018). Rancangan aplikasi pengamanan data dengan algoritma Advanced Encryption Standard (AES). *Jurnal Teknik Informatika*, 11(2), 177–186.

https://doi.org/10.15408/jti.v11i2.7811

Nyoman Putri Purnama Santhi, N., & Nengah Nuarta, I. (2023). Penguatan penegakan hukum Polri dalam rangka optimalisasi penanggulangan cybercrime di Indonesia. *Scientific Journal of Multidisciplinary Science*, 2(1), 15–27.

Permana, A. A. (2018). Penerapan kriptografi pada teks pesan dengan menggunakan metode Vigenere Cipher berbasis Android. *Jurnal AL-AZHAR Indonesia Seri Sains dan Teknologi*, 4(3), 110–115.

Putra, W., Fahlevi, M. R., & Hidayat, A. T. (2023). Implementasi algoritma Advanced Encryption Standard untuk kemanan dokumen. *Jurnal Teknologi dan Informasi*, 1(2), 76–83. Retrieved from https://journal.grahamitra.id/index.php/jurikti/article/view/55 https://journal.grahamitra.id/index.php/jurikti/article/download/55/181

Ramli, M., et al. (2023). Monitoring dan evaluasi keamanan jaringan dengan pendekatan System Information and Security Management (SIEM). *Faktore Exacta*, 16(1), 1979–276. https://doi.org/10.30998/faktorexacta.v16i1.16534

Samad, M. Y., & Persadha, P. D. (2022). Memahami perang siber dan peran Badan Intelijen Negara dalam menangkal ancaman di siber. *Jurnal IPTEKKOM: Jurnal Ilmu Pengetahuan dan Teknologi Informasi*, 24(2), 135–146. https://doi.org/10.17933/iptekkom.24.2.2022.135-146

Watts, S. (2023). Format acara umum (CEF): Pengantar. Splunk. Retrieved from https://www.splunk.com/en_us/blog/learn/common-event-format-cef.html