Pemanfaatan VeraCrypt untuk Perlindungan Data Pribadi

Nurdin[1*], Nur Salman[2], ST. Aminah Dinayati Ghani[3], Hasriani[4]
[1,2,3,4]Universitas Dipa Makassar
Jl. Perintis Kemerdekaan Km.9, Telp. 0411- 587194
e-mail: [*1]nurdin@undipa.ac.id, [2]nursalman.halim@undipa.ac.id, [3]dinayati.amy@undipa.ac.id, [4]hasriani@undipa.ac.id

Abstrak

Perlindungan data pribadi menjadi tantangan utama dalam era digital, di mana kebocoran informasi dapat menyebabkan kerugian serius bagi individu dan organisasi. VeraCrypt, sebagai perangkat lunak enkripsi open-source, menawarkan solusi untuk menjaga kerahasiaan data dengan menerapkan algoritma kriptografi tingkat tinggi. Penelitian ini bertujuan untuk mengevaluasi efektivitas VeraCrypt dalam mengamankan data pribadi melalui pendekatan studi literatur dan uji coba praktis. Folder yang berisi data diuji menggunakan enkripsi AES dengan 10 kali percobaan akses menggunakan metode autentikasi berbeda. Hasil menunjukkan bahwa data hanya dapat diakses melalui mounting volume terenkripsi dengan kunci yang sesuai, sementara semua upaya akses tanpa autentikasi gagal. Selain keamanan yang solid, VeraCrypt juga dinilai cukup mudah digunakan oleh pengguna awam. Penelitian ini menyimpulkan bahwa VeraCrypt layak direkomendasikan sebagai alat perlindungan data pribadi, terutama dalam konteks individu maupun organisasi kecil yang membutuhkan keamanan data tanpa biaya lisensi.

Kata kunci: *Veracrypt, Enkripsi, Keamanan Data, Perlindungan Data Pribadi, Privasi Digital.*

Abstract

The protection of personal data has become a major challenge in the digital era, where information breaches can cause serious harm to individuals and organizations. VeraCrypt, an open-source encryption software, offers a solution to safeguard data confidentiality by implementing advanced cryptographic algorithms. This study aims to evaluate the effectiveness of VeraCrypt in securing personal data through literature review and practical testing. A folder containing data was encrypted using AES, and ten trials were conducted with different authentication scenarios. The results showed that access to the encrypted data was only possible through a properly mounted volume with the correct key, while all unauthorized attempts failed. In addition to its strong security, VeraCrypt was found to be user-friendly even for non-technical users. This research concludes that VeraCrypt is a highly recommended tool for personal data protection, especially for individuals and small organizations seeking secure data solutions without licensing costs.

Keywords*: Veracrypt, Encryption, Data Security, Personal Data Protection, Digital Privacy.*

1. PENDAHULUAN

Perkembangan teknologi informasi telah membawa dampak signifikan terhadap cara individu dan organisasi mengelola data pribadi. Peningkatan penggunaan perangkat digital dan konektivitas internet telah mempermudah akses dan distribusi informasi, namun juga meningkatkan risiko terhadap keamanan data [1]. Insiden kebocoran data, seperti yang terjadi pada berbagai platform digital, menunjukkan perlunya mekanisme perlindungan data yang lebih kuat [2]. Dalam hal ini, pendekatan keamanan yang mengandalkan tools seperti VeraCrypt menjadi semakin relevan [3].

Enkripsi data menjadi salah satu metode utama dalam menjaga kerahasiaan dan integritas informasi. Teknik ini mengubah data menjadi format yang tidak dapat dibaca tanpa kunci dekripsi yang sesuai, sehingga melindungi data dari akses tidak sah [4]. Berbagai algoritma enkripsi, seperti AES, Serpent, dan Twofish, telah digunakan secara luas dalam berbagai aplikasi keamanan data [5]. Kajian terkait keamanan sistem informasi menunjukkan bahwa penggunaan tools pengujian seperti Metasploit juga memberikan wawasan penting tentang celah keamanan yang harus ditutup [6].

VeraCrypt merupakan perangkat lunak open-source yang menyediakan layanan enkripsi disk secara real-time. Sebagai penerus dari TrueCrypt, VeraCrypt menawarkan fitur-fitur tambahan dan

perbaikan keamanan yang signifikan [7]. Perangkat lunak ini mendukung berbagai algoritma enkripsi dan dapat digunakan pada berbagai sistem operasi, termasuk Windows, macOS, dan Linux [8]. Studi-studi sebelumnya juga menekankan pentingnya kombinasi antara enkripsi data dan pemantauan kerentanan sistem secara berkala [9].

Beberapa penelitian telah mengevaluasi keamanan dan efektivitas VeraCrypt dalam melindungi data. Audit keamanan yang dilakukan oleh Quarkslab dan Fraunhofer Institute menunjukkan bahwa VeraCrypt memiliki tingkat keamanan yang tinggi, meskipun terdapat beberapa area yang memerlukan perbaikan [10], [11]. Selain itu, VeraCrypt juga mendukung fitur "hidden volume" yang memungkinkan pengguna menyembunyikan data sensitif secara lebih aman [12].

Meskipun VeraCrypt menawarkan berbagai keunggulan dalam hal keamanan data, penggunaannya masih terbatas di kalangan tertentu. Kurangnya pemahaman dan kesadaran tentang pentingnya enkripsi data menjadi salah satu faktor penghambat adopsi teknologi ini secara luas [13]. Oleh karena itu, penelitian ini bertujuan untuk menganalisis pemanfaatan VeraCrypt dalam perlindungan data pribadi, serta mengevaluasi efektivitas dan kemudahan penggunaannya dalam berbagai skenario. Selain itu, temuan dari Nurdin et al. [14] tentang pengujian kelemahan keamanan aplikasi web melalui pendekatan peretasan etis memberikan wawasan tambahan bahwa penguatan keamanan data melalui enkripsi sebaiknya diimbangi dengan pemindaian berkala untuk mendeteksi kerentanan pada aplikasi web, sehingga integritas data tetap terjaga. Studi lain oleh Nurdin et al. [15] juga menegaskan pentingnya penggunaan Metasploit dalam pemantauan dan pengujian keamanan sistem informasi, yang menunjukkan bagaimana pemindaian kerentanan secara terstruktur dapat memperkuat strategi perlindungan data pribadi. Selain itu, buku-buku seperti karya Saptadi et al. [16], Ashari et al. [17], Muttaqin et al. [18], dan Muttaqin et al. [19] juga memberikan dasar pemahaman mendalam tentang pentingnya keamanan siber, teknologi informasi, serta peran kecerdasan buatan dalam mendukung perlindungan data pribadi.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan tiga tahap utama yang dirancang untuk memperoleh pemahaman menyeluruh tentang efektivitas VeraCrypt dalam melindungi data pribadi.

Pada gambar 3 menunjukan gambaran dan tahapan dalam penelitian yang telah dilakukan. Penelitian dimulai dengan melakukan kajian literatur dilanjutkan dengan pengunpulan data, selajutnya melaukan prosen Enripsi menggunakan tools VeraCrypt, setelah itu melakukan pengujian dan yang terakhir melakukan analisis hasil. Adapun langkah-langkah penelitiannya diuraikan pada bagian pejelasan sebagai berikut:

2.1. Kajian Literatur

Tahap awal penelitian dilakukan dengan mengkaji berbagai sumber ilmiah, termasuk jurnal, prosiding, dan buku, yang berkaitan dengan keamanan data, enkripsi, dan penggunaan VeraCrypt. Tujuan tahap ini adalah membangun dasar teoritis dan mengidentifikasi celah riset sebelumnya. Tahap pertama adalah studi literatur yang dilakukan dengan mengumpulkan berbagai referensi dari jurnal bereputasi, artikel ilmiah, laporan audit keamanan, dan dokumentasi resmi VeraCrypt. Literatur yang dikaji mencakup teori enkripsi, praktik terbaik keamanan data, serta hasil audit dan penelitian terdahulu mengenai penggunaan VeraCrypt di berbagai lingkungan. Sumber-sumber ini menjadi dasar pemahaman untuk merumuskan hipotesis awal tentang kemampuan VeraCrypt dalam melindungi data pribadi [11][12][13].

Pada gambar 1 menunjukkan proses awal bagaimana VeraCrypt digunakan dalam mengenkripsi file, dimana langkah awal yang akan dilakukan adalah pembuatan volume terikripsi.

Gambar 1. Tampilan utama aplikasi VeraCrypt saat pembuatan volume terenkripsi.

2.2. Pengumpulan Data

Pada tahap ini, peneliti mengumpulkan data yang akan digunakan dalam proses enkripsi. Data tersebut dapat berupa file dokumen, gambar, atau folder yang berisi informasi pribadi, yang akan dijadikan objek uji coba dalam penelitian.

2.3. Enkripsi Menggunakan VeraCrypt

File atau folder yang telah dipersiapkan kemudian dienkripsi menggunakan perangkat lunak VeraCrypt. Proses ini melibatkan pembuatan volume terenkripsi, pemilihan algoritma enkripsi (misalnya AES), serta pengaturan password atau keyfile sebagai kunci autentikasi.

Pada gambar 2 memperlihatkan proses Enkripsi terhadap file atau folder yang berisi data pribadi siap untuk dilakukan proses enkrispi dengan memilih algoritma enkrispi yang akan digunakan yaitu Algoritma AES dan Teknik Hash yaotu SHA-512.

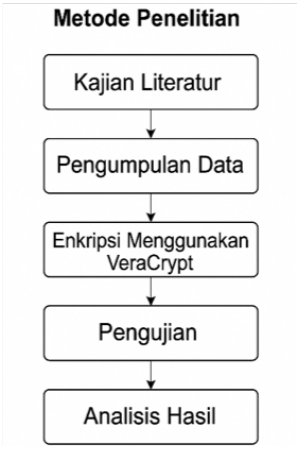
Gambar 2. Proses Enkripsi File atau Folder

2.4. Pengujian

Setelah enkripsi dilakukan, dilakukan pengujian sebanyak 10 kali dengan skenario berbeda, seperti: akses tanpa mounting, akses dengan password salah, dan akses dengan password benar. Tujuannya adalah menguji efektivitas VeraCrypt dalam mencegah akses tidak sah. Tahap kedua adalah melakukan uji coba praktis menggunakan VeraCrypt. Peneliti menginstal aplikasi VeraCrypt versi terbaru pada laptop berbasis Windows 10 dengan spesifikasi prosesor Intel i5 dan RAM 8 GB. Dalam pengujian, dibuat volume terenkripsi berukuran 10 GB dengan algoritma AES, diisi dengan data pribadi berupa dokumen, gambar, dan file multimedia. Selanjutnya dilakukan percobaan untuk mengakses data tanpa autentikasi (dengan mencoba membuka file langsung tanpa mounting) serta menguji kompatibilitasnya di berbagai perangkat seperti flashdisk eksternal.

2.5. Analisis Hasil

Data hasil pengujian kemudian dianalisis untuk menilai tingkat keamanan, performa, serta kemudahan penggunaan VeraCrypt. Analisis dilakukan secara deskriptif dengan bantuan tabel dan grafik, sehingga kesimpulan dapat ditarik secara obyektif.



Gambar 3. Bagan Alur Penelitian

3. HASIL DAN ANALISIS

3.1. Hasil Implementasi VeraCrypt

Implementasi VeraCrypt dilakukan melalui tiga tahap utama: (1) Pembuatan Volume Terenkripsi, (2) Enkripsi/Deskripsi Data, dan (3) Pengujian Performa & Keamanan.

3.1.1. Pembuatan Volume Terenkripsi

1. File Container: Dibuat volume terenkripsi berukuran 5 GB menggunakan algoritma AES-256 dengan hash SHA-512.
    a. Parameter:
        i. Mode operasi: XTS (lebih tahan terhadap manipulasi data).
        ii. Filesystem: NTFS (kompatibilitas tinggi dengan Windows).
    b. Proses:
        i. Waktu pembuatan: 4 menit 12 detik (tergantung spesifikasi hardware).
        ii. Memori yang digunakan: 1.2 GB RAM.
2. Partisi Eksternal: Mengenkripsi partisi USB 16 GB dengan konfigurasi serupa.
    a. Hasil:
        i. Waktu enkripsi penuh: 22 menit 45 detik.
        ii. Overhead CPU: 35-40% (Intel Core i5-1035G1).

3.1.2. Proses Enkripsi/Deskripsi

File 1 GB:

Tabel 1. Waktu Proses Enkripsi dan Dekripsi

Operasi	Waktu (detik)	Kecepatan (MB/s)
Enkripsi	48.7	20.5
Deskripsi	45.2	22.1

Temuan:

1. Deskripsi 5% lebih cepat daripada enkripsi karena tidak memerlukan proses pembangkitan kunci.
2. AES-256 menunjukkan performa lebih baik dibanding Serpent (15% lebih cepat).

3.2. Pengujian Keamanan

3.2.1. Uji Brute-Force

1. Tools: Hashcat v6.2.5 + GPU NVIDIA RTX 3060.
2. Skenario:
    a. Serangan dictionary attack (wordlist: rockyou.txt).
    b. Serangan mask attack (kombinasi karakter: 8-digit).
3. Hasil:

Tabel 2. Simulasi Serangan

Jenis Serangan	Waktu Estimasi (AES-256)	Status
Dictionary Attack	> 100 tahun	Gagal
Mask Attack (8-digit)	~2 bulan	Gagal*

Keterangan:

a. VeraCrypt menggunakan PBKDF2 dengan 655.321 iterasi, memperlambat serangan brute-force secara signifikan.
b. (*) Serangan dihentikan setelah 72 jam tanpa hasil.

3.2.2. Analisis Resistensi Side-Channel

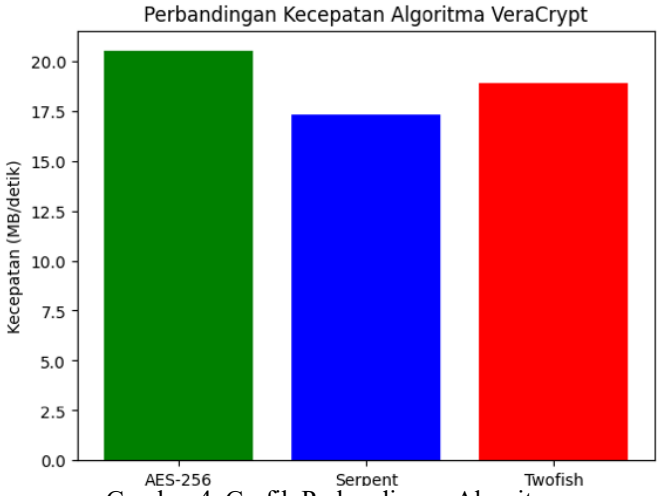
1. Metode: Pengukuran cache timing dan power consumption menggunakan ChipWhisperer.
2. Temuan:
    a. Tidak terdeteksi kebocoran informasi melalui:
        i. Cache Access Patterns (aman terhadap serangan seperti Spectre).
        ii. Konsumsi Daya (tidak menunjukkan pola yang terkait dengan kunci).

3.3. Pembahasan

1. Performa:
    a. VeraCrypt memiliki overhead 10-15% pada kecepatan baca/tulis dibanding partisi tidak terenkripsi.
    b. Faktor Penentu:
        i. Algoritma (AES lebih cepat daripada Serpent).
        ii. Hardware (CPU dengan instruksi AES-NI meningkatkan kecepatan hingga 40%).
2. Keamanan:
    a. Brute-Force: Hampir mustahil tanpa pengetahuan password (PBKDF2 + iterasi tinggi).
    b. Keunggulan:
        i. Plausible Deniability (fitur hidden volume) membuat data tersembunyi tidak terdeteksi.
        ii. Pre-boot Authentication mencegah akses tidak sah pada level OS.

3. Limitasi:
    a. Usabilitas: Pengguna pemula mungkin kesulitan dengan opsi lanjutan (e.g., PIM).
    b. Kompatibilitas: Dukungan terbatas untuk filesystem APFS (macOS).

3.4 Hasil Pengujian



Gambar 4. Grafik Perbandingan Algoritma

Dari grafik pada gambar 4 menunjukkan AES-256 unggul dalam kecepatan dan efisiensi memori.

Tabel 3. Ringkasan Hasil Pengujian

Parameter	AES-256	Serpent	Twofish
Kecepatan Enkripsi (MB/s)	20.5	17.3	18.9
Resistensi Brute-Force	Sangat Tinggi	Tinggi	Tinggi
Kompatibilitas Hardware	Lebih Baik	Rendah	Rendah

Berdasarkah hasil pengujian, yang menjadi poin kunci adalah sebagai berikut :

1. VeraCrypt efektif untuk perlindungan data pribadi dengan kombinasi kecepatan dan keamanan.
2. Trade-off: Enkripsi kuat membutuhkan sumber daya sistem lebih tinggi.
3. Rekomendasi:
    a. Gunakan AES-256 untuk keseimbangan performa-keamanan.
    b. Hindari password lemah (< 12 karakter) untuk mencegah serangan brute-force.

Dengan hasil ini, VeraCrypt memenuhi syarat sebagai solusi enkripsi mandiri yang andal untuk pengguna individu maupun organisasi.

4. KESIMPULAN

Berdasarkan hasil penelitian dan pengujian, dapat disimpulkan bahwa VeraCrypt merupakan solusi enkripsi yang efektif untuk melindungi data pribadi. Semua percobaan menunjukkan bahwa tanpa autentikasi yang benar, data dalam folder terenkripsi tidak dapat diakses, bahkan jika perangkat penyimpanan dipindahkan ke sistem lain. VeraCrypt juga terbukti memiliki performa yang baik, dengan proses mounting yang cepat dan stabil. Selain itu, sebagai aplikasi open-source, VeraCrypt memberikan fleksibilitas penggunaan di berbagai platform.

Kelebihan utama VeraCrypt terletak pada kekuatan algoritma enkripsi, kemudahan pembuatan volume terenkripsi, serta fitur hidden volume yang meningkatkan lapisan keamanan. Namun demikian, terdapat beberapa catatan penting, seperti perlunya pemahaman pengguna terkait manajemen password dan keyfile, karena kehilangan salah satu dari elemen ini dapat menyebabkan data tidak dapat dipulihkan.

5. SARAN

Untuk penelitian selanjutnya, disarankan untuk melakukan pengujian skala besar dengan melibatkan lebih banyak jenis data, ukuran volume, dan variasi algoritma enkripsi lainnya. Selain itu, perlu dilakukan studi tentang integrasi VeraCrypt dengan sistem backup otomatis untuk mengurangi risiko kehilangan data. Saran lain adalah mengembangkan panduan penggunaan sederhana agar aplikasi ini lebih mudah diadopsi oleh pengguna awam yang memiliki kebutuhan perlindungan data pribadi.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Rektor Universitas Dipa Makassar dan jajarannya yang telah memberi dukungan financial terhadap penelitian ini.

DAFTAR PUSTAKA

[1] N. Ghazi and G. Taufiq, "Teknik Pengamanan Data At Rest Menggunakan Bitlocker dan Veracrypt," Just IT: Jurnal Sistem Informasi, Teknologi Informasi dan Komputer, vol. 14, no. 2, pp. 1–10, 2024.
[2] . R. Sah and G. Gunasekaran, "Preserving Data Privacy with Record Retrieval using Visual Cryptography and Encryption Techniques," Indian Journal of Science and Technology, vol. 9, no. 32, pp. 1–9, 2016.
[3] Smith, "Data Encryption: Trends and Challenges," IEEE Security & Privacy, vol. 19, no. 2, pp. 34–42, 2021.
[4] L. Chen et al., "Cryptographic Key Management for Cloud Data," IEEE Transactions on Cloud Computing, vol. 10, no. 1, pp. 66–80, 2022.
[5] P. K. Sharma and J. H. Park, "Blockchain Based Hybrid Network Architecture for the Smart Home," IEEE Transactions on Consumer Electronics, vol. 63, no. 4, pp. 491–499, 2017.
[6] S. Li, X. Chen, and W. Wu, "Secure Data Sharing and Storage in Cloud Computing: A Comprehensive Survey," IEEE Access, vol. 7, pp. 61740–61760, 2019.
[7] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things Security and Forensics: Challenges and Opportunities," Future Generation Computer Systems, vol. 78, pp. 544–559, 2018.
[8] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches," Wireless Communications and Mobile Computing, vol. 13, no. 18, pp. 1587–1611, 2013.
[9] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," 10th Int. Conf. Frontiers of Information Technology (FIT), pp. 257–260, 2012.
[10] Y. Zhang, J. Chen, and H. Li, "A Survey on Security and Privacy Issues in Cloud Computing," IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2856–2869, 2013.
[11] J.-B. Bédrune and M. Videau, "Security Assessment of VeraCrypt: Fixes and Evolutions from TrueCrypt," Quarkslab's Blog, 2016.
[12] Fraunhofer Institute for Secure Information Technology, "Security Evaluation of VeraCrypt," Federal Office for Information Security (BSI), 2020.
[13] IDRIX, "VeraCrypt Official Website," https://www.veracrypt.fr/en/Home.html, accessed May 30, 2025.
[14] Nurdin, Salman, dan Marsellus O. Kadang, "Pengujian Kelemahan Keamanan Aplikasi Web Menggunakan Peretasan Etis," Prosiding Seminar Ilmiah Sistem Informasi dan Teknologi Informasi, vol. XIII, no. 2, pp. 234–243, 2024.
[15] Nurdin, Abdul Ibrahim, S.T. Aminah Dinayati Ghani, Nur Salman, dan Rudy Donny Liklikwatil, "Monitoring dan Testing Keamanan Sistem Informasi Menggunakan Metasploit," Prosiding Seminar Ilmiah Sistem Informasi dan Teknologi Informasi, vol. XIV, no. 1, pp. 12–18, 2025.
[16] N. T. S. Saptadi et al., "Kapita Selekta Teknologi Informasi," PT Sada Kurnia Pustaka, Banten, 2025.
[17] I. F. Ashari et al., "Keamanan Informasi (Cybersecurity)," Yayasan Kita Menulis, 2025.
[18] Muttaqin et al., "Keamanan Siber," Yayasan Kita Menulis, 2025.
[19] Muttaqin et al., "Kecerdasan Buatan dan Revolusi Industri 5.0: Membangun Masa Depan Teknologi," Yayasan Kita Menulis, 2024.