PENGGUNAAN ALGORITMA AES (*ADVANCED ENCRYPTION STANDARD*) PADA VERACRYPT UNTUK MENGAMANKAN DATA PADA PERANGKAT PENYIMPANAN

A'la Faradisil Jannah, Muhlis Tahir, Maduratna Sari Saputri,
Qurrotul Aini, Tegar Wicaksono Hermawan
Pendidikan Informatika, Universitas Trunojoyo Madura
Jl. Raya Telang, Perumahan Telang Indah, Telang, Kec. Kamal, Kabupaten Bangkalan, Jawa Timur 69162
220631100101@student.trunojoyo.ac.id

ABSTRAK

Keamanan data merupakan hal yang sangat penting dalam era digital saat ini, terutama dalam melindungi informasi yang tersimpan pada perangkat penyimpanan. Permasalahan utama yang dihadapi adalah bagaimana cara melindungi data dari ancaman akses tidak sah, pencurian data, dan berbagai bentuk ancaman digital lainnya. Penelitian ini bertujuan untuk menganalisis cara kerja algoritma AES (*Advanced Encryption Standard*) dalam perangkat lunak VeraCrypt serta mengukur efektivitas dan tingkat keamanan enkripsi data yang dihasilkan. Metode penelitian yang digunakan adalah eksperimen. Hasil penelitian menunjukkan bahwa penggunaan AES pada VeraCrypt mampu melindungi data dari akses tidak sah dengan tetap menjaga kinerja sistem dalam batas yang wajar. Dengan demikian, kombinasi antara VeraCrypt dan AES dapat menjadi solusi yang tepat dalam mengamankan data pada perangkat penyimpanan.

Kata kunci : *Keamanan data, Algoritma AES, VeraCrypt, Enkripsi*

1. PENDAHULUAN

Di tengah dunia digital saat ini, berbagai macam bentuk data mudah diakses melalui media sosial. Karena itu pengguna harus terus waspada dan meningkatkan kesadaran diri tentang pentingnya menjaga privasi dan keamanan data. Dengan terus berkembangnya teknologi, ancaman terhadap data pribadi sangat kompleks. Mulai dari peretasan hingga kebocoran informasi sensitif yang dapat merugikan individu hingga organisasi. Hal ini menegaskan pentingnya sistem keamanan yang kuat untuk melindungi data dari kebocoran. Proses keamanan ini melibatkan serangkaian tindakan untuk memastikan bahwa data hanya tersedia bagi pihak yang berwenang, dan tidak dapat diakses oleh pihak yang tidak berwenang [1]. Ancaman-ancaman ini menuntut implementasi solusi nyata dalam bentuk perlindungan data yang lebih kuat dan terukur.

Tingginya jumlah kasus pencurian atau kebocoran data dari perangkat penyimpanan menunjukkan perlunya penerapan sistem keamanan yang lebih kuat, peningkatan kesadaran pengguna, serta dukungan kebijakan dan regulasi yang tegas. Salah satu contoh nyata dari lemahnya sistem keamanan yang ada dapat dilihat dari serangan siber besar yang terjadi baru-baru ini yakni Serangan siber pada Pusat Data Nasional Sementara (PDNS) 2 Surabaya pada Juni 2024 yang disebabkan oleh ransomware Braincipher, varian dari Lockbit 3.0. yang dikenal karena kemampuannya mengenkripsi data secara masif dan menyulitkan proses pemulihan tanpa kunci dekripsi. [2]. Serangan ini mengakibatkan gangguan pada layanan publik, termasuk layanan keimigrasian, dengan dampak serius bagi aktivitas masyarakat dan kerugian finansial yang signifikan. Salah satu langkah penting yang dapat diterapkan untuk meminimalkan risiko serupa di masa mendatang adalah dengan menerapkan enkripsi sebagai fondasi utama dalam sistem keamanan data.

Menurut Dedi Purwanto, Enkripsi digunakan untuk menyandikan data atau informasi sehingga tidak dapat diakses oleh orang yang tidak berhak. Dengan enkripsi, data disandikan (*encrypted*) menggunakan sebuah Password (*key*). Untuk membuka enkripsi (*decrypt*), menggunakan sebuah Password juga [3]. Alisa Almadira menyebutkan dalam tulisannya bahwa enkripsi dan keamanan data saling berhubungan, dimana dengan mengimplementasikan enkripsi, data yang dikirim dan disimpan dapat terlindungi dari akses yang tidak sah dari oknum tidak bertanggung jawab. Ia juga menyebutkan bahwa meskipun terjadi kebocoran data, informasi yang terenkripsi akan sulit dimanfaatkan tanpa password yang benar, sehingga enkripsi menjadi inti dalam setiap kebijakan keamanan data digital [4]. Salah satu bentuk implementasi nyata dari teknologi enkripsi tersebut dapat ditemukan pada perangkat lunak seperti VeraCrypt.

VeraCrypt merupakan perangkat lunak enkripsi disk open source gratis untuk Windows, Mac OSX dan Linux. VeraCrypt menambahkan keamanan yang ditingkatkan ke algoritma yang digunakan untuk enkripsi sistem dan partisi sehingga membuatnya kebal terhadap perkembangan baru dalam serangan brute-force. Salah satu algoritma yang digunakan oleh VeraCrypt adalah AES (*Advanced Encryption Standard*), yang telah menjadi standar global dalam pengamanan data. [5]

Dipilihnya algoritma AES (*Advanced Encryption Standard*) karena dirancang khusus untuk keamanan tingkat tinggi serta ketahanan terhadap berbagai jenis serangan, bahkan kesederhanaan rancangan, kekompakan kode dan kecepatan mengenkripsi dan deskripsi setiap file atau data. [6]

Sejalan dengan penjelasan mengenai penerapan

algoritma AES dalam VeraCrypt dan fungsinya dalam meningkatkan keamanan data, penelitian ini bertujuan untuk menganalisis cara kerja algoritma AES (*Advanced Encryption Standard*) dalam perangkat lunak VeraCrypt serta mengukur efektivitas dan tingkat keamanan enkripsi data yang dihasilkan. Selain itu, Penelitian ini juga difokuskan untuk menilai bagaimana AES bekerja pada VeraCrypt dan sejauh mana algoritma tersebut efektif dalam menjamin kerahasiaan data serta tahan terhadap berbagai bentuk ancaman keamanan digital.

2. TINJAUAN PUSTAKA

2.1 Keamanan Data dan Enkripsi

Keamanan data adalah suatu upaya untuk melindungi data dari ancaman yang dapat mengganggu kerahasiaan (*confidentiality*), Integritas (*integrity*), dan ketersediaan (*availability*) data tersebut. Keamanan data bertujuan untuk memastikan bahwa informasi yang disimpan, diproses, dan ditransmisikan tidak dapat diakses oleh pihak yang tidak berwenang, tidak mudah dimodifikasi secara tidak sah, dan selalu tersedia bagi pihak yang berwenang saat dibutuhkan.

Mengenai tujuan keamanan informasi diantaranya menurut Edy Soesanto ialah sebagai berikut:

a. *Confidentiality*, merupakan bagian yang menjaga kerahasiaan informasi atau data dan memastikan bahwa hanya pihak-pihak terkait yang memiliki akses terhadap informasi tersebut [7]
b. *Integrity*, adalah bagian yang melindungi informasi agar informasi tidak dapat diubah tanpa persetujuan data, menjamin keutuhan data dan mencangkup kerusakan dan ancaman dari pihak lain yang dapat menyebabkan perubahan atau kegagalan data asli atau informasi [7]
c. *Availability*, adalah bagian ketersediaan yang memastikan bahwa informasi siap saat dibutuhkan dan melindungi pengguna dari akses gratis data [7].

Menurut Hasibuan, Enkripsi adalah satu teknik yang digunakan untuk melindungi basis data dari akses yang tidak berhak dan tindakan-tindakan yang tidak diinginkan dari pengguna-pengguna luar [8]. Tujuan enkripsi yaitu untuk melindungi data dari akses yang tidak sah, terutama saat mengirim data melalui jaringan publik atau disimpan dalam media digital. Data yang telah dienkripsi hanya dapat dikembalikan ke bentuk aslinya melalui proses dekripsi dengan menggunakan kunci yang sesuai.

Berdasarkan mekanisme penggunaan kunci, algoritma enkripsi dibagi menjadi dua jenis utama yaitu enkripsi simetris (*Symmetric encryption*) dan enkripsi asimetris (*Asymmetric Encryption*). Enkripsi simetris menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi pesan, sedangkan enkripsi asimetris menggunakan kunci yang berbeda, yaitu kunci public dank unci private [9]
Contoh algoritma enkripsi simetris sebagai berikut:

a. AES (*Advenced Encryption Standard*)
AES (*Advenced Encryption Standard*) adalah algoritma yang menggunakan kunci dan masukan dengan panjang 128 bit. Setiap masukan 128 bit plaintext dimasukan ke dalam state yang berbentuk bujur sangkar berukuran 4 x 4 byte [10]. Hasil dari state nantinya akan di XOR dengan key kemudian diolah 10 kali dengan substitusi-transformasi liniear-addkey.
b. DES (*Data Encryption Standard*)
DES merupakan algoritma enkripsi simetris yang dikembangkan oleh IBM. DES menggunakan kunci sepanjang 56-bit kemudian memproses data dalam blok 64-bit melalui rounds substitusi dan permutasi. Kelebihan menggunakan DES yaitu cukup efisien dan sudah banyak digunakan dalam berbagai sistem keamanan.
c. 3DES (*Triple DES*)
3DES merupakan pengembangan dari DES dengan meningkatkan keamanannya melalui proses DES sebanyak tiga kali menggunakan dua atau tiga kunci yang berbeda. penggunaan 3DES lebih aman disbanding DES dengan total ukuran kunci 112-bit (2-key) atau 168-bit (3-key).
d. RC4 dan RC5 (*Rivest Cipher*)
RC4 dan RC5 dikembangkan oleh Ron Rivest, RC4 bekerja dengan cara meng-enkripsi data bit demi bit, ukuran kunci RC4 sifatnya fleksibel mulai dari 40 hingga 2028 bit. RC5 merupakan block cipher yang dirancang agar fleksibel dan mudah untuk diimplentasikan. RC5 dianggap lebih aman dan kuat disbanding RC4, meskipun tidak sepopuler AES dalam penggunaan saat ini.

Sementara Enkripsi Asimetris (*Asymmetric Encryption*) adalah sebagai berikut:

a. RSA (*Rivest Shamir Adleman*)
RSA merupakan sebuah algoritma yang sesuai dengan tanda tangan digital seperti enkripsi dan menjadi sebuah algoritma yang paling depan di bagian kriptografi public key [11]. RSA sudah dipercaya mengamankan sebuah data dengan menggunakan kunci yang cukup panjang. RSA memiliki tiga tahapan seperti pembangkit kunci, enkripsi dan dekripsi.
b. ECC (*Eliptic Curve Cryptography*)
ECC adalah sebuah algoritma enkripsi asimetris yang menggunakan kurva eliptik di dalam perhitungannya. Keunggulan mengunakan algoritma ECC yaitu dapat mencapai keamanan yang tinggi dengan menggunakan ukuran kunci yang lebih kecil, sehingga dalam hal kecepatan dan penggunaan sumber daya lebih efisien.
c. DSA (*Digital Signature Algorithm*)
DSA merupakan algoritma yang dirancang khusus sebagai kepertluan tanda tangan digital. DSA digunakan untuk memastikan keaslian pesan atau dokumen digital, dan bukan sebagai proses enkripi data secara umum.

2.2 Algoritma AES (*Advanced Encryption Standard*)

Algoritma AES adalah blok chipertext simetrik yang digunakan untuk mengenkripsi (*encipher*) dan mendekripsi (*decipher*) informasi. AES adalah algoritma kriptografi untuk mengamakan data dimana algoritmanya adalah blok chipertext simetrik yang dapat mengenkripsi dan mendekripsi informasi [12] Enkripsi AES adalah transformasi terhadap state secara berulang dalan beberapa ronde. State yang menjadi keluaran ronde k menjadi masukan untuk ronde ke k+1. Secara ringkas algoritma deskripsi AES merupakan kebalikan algoritma enkripsi AES. Algoritma deskripsi AES menggunakan transformasi invers semua transformasi dasar yang digunakan pada algooritma enkripsi AES [13]

2.3 Struktur Blok & *Key Size*

Struktur algoritma AES (*Advanced Encryption Standard*) terdiri dari ukuran blok yang tetap, yaitu sebesar 128-bit. Sementara itu, ukuran kunci (*key size*) yang digunakan dapat bervariasi, yaitu 128-bit, 192-bit, dan 256-bit. Kemudian untuk jumlah putaran (*round*) yang dilakukan oleh algoritma tergantung pada panjang kunci yang digunakan: AES-128 menggunakan 10 putaran, AES-192 menggunakan 12 putaran, dan AES-256 menggunakan 14 putaran. Variasi jumlah putaran ini bertujuan untuk meningkatkan kompleksitas proses enkripsi seiring bertambahnya panjang kunci, sehingga memperkuat keamanan data terhadap berbagai jenis serangan kriptografi. [14]

2.4 Proses Enkripsi AES (*Advanced Encryption Standard*)

Proses enkripsi dalam algoritma AES terdiri dari beberapa tahapan yang diulang dalam setiap putarannya, kecuali pada putaran terakhir. Setiap putaran mencakup empat langkah utama, yaitu: *SubBytes*, yaitu proses substitusi byte berbasis pada tabel substitusi nonlinier (S-Box); *ShiftRows*, yaitu operasi pergeseran baris dalam matriks data untuk menciptakan difusi; *MixColumns*, yaitu transformasi kolom yang bertujuan menyebarkan entropi lebih merata di seluruh blok data; dan *AddRoundKey*, di mana data hasil transformasi dioperasikan dengan kunci putaran atau *round key* menggunakan operasi XOR [15].

Sementara itu, proses dekripsi merupakan kebalikan dari proses enkripsi dan dilakukan dengan menggunakan operasi inversi dari setiap tahapan enkripsi. Hal ini meliputi penggunaan inverse S-Box untuk tahap *SubBytes*, inverse *ShiftRows*, serta inverse *MixColumns*. Dengan melakukan proses inversi ini, data yang sebelumnya telah dienkripsi akan dikembalikan ke bentuk awalnya dengan syarat kunci yang diinputkan pada dekripsi sama dengan kunci enkripsi [15].

2.5 VeraCrypt

VeraCrypt merupakan perangkat lunak enkripsi disk open source gratis untuk Windows, Mac OSX dan Linux. VeraCrypt menambahkan keamanan yang ditingkatkan ke algoritma yang digunakan untuk enkripsi sistem dan partisi sehingga membuatnya kebal terhadap perkembangan baru dalam serangan brute-force [5].

VeraCrypt dapat menjadi alternatif dalam melakukan pengamanan data pada drive. Pada segi proses *Bitlocker* memiliki tahapan yang lebih sederhana dan sedikit sedangkan Veracrypt lebih panjang dan banyak pilihan opsi pada enkripsi drive.Veracrypt menawarkan fitur seperti enkripsi kata sandi, penguncian file atau penguncian perangkat keras, dan kemampuan untuk menyembunyikan volume terenkripsi di dalam volume yang ada. Berkat fitur keamanan dan fleksibilitas yang ditawarkannya, Veracrypt adalah pilihan populer bagi mereka yang ingin meningkatkan keamanan data mereka terhadap ancaman kejahatan siber [5].

Veracrypt memungkinkan pengguna membuat volume terenkripsi untuk file, mengenkripsi seluruh disk atau partisi, atau membuat volume terenkripsi yang terlihat seperti disk virtual. Enkripsi yang disediakan oleh Veracrypt adalah salah satu yang terkuat yang tersedia untuk umum dan telah diuji secara ekstensif oleh komunitas keamanan [16]

Veracrypt menawarkan fitur seperti enkripsi kata sandi, penguncian file atau penguncian perangkat keras, dan kemampuan untuk menyembunyikan volume terenkripsi di dalam volume yang ada [16].

2.6 Penelitian Terkait

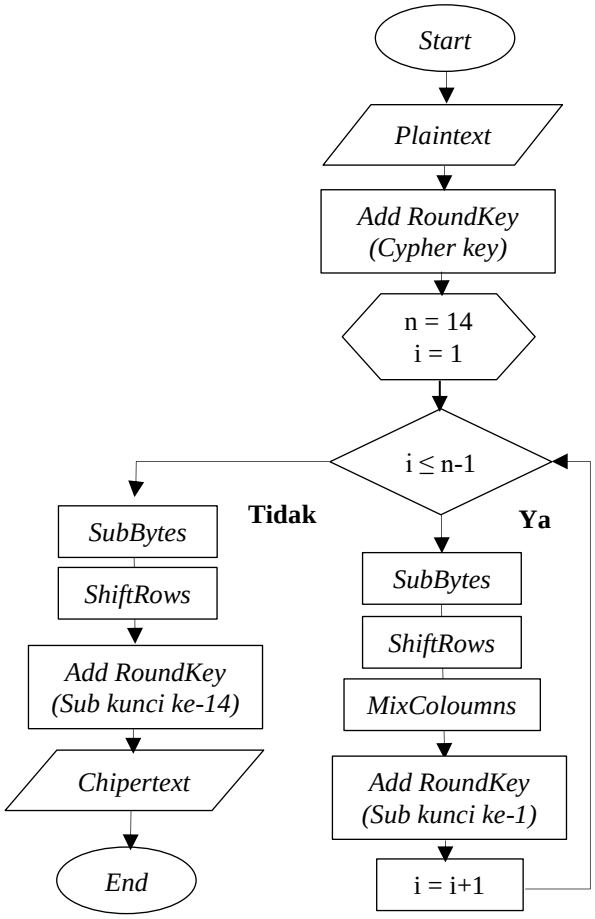
Terkait dengan penggunaan algoritma AES dalam pengamanan file dan data, sejumlah penelitian sebelumnya telah dilakukan, diantaranya penelitian yang dilakukan oleh Khoirudin yang berjudul "Penerapan Algoritma *Advanced Encryption Standard* (AES-512) untuk Pengamanan File Berbasis Web". Penerapan algoritma AES-512 dalam penelitian ini difokuskan pada pengamanan data penting perusahaan PT. Skemanusa Consultama Teknik yang sebelumnya disimpan secara tidak aman. Pengujian dilakukan dengan mengukur kecepatan dan keberhasilan enkripsi serta dekripsi berbagai jenis file pada sistem yang dirancang berbasis web. Hasil menunjukkan bahwa seluruh proses enkripsi dan dekripsi berhasil dilakukan dengan waktu yang efisien dan tanpa perubahan ukuran file asli. AES-512 terbukti mampu memberikan perlindungan yang kuat terhadap file digital menjadikan algoritma ini sebagai solusi efektif dalam pengamanan data [17].

3. METODE PENELITIAN

Penelitian ini dilakukan dengan pendekatan eksperimen yang bertujuan untuk menganalisis efektivitas algoritma AES dalam mengamankan data pada perangkat penyimpanan menggunakan perangkat lunak VeraCrypt. Fokus utama terletak pada proses

enkripsi menggunakan AES dan pengujian terhadap performa serta keamanannya.

Berikut merupakan alur proses enkripsi algoritma AES yang digunakan dalam VeraCrypt:



Gambar 1. Flowchart proses enkripsi

Flowchart di atas menggambarkan alur proses enkripsi data menggunakan algoritma AES (*Advanced Encryption Standard*) dalam implementasinya pada VeraCrypt, khususnya dengan panjang kunci 256-bit yang memerlukan 14 ronde enkripsi.

a. *Start*
   Proses enkripsi dimulai dengan menerima data asli (*plaintext*) dan kunci enkripsi (*cipher key*) sebagai input.
b. *AddRoundKey*
   Langkah pertama adalah menggabungkan data plaintext dengan kunci utama menggunakan operasi XOR.
c. Inisialisasi Ronde
   Proses enkripsi terdiri dari 14 ronde untuk AES-256. Variabel i diset mulai dari 1.
d. Ronde 1 hingga 13 (i ≤ n - 1)
   Untuk ronde pertama hingga ke-13, dilakukan empat proses utama yaitu *SubBytes* untuk mengganti setiap byte data dengan nilai dari tabel substitusi (S-Box), *ShiftRows* untuk menggeser baris dalam blok data untuk meningkatkan difusi, *MixColumns* untuk mengacak kolom untuk menciptakan keterkaitan antar byte, *AddRoundKey* untuk menggabungkan hasil transformasi dengan sub-kunci ke-i.
e. Ronde ke-14 (Akhir)
   Ronde terakhir dilakukan tanpa MixColumns (sesuai dengan standar AES)
f. *Ciphertext*
   Hasil akhir dari proses enkripsi adalah *ciphertext*, yaitu data terenkripsi yang tidak dapat dibaca tanpa kunci.
g. *End*
   Proses enkripsi selesai.

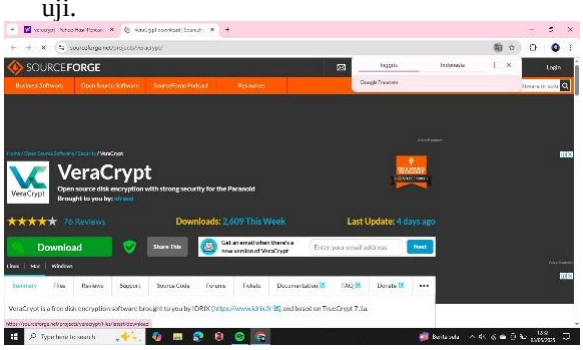
Ketika pengguna membuat volume terenkripsi di VeraCrypt dan memilih algoritma AES-256, proses internal yang dijalankan adalah seperti pada flowchart ini. VeraCrypt secara otomatis menerapkan tahapan enkripsi tersebut untuk semua data yang disimpan dalam volume, sehingga keamanan file terjamin secara kriptografis.

4. HASIL DAN PEMBAHASAN

4.1. Implementasi VeraCrypt dengan Algoritma AES

Implementasi dilakukan melalui beberapa tahap sebagai berikut:

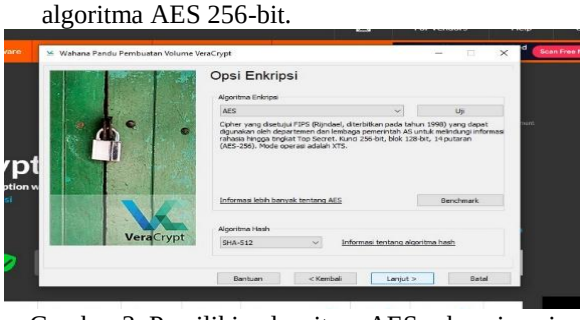
a. Intalasi perangkat lunak VeraCrypt pada komputer uji.



Gambar 2. Instalasi Software VeraCrypt

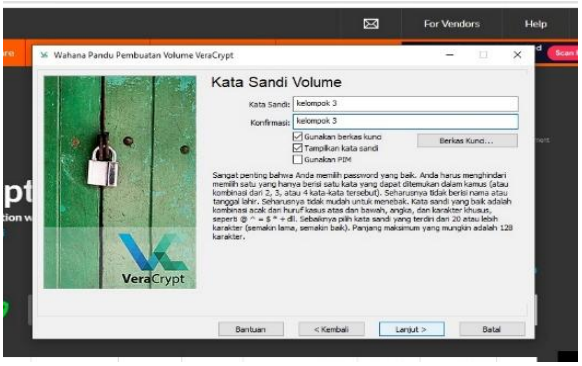
Gambar diatas memperlihatkan proses awal instalasi VeraCrypt melalui situs SourceForge, sebagai langkah penting dalam menyiapkan lingkungan pengujian. Instalasi dilakukan untuk mendukung implementasi serta analisis sistem enkripsi pada komputer uji.

b. Membuat volume terenkripsi baru menggunakan algoritma AES 256-bit.



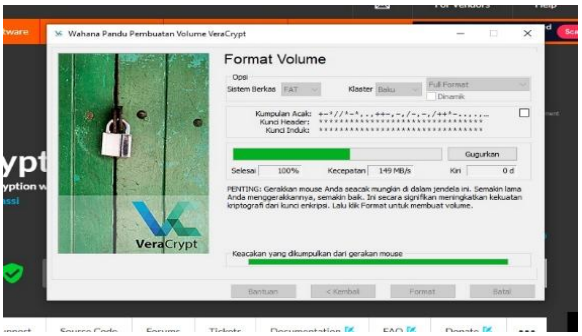
Gambar 3. Pemilihin algoritma AES sebagai opsi enkripsi

Pada gambar diatas, user diminta untuk memilih metode enkripsi untuk volume yang akan dibuat. Pada penelitian ini, algoritma AES (*Advanced Encryption Standard*) dipilih sebagai algoritma yang akan digunakan untuk melindungu volume yang dibuat.



Gambar 4. Membuat password untuk volume

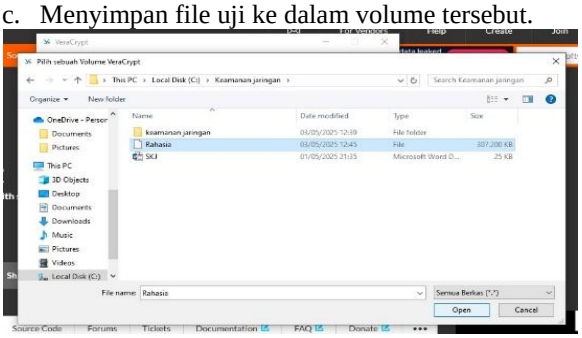
Gambar diatas menampilkan jendela "Volume Password" dari VeraCrypt Dimana jendela ini meminta user untuk memasukkan dan mengkonfirmasi kata sandi untuk volume yang akan dibuat



Gambar 5. Proses formal volume

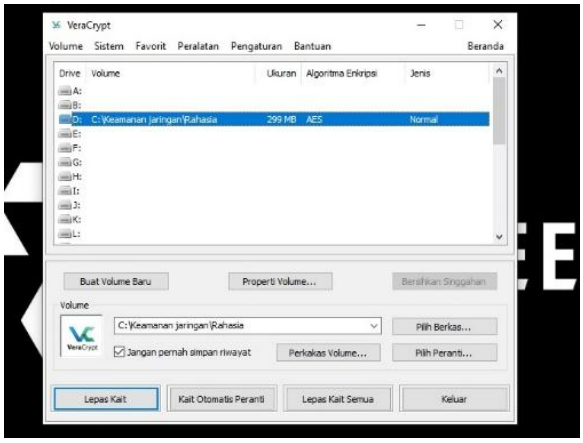
Gambar tersebut menunjukkan proses format volume pada perangkat lunak VeraCrypt, di mana pengguna dapat memilih sistem berkas, tipe klaster, serta metode format. Selain itu, VeraCrypt mengumpulkan keacakan dari pergerakan mouse pengguna untuk meningkatkan kekuatan kriptografi pada kunci enkripsi. Setelah proses format selesai, volume terenkripsi siap digunakan untuk menyimpan data secara aman.

c. Menyimpan file uji ke dalam volume tersebut.



Gambar 6. Pemilihan file uji untuk disimpan ke dalam volume terenkripsi

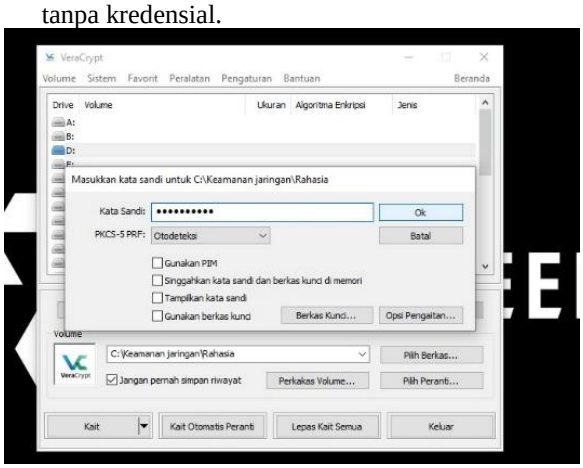
Gambar diatas menunjukkan proses pemilihan file uji dari direktori penyimpanan yang akan dimasukkan ke dalam volume terenkripsi. File ini nantinya akan digunakan untuk menguji integritas dan fungsi dari sistem enkripsi yang telah dibuat.



Gambar 7. File uji berhasil disimpan dan diakses dalam volume terenkripsi

Setelah file dimasukkan ke dalam volume, VeraCrypt menampilkan isi volume terenkripsi yang telah berhasil dipasang (*mounted*), menandakan bahwa file uji telah tersimpan dengan aman dan dapat diakses seperti penyimpanan biasa, namun dengan perlindungan enkripsi.

d. Menganalisis keamanan dengan menguji akses tanpa kredensial.



Gambar 8. VeraCrypt saat meminta kredensial untuk mengakses volume terenkripsi.

Gambar diatas menunjukkan bahwa saat pengguna mencoba mengakses volume terenkripsi, VeraCrypt secara otomatis meminta kata sandi sebagai bentuk autentikasi. Hal ini membuktikan bahwa tanpa kredensial yang benar, volume tidak dapat diakses, sehingga data di dalamnya tetap terlindungi dan mendukung analisis keamanan terhadap upaya akses tanpa otorisasi

4.2. Hasil Pengujian Kecepatan dan Performa

Tabel 1. Hasil pengujian enkripsi

Algoritma	Read (MB/s)	Write (MB/s)	CPU Usage (%)	Overhead vs Non-Enkripsi
AES-128	470	445	3–5%	+6% latency
AES-256	462	437	4–7%	+9% latency
Tanpa Enkripsi	480	450	<1%	—

Hasil pengujian menunjukkan bahwa waktu *mounting* volume tanpa enkripsi hanya memerlukan waktu kurang dari 1 detik, sedangkan pada volume terenkripsi dengan AES-256, proses mounting memerlukan waktu sekitar 3 detik. Selanjutnya, dalam pengujian transfer file berukuran 2 GB, volume tanpa enkripsi mencatat waktu sekitar 50 detik, sementara volume dengan enkripsi AES-256 membutuhkan waktu sekitar 58 detik. Perbedaan ini menunjukkan adanya sedikit penurunan performa akibat proses enkripsi, namun tetap dalam batas yang dapat diterima.

Peningkatan efisiensi enkripsi ini didukung oleh teknologi AES-NI (*Advanced Encryption Standard New Instructions*), yaitu instruksi khusus yang tersedia pada prosesor modern. AES-NI memungkinkan eksekusi algoritma enkripsi langsung oleh CPU tanpa harus melalui jalur perangkat lunak biasa. Teknologi ini terbukti mampu mengurangi waktu enkripsi hingga 60% dan menghilangkan potensi timing attack berbasis cache, sehingga memperkuat keamanan sekaligus menjaga kinerja sistem.

4.3. Perbandingan dengan Data yang Tidak Terenkripsi

Perbedaan antara data yang tidak terenkripsi dan data yang terenkripsi terletak pada kecepatan transfer dan tingkat keamanannya. Data yang tidak terenkripsi dapat ditransfer dengan lebih cepat, namun rentan terhadap pencurian fisik dan cold-boot attack. Sementara itu, enkripsi AES menambahkan lapisan perlindungan yang kuat tanpa mengorbankan performa secara signifikan, dengan penurunan kinerja sekitar 7–10%.

4.4. Efektivitas Enkripsi (Keamanan)

Berdasarkan hasil pengujian, algoritma AES yang diterapkan dalam VeraCrypt terbukti mampu memberikan perlindungan data dengan tingkat enkripsi yang sangat tinggi. AES merupakan algoritma enkripsi simetris yang diakui secara global dan telah digunakan oleh berbagai institusi seperti lembaga pemerintah dan militer karena keandalan dan kekuatannya.

Secara khusus, penggunaan AES-256 menawarkan tingkat keamanan yang sangat tinggi karena panjang kunci mencapai 256 bit, sehingga sangat sulit untuk ditembus melalui serangan *brute-force*. Selama proses pengujian, tidak ditemukan indikasi kebocoran data maupun celah keamanan, yang menunjukkan bahwa proses enkripsi dan dekripsi berlangsung secara aman, stabil, dan andal.

4.5. Kinerja Sistem

Implementasi algoritma AES pada VeraCrypt menghasilkan proses enkripsi yang cepat dan efisien, dengan performa yang sangat bergantung pada beberapa faktor. Salah satu faktor utama adalah spesifikasi perangkat keras, khususnya jika CPU mendukung instruksi AES-NI yang dapat mempercepat proses enkripsi secara signifikan melalui akselerasi perangkat keras. Selain itu, ukuran file yang dienkripsi juga memengaruhi waktu pemrosesan; semakin besar ukuran file, maka waktu yang dibutuhkan untuk proses enkripsi akan meningkat. Meskipun demikian, hasil pengujian menunjukkan bahwa waktu pemrosesan tetap berada dalam batas toleransi yang wajar dan stabil.

4.6. Perlindungan terhadap Akses Tidak Sah

VeraCrypt yang menggunakan algoritma AES (*Advanced Encryption Standard*) menyediakan sistem keamanan tambahan untuk melindungi data dari akses yang tidak sah. Salah satu bentuk perlindungan ini adalah autentikasi berbasis kata sandi yang kuat, yang harus di-*input* kan untuk mengakses volume terenkripsi. Selain itu, VeraCrypt juga menyediakan fitur seperti *hidden volume*, yang dirancang untuk memberikan tingkat perlindungan privasi yang lebih tinggi dengan menyembunyikan data sensitif di dalam volume terenkripsi lainnya. Akses terhadap file yang telah dienkripsi tidak dapat dilakukan secara langsung tanpa melalui proses *mounting*, sehingga upaya penyalahgunaan data dapat dicegah secara efektif.

4.7. Uji Coba Terhadap Serangan

Dalam simulasi serangan seperti *brute force* maupun akses fisik terhadap media penyimpanan, VeraCrypt yang menggunakan algoritma AES menunjukkan ketahanan yang sangat baik. Algoritma AES terbukti sangat tangguh terhadap upaya *brute force*, karena membutuhkan waktu komputasi yang sangat besar untuk memecahkan kunci enkripsi tanpa informasi autentik. Selain itu, tanpa keberadaan kata sandi atau *keyfile* yang sah, data yang telah dienkripsi tidak dapat diakses, meskipun penyerang memiliki akses langsung terhadap file atau perangkat penyimpanan tersebut. Hal ini menunjukkan bahwa sistem enkripsi yang digunakan mampu memberikan perlindungan efektif terhadap berbagai bentuk ancaman keamanan.

5. KESIMPULAN DAN SARAN

AES dalam VeraCrypt adalah solusi enkripsi yang sangat efektif. Keamanannya sangat kuat, bahkan menghadapi teknik kriptoanalisis modern. Meskipun ada sedikit penurunan kecepatan di beberapa perangkat keras, manfaat perlindungan data jauh lebih besar daripada dampak tersebut. AES-256 di

VeraCrypt memberikan perlindungan tingkat tinggi untuk kebanyakan kebutuhan pengguna, menjadikannya pilihan ideal untuk menjaga data yang sensitif.

Berdasarkan hasil pembahasan, disarankan untuk menggunakan algoritma AES-256 pada skenario yang memerlukan tingkat keamanan tinggi, seperti penyimpanan data sensitif di instansi pemerintahan atau sektor finansial. Sementara itu, untuk kebutuhan umum seperti laptop pribadi atau sistem bisnis, AES-128 dinilai sudah cukup aman dan efisien. Selain itu, pemanfaatan fitur AES-NI pada perangkat keras yang mendukung perlu dioptimalkan guna meningkatkan kecepatan proses kriptografi tanpa mengurangi tingkat keamanan.

DAFTAR PUSTAKA

[1] A. M. Ujung, M. Irwan, and P. Nasution, "Pentingnya Sistem Keamanan Database untuk melindungi data pribadi," *JISKA: Jurnal Sistem Informasi Dan Informatika*, vol. 1, no. 2, p. 44, 2023, [Online]. Available: http://jurnal.unidha.ac.id/index.php/jteksis

[2] Y. W. Ghalib *et al.*, "ANALISIS PERKEMBANGAN KEAMANAN SIBER DAMPAK DARI KEBOCORAN DATA PUSAT DATA NASIONAL SEMENTARA 2 SURABAYA ASSESSING AND UNDERSTANDING THE CURRENT SITUATION: ANALYSIS OF CYBER SECURITY DEVELOPMENTS THE IMPACT OF THE TEMPORARY NATIONAL DATA CENTER DATA LEAKS 2 SURABAYA Oleh," Jul. 2024.

[3] D. Purwanto, "PERANAN KRIPTOGRAFI DALAM PENINGKATAN PENGAMANAN SISTEM INFORMASI," *Seminar of Social Sciences Engineering & Humaniora*, 2020.

[4] A. Almadira, Y. Pratama, and F. Purwani, "MELINDUNGI DATA DI DUNIA DIGITAL: PERAN STATEGIS ENKRIPSI DALAM KEAMANAN DATA," *Journal of Scientech Research and Development*, vol. 6, no. 2, pp. 540–549, 2024.

[5] A. N. Ghazi and G. Taufiq, "TEKNIK PENGAMANAN DATA AT REST MENGGUNAKAN BITLOCKER DAN VERACRYPT," 2024. [Online]. Available: https://jurnal.umj.ac.id/index.php/just-it/index

[6] S. Saripa, "Implementation of a File Security System Using the AES Algorithm to Secure Personal Files," *Progressive Information, Security, Computer, and Embedded System*, vol. 1, no. 2, pp. 138–148, Sep. 2023, doi: 10.61255/pisces.v1i2.100.

[7] Edy Soesanto, Nova Astia Ningsih, Lili Khoerunisa, and Muhammad Ilham Faturrahman, "Keamanan Informasi Data Dalam Pemanfaatan Teknologi Informasi Pada PT Bank Central Asia (BCA)," *Student Research Journal*, vol. 1, no. 3, pp. 227–238, Jun. 2023, doi: 10.55606/srjyappi.v1i3.334.

[8] Y. Warni Hasibuan and R. Budhiati Veronica, "Perancangan dan Implementasi Aplikasi Kriptografi Algoritma Hill Cipher dalam Dekripsi Enkripsi Data Keuangan Nasabah Bank Sampoerna Menggunakan Kode ASCII," *UNNES Journal of Mathematics*, 2022, [Online]. Available: http://journal.unnes.ac.id/sju/index.php/ujm

[9] S. R. Siburian, R. Alek, S. Sinaga, and F. Yudistira, "KRIPTOSISTEM HYBRID MENGGUNAKAN KOMBINASI AES DAN RSA UNTUK ENKRIPSI TEKS PESAN," *Journal Science Informatica and Robotics*, 2023, [Online]. Available: https://jurnal.ittc.web.id/index.php/jct/

[10] F. Bibiola, T. U. Kalsum, and H. Alamsyah, "Penerapan Algoritma Advance Encryption Standard (AES) Untuk Pengamanan File Pada Aplikasi Berbasis WEB," *JURNAL SURYA ENERGY*, vol. 8, no. 1, p. 35, Sep. 2023, doi: 10.32502/jse.v8i1.6461.

[11] F. Farhan and D. Leman, "Implementasi Metode Rivest Shamir Adleman (RSA) Untuk Kerahasiaan Database Perum Bulog Kanwil SUMUT," *Journal of Machine Learning and Data Analytics (MALDA)*, vol. 02, no. 01, pp. 18–27, 2023.

[12] I. Asih, R. Simbolon, I. Gunawan, I. O. Kirana, R. Dewi, and S. Solikhun, "Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar," *Journal of Computer System and Informatics (JoSYC)*, vol. 1, no. 2, 2020.

[13] L. Mustika, "Implementasi Algoritma AES Untuk Pengamanan Login Dan Data Customer Pada E-Commerce Berbasis Web," *JURIKOM (Jurnal Riset Komputer)*, vol. 7, no. 1, p. 148, Feb. 2020, doi: 10.30865/jurikom.v7i1.1943.

[14] M. Azhari, J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *Jurnal Pendidikan Sains dan Komputer*, vol. 2, no. 1, pp. 2809–476, 2022, doi: 10.47709/jpsk.v2i1.1390.

[15] A. Ridho and A. Romli, "SISTEM PENGAMANAN DOKUMEN MENGGUNAKAN ALGORITMA KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD (AES-256)," *Jurnal Informatika Teknologi dan Sains (JINTEKS)*, 2024.

[16] H. Jurnal, A. P. Ashilah, and R. Rahman, "FORENSIK JARINGAN UNTUK INVESTIGASI KEJAHATAN CYBER PADA STUDI KASUS PEMBOBOLAN DATA KOMINFO OLEH BJORKA," *JURNAL RISET SISTEM INFORMASI*, 2024, doi: 10.69714/g2pay047.

[17] N. H. Khoirudin and W. Windarto, "Penerapan Algoritme Advanced Encryption Standard (AES-512) untuk Pengamanan File Berbasis Web," *KRESNA: Jurnal Riset dan Pengabdian Masyarakat*, vol. 4, no. 1, pp. 62–71, 2024