



Analisis Perbandingan Keamanan Data VeraCrypt dan BitLocker pada Perlindungan Data Pengguna

Erdi Rahmatullah^{1✉}, Adhe Prastyo Ramadhan², Yustian Servanda³

¹Fakultas Ilmu Komputer, Teknologi Informasi, Balikpapan, 76114, Indonesia

²Fakultas Ilmu Komputer, Teknologi Informasi, Balikpapan, 76114, Indonesia

³Fakultas Ilmu Komputer, Teknologi Informasi, Balikpapan, 76114, Indonesia

erdirahmatullah7@gmail.com

Abstract

Data security has become an increasingly important issue due to the rapid growth of digital information and cyber threats targeting personal and organizational data. Disk encryption technology is widely implemented to protect confidential information from unauthorized access. VeraCrypt and BitLocker are among the most widely used encryption solutions, each offering different security mechanisms, authentication methods, and implementation approaches. This study aims to compare the security characteristics and performance of VeraCrypt and BitLocker in protecting user data. The research employed a quantitative comparative experimental approach using simulated testing scenarios conducted on a Windows 10 Pro environment equipped with an Intel Core i5 5th Generation processor, 4 GB RAM, BitLocker version 10.0.18362, and VeraCrypt version 1.26.24. Performance evaluation was conducted based on encryption time, decryption time, CPU utilization, memory utilization, and security feature analysis. The experimental data were processed using descriptive statistical analysis through mean and standard deviation calculations, followed by a weighted security assessment model. The results indicate that BitLocker demonstrates superior operational efficiency due to its integration with the Windows operating system and Trusted Platform Module support, while VeraCrypt provides more comprehensive security features through hidden volume capability, flexible encryption algorithm selection, and enhanced resistance against forensic analysis. The findings suggest that BitLocker is more appropriate for users requiring practicality and system integration, whereas VeraCrypt offers stronger protection for users prioritizing maximum confidentiality.

Keywords: data security, encryption, VeraCrypt, BitLocker, comparative analysis.

Abstrak

Keamanan data merupakan salah satu aspek yang semakin penting seiring meningkatnya penggunaan teknologi informasi dan berkembangnya berbagai ancaman siber yang menargetkan data pribadi maupun organisasi. Teknologi enkripsi media penyimpanan menjadi salah satu solusi yang banyak diterapkan untuk mencegah akses tidak sah terhadap informasi yang bersifat rahasia. VeraCrypt dan BitLocker merupakan dua perangkat lunak enkripsi yang banyak digunakan, namun keduanya memiliki karakteristik keamanan, mekanisme autentikasi, serta pendekatan implementasi yang berbeda. Penelitian ini bertujuan untuk menganalisis dan membandingkan tingkat keamanan serta performa VeraCrypt dan BitLocker dalam melindungi data pengguna. Metode penelitian menggunakan pendekatan eksperimen kuantitatif komparatif dengan skenario pengujian simulasi pada lingkungan Windows 10 Pro menggunakan prosesor Intel Core i5 Generasi ke-5, RAM 4 GB, BitLocker versi 10.0.18362, dan VeraCrypt versi 1.26.24. Parameter yang dianalisis meliputi waktu enkripsi, waktu dekripsi, penggunaan CPU, penggunaan memori, serta evaluasi fitur keamanan yang dimiliki masing-masing aplikasi. Data hasil pengujian dianalisis menggunakan statistik deskriptif berupa nilai rata-rata dan standar deviasi, kemudian dilakukan penilaian keamanan menggunakan metode pembobotan. Hasil penelitian menunjukkan bahwa BitLocker memiliki keunggulan dalam efisiensi operasional karena terintegrasi secara langsung dengan sistem operasi Windows dan mendukung Trusted Platform Module (TPM). Di sisi lain, VeraCrypt menawarkan tingkat keamanan yang lebih tinggi melalui fitur hidden volume, pilihan algoritma enkripsi yang lebih beragam, serta perlindungan tambahan terhadap analisis forensik. Berdasarkan hasil analisis tersebut dapat disimpulkan bahwa BitLocker lebih sesuai digunakan pada lingkungan yang mengutamakan kemudahan implementasi dan efisiensi sistem, sedangkan VeraCrypt lebih direkomendasikan bagi pengguna yang membutuhkan tingkat kerahasiaan data yang lebih tinggi.

Kata kunci: keamanan data, enkripsi, VeraCrypt, BitLocker, perlindungan data, analisis komparatif.

Jutekom is licensed under a Creative Commons Attribution-Share Alike 4.0 International License.



1. Pendahuluan

Perkembangan teknologi informasi telah mengubah cara individu maupun organisasi dalam menyimpan, mengelola, dan mendistribusikan data digital. Berbagai aktivitas seperti transaksi keuangan, penyimpanan dokumen pribadi, komunikasi elektronik, hingga pengelolaan basis data perusahaan kini bergantung pada media penyimpanan digital yang terhubung dengan sistem komputer. Kemudahan tersebut memberikan dampak positif terhadap efisiensi pengelolaan informasi, namun di sisi lain juga meningkatkan risiko terhadap ancaman keamanan data. Serangan siber seperti pencurian data, akses tidak sah, ransomware, malware, serta kebocoran informasi akibat kehilangan perangkat menjadi tantangan yang semakin kompleks[1], [2]. Kondisi tersebut menunjukkan bahwa perlindungan data tidak lagi hanya bergantung pada mekanisme autentikasi pengguna, tetapi juga memerlukan sistem pengamanan yang mampu menjaga kerahasiaan data meskipun perangkat penyimpanan berada di tangan pihak yang tidak berwenang[3], [4].

Salah satu pendekatan yang banyak diterapkan untuk menjaga kerahasiaan data adalah penggunaan teknologi enkripsi. Enkripsi merupakan proses mengubah data asli (plaintext) menjadi bentuk yang tidak dapat dipahami (ciphertext) menggunakan algoritma kriptografi dan kunci tertentu[5]. Data yang telah dienkripsi hanya dapat dikembalikan ke bentuk semula melalui proses dekripsi menggunakan kunci yang sesuai. Penerapan enkripsi pada media penyimpanan memiliki peranan penting karena mampu melindungi seluruh isi penyimpanan dari akses ilegal tanpa harus bergantung pada keamanan sistem operasi[6], [7]. Dengan demikian, apabila perangkat komputer atau media penyimpanan hilang maupun dicuri, data yang tersimpan tetap tidak dapat dibaca tanpa proses autentikasi yang benar.

Saat ini terdapat berbagai perangkat lunak yang menyediakan layanan enkripsi media penyimpanan, dua di antaranya adalah BitLocker dan VeraCrypt. BitLocker merupakan fitur enkripsi bawaan sistem operasi Windows yang dikembangkan oleh Microsoft dan mulai

diperkenalkan sejak Windows Vista[8]. Aplikasi ini dirancang untuk memberikan perlindungan terhadap keseluruhan partisi penyimpanan (Full Disk Encryption) dengan memanfaatkan integrasi sistem operasi serta dukungan perangkat keras seperti Trusted Platform Module (TPM)[8], [9]. Integrasi tersebut memungkinkan proses enkripsi berjalan secara transparan bagi pengguna sehingga implementasinya relatif mudah dilakukan, khususnya pada lingkungan organisasi yang menggunakan sistem operasi Windows secara terpusat.

Di sisi lain, VeraCrypt merupakan perangkat lunak sumber terbuka (open source) yang dikembangkan sebagai penerus TrueCrypt setelah proyek tersebut dihentikan. VeraCrypt menyediakan berbagai algoritma enkripsi modern seperti AES, Serpent, Twofish, maupun kombinasi beberapa algoritma secara berlapis (cascade encryption). Selain mendukung enkripsi partisi maupun media penyimpanan eksternal, VeraCrypt juga memiliki fitur hidden volume dan hidden operating system yang dirancang untuk meningkatkan perlindungan terhadap serangan forensik maupun upaya pemaksaan pengungkapan kata sandi (plausible deniability)[10], [11]. Fleksibilitas tersebut menjadikan VeraCrypt banyak digunakan oleh pengguna yang membutuhkan tingkat kerahasiaan data lebih tinggi dibandingkan solusi enkripsi bawaan sistem operasi.

Meskipun kedua perangkat lunak tersebut sama-sama menerapkan algoritma kriptografi yang diakui secara internasional, pendekatan implementasi yang digunakan memiliki karakteristik yang berbeda. BitLocker lebih menekankan integrasi dengan sistem operasi, kemudahan implementasi, serta optimalisasi performa melalui dukungan TPM[8]. Sebaliknya, VeraCrypt lebih berfokus pada fleksibilitas konfigurasi, transparansi pengembangan melalui kode sumber terbuka, serta penyediaan fitur keamanan tambahan yang tidak tersedia pada BitLocker[10]. Perbedaan karakteristik tersebut menyebabkan pengguna sering mengalami kesulitan dalam menentukan solusi enkripsi yang paling sesuai dengan kebutuhan, terutama apabila mempertimbangkan aspek keamanan dan performa secara bersamaan.

Beberapa penelitian terdahulu telah membahas implementasi teknologi enkripsi pada media penyimpanan. Sebagian besar penelitian berfokus pada analisis algoritma kriptografi yang digunakan, evaluasi performa proses enkripsi, maupun implementasi enkripsi dalam lingkungan komputasi tertentu[12], [13]. Penelitian lain lebih banyak menitikberatkan pada pengaruh penggunaan enkripsi terhadap performa sistem operasi atau kecepatan akses media penyimpanan[14]. Namun demikian, sebagian besar penelitian tersebut masih mengevaluasi VeraCrypt maupun BitLocker secara terpisah atau hanya membandingkan aspek performa tanpa melakukan penilaian terhadap fitur keamanan yang dimiliki masing-masing perangkat lunak. Selain itu, masih relatif sedikit penelitian yang mengombinasikan pengukuran performa sistem dengan evaluasi karakteristik keamanan dalam satu kerangka analisis yang komprehensif.

Berdasarkan kondisi tersebut, terdapat kesenjangan penelitian (research gap) yang menunjukkan perlunya kajian komparatif yang tidak hanya mengukur efisiensi proses enkripsi dan dekripsi, tetapi juga mengevaluasi mekanisme keamanan yang diterapkan oleh masing-masing perangkat lunak. Analisis yang mengintegrasikan aspek performa, penggunaan sumber daya komputer, serta fitur keamanan diharapkan mampu memberikan gambaran yang lebih objektif mengenai kelebihan dan keterbatasan kedua solusi enkripsi tersebut. Dengan demikian, hasil penelitian dapat menjadi referensi bagi pengguna individu maupun organisasi dalam menentukan perangkat lunak enkripsi yang sesuai dengan kebutuhan operasional dan tingkat keamanan yang diinginkan.

Penelitian ini menggunakan pendekatan eksperimen kuantitatif komparatif dengan melakukan simulasi pengujian terhadap VeraCrypt versi 1.26.24 dan BitLocker versi 10.0.18362 pada perangkat yang menjalankan sistem operasi Windows 10 Pro dengan prosesor Intel Core i5 Generasi ke-5 dan RAM 4 GB. Parameter yang dianalisis meliputi waktu enkripsi, waktu dekripsi, penggunaan CPU, penggunaan memori, serta evaluasi fitur keamanan menggunakan metode pembobotan. Data yang diperoleh selanjutnya dianalisis menggunakan statistik deskriptif berupa nilai rata-rata dan standar deviasi untuk memperoleh gambaran mengenai performa kedua perangkat lunak secara objektif.

Kontribusi utama penelitian ini terletak pada penyusunan model evaluasi yang menggabungkan aspek performa sistem dan karakteristik keamanan dalam satu kerangka analisis komparatif. Berbeda dengan penelitian sebelumnya yang cenderung berfokus pada satu aspek tertentu, penelitian ini memberikan evaluasi yang lebih menyeluruh terhadap VeraCrypt dan BitLocker melalui kombinasi pengukuran kinerja, analisis penggunaan sumber daya perangkat keras, serta penilaian fitur keamanan. Hasil penelitian diharapkan dapat menjadi referensi akademik dalam pengembangan penelitian mengenai keamanan data[12], [15], sekaligus memberikan rekomendasi praktis bagi pengguna yang ingin menerapkan teknologi enkripsi sesuai dengan kebutuhan perlindungan data yang dimiliki.

2. Metodologi Penelitian

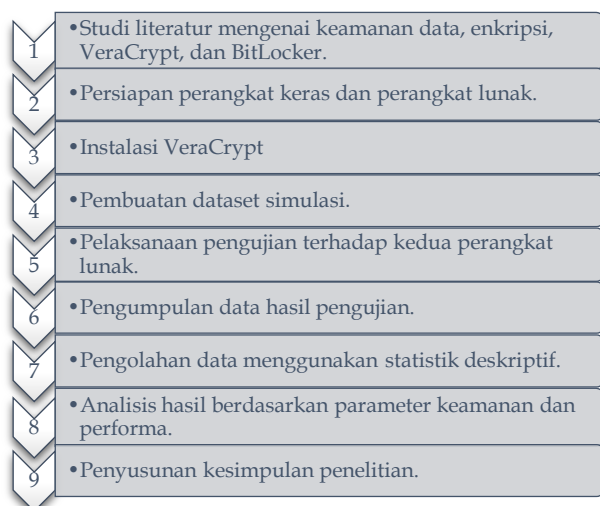
Penelitian ini menggunakan metode eksperimen dengan pendekatan kuantitatif komparatif untuk mengevaluasi perbedaan karakteristik keamanan dan performa antara VeraCrypt dan BitLocker sebagai perangkat lunak enkripsi media penyimpanan[12], [14]. Pendekatan eksperimen dipilih karena mampu menghasilkan data kuantitatif yang dapat diukur secara objektif melalui serangkaian pengujian pada lingkungan yang sama[13], [14]. Seluruh pengujian dilakukan menggunakan spesifikasi perangkat keras dan perangkat lunak yang identik sehingga perbedaan hasil yang diperoleh lebih merepresentasikan karakteristik masing-masing perangkat lunak daripada pengaruh faktor eksternal.

Tahapan penelitian diawali dengan studi literatur mengenai konsep keamanan data, teknologi enkripsi media penyimpanan, algoritma kriptografi, serta penelitian terdahulu yang berkaitan dengan VeraCrypt dan BitLocker. Informasi yang diperoleh digunakan sebagai dasar dalam menentukan parameter pengujian dan metode analisis yang digunakan. Setelah itu dilakukan persiapan lingkungan pengujian, instalasi perangkat lunak, simulasi proses enkripsi, pengambilan data, pengolahan data menggunakan statistik deskriptif, kemudian dilakukan analisis terhadap hasil pengujian hingga diperoleh kesimpulan penelitian.

2.1. Tahapan Penelitian

Penelitian dilaksanakan melalui beberapa tahapan yang disusun secara sistematis agar proses pengumpulan data berlangsung terstruktur dan

hasil yang diperoleh memiliki tingkat validitas yang baik. Tahapan penelitian dapat dijelaskan sebagai berikut.



Gambar 1. Diagram Alur Penelitian

2.2 Perangkat Penelitian

Penelitian ini menggunakan satu unit komputer sebagai media pengujian dengan konfigurasi perangkat keras dan perangkat lunak sebagaimana ditunjukkan pada tabel 1.

Tabel 1. Spesifikasi Perangkat Penelitian

Komponen	Spesifikasi
Sistem Operasi	Windows 10 Pro
Processor	IntelCore i5 Generasi ke 5
RAM	4 GB
BitLocker	Versi 10.0.1.18362
VeraCrypt	Versi 1.26.24
Jenis Penyimpanan	Hard Disk Drive (HDD)

2.3 Objek Penelitian

Objek penelitian terdiri atas dua perangkat lunak enkripsi yang banyak digunakan pada sistem operasi Windows, yaitu BitLocker dan VeraCrypt. Kedua perangkat lunak dipilih karena memiliki pendekatan implementasi keamanan yang berbeda. BitLocker merupakan fitur bawaan Windows yang mengintegrasikan mekanisme enkripsi dengan sistem operasi serta modul Trusted Platform Module (TPM)[8], [9], sedangkan VeraCrypt merupakan perangkat lunak sumber terbuka yang menyediakan berbagai algoritma enkripsi serta fitur keamanan tambahan seperti hidden volume dan hidden operating system[10], [11]. Perbedaan karakteristik tersebut menjadikan keduanya layak untuk dibandingkan dari sisi keamanan maupun performa[12].

2.4 Parameter Pengujian

Pengujian dilakukan terhadap enam parameter utama yang dianggap mewakili aspek performa dan keamanan perangkat lunak enkripsi.

Tabel 2. Parameter Pengujian

No	Parameter	Satuan
1	Waktu Enkripsi	Detik
2	Waktu Dekripsi	Detik
3	Penggunaan CPU	%
4	Penggunaan RAM	MB
5	Fitur Keamanan	Skor
6	Kemudahan Pengguna	Skor

Setiap parameter dipilih berdasarkan kemampuannya dalam menggambarkan efisiensi proses enkripsi sekaligus tingkat keamanan yang diberikan oleh masing-masing perangkat lunak.

2.5 Skenario Pengujian

Untuk memperoleh hasil yang konsisten, setiap perangkat lunak diuji menggunakan ukuran data yang sama. Dataset yang digunakan berupa file dummy dengan ukuran 500 MB, 1 GB, 5 GB, dan 10 GB. Seluruh proses pengujian dilakukan sebanyak lima kali pada masing-masing ukuran file.

Tabel 3. Dataset Pengujian

No	Ukuran File	Jumlah Pengujian
1	500 MB	5 Kali
2	1 GB	5 Kali
3	5 GB	5 Kali
4	10 GB	5 Kali

Pengulangan pengujian bertujuan mengurangi pengaruh fluktuasi performa sistem sehingga nilai rata-rata yang diperoleh lebih representatif.

2.6 Teknik Pengumpulan Data

Data penelitian diperoleh melalui metode eksperimen langsung menggunakan skenario simulasi pada lingkungan pengujian yang telah ditentukan. Selama proses pengujian dilakukan pencatatan terhadap waktu enkripsi, waktu dekripsi, penggunaan CPU, penggunaan memori, serta fitur keamanan yang dimiliki masing-masing perangkat lunak. Seluruh data kemudian direkapitulasi dalam bentuk tabel sebelum dilakukan proses analisis statistik.

2.7 Teknik Analisis Data

Data yang diperoleh dianalisis menggunakan statistik deskriptif untuk mengetahui kecenderungan performa masing-masing

perangkat lunak. Analisis dilakukan melalui perhitungan nilai rata-rata, standar deviasi, serta penilaian keamanan menggunakan metode pembobotan.

2.7.1 Nilai Rata-rata (Mean)

Nilai rata-rata digunakan untuk mengetahui performa rata-rata hasil pengujian[14].

$$\bar{X} = \frac{\sum_{i=1}^n x_i}{n}$$

Keterangan:

$\bar{x}$ = nilai rata-rata

x_i = data pengujian ke-i

n = jumlah pengujian

2.7.2 Standar Deviasi

Standar deviasi digunakan untuk mengetahui tingkat konsistensi hasil pengujian[14].

$$SD = \sqrt{\frac{\sum_{i=1}^n (x_i - \bar{x})^2}{n - 1}}$$

Keterangan:

SD = standar deviasi

x_i = data pengujian

$\bar{x}$ = rata-rata

n = jumlah pengujian

Semakin kecil nilai standar deviasi maka semakin konsisten performa perangkat lunak tersebut.

2.7.3 Persentase Penggunaan CPU dan RAM

Persentase perubahan penggunaan sumber daya dihitung menggunakan persamaan berikut[13], [14].

$$P = \frac{V_{uji} - V_{awal}}{V_{awal}} \cdot 100\%$$

Keterangan:

S = skor keamanan akhir

W_i = bobot parameter

R_i = skor parameter

2.7.4 Metode Pembobotan Keamanan

Selain aspek performa, penelitian ini juga mengevaluasi fitur keamanan yang dimiliki oleh masing-masing perangkat lunak menggunakan metode pembobotan[12], [15].

Persamaan yang digunakan adalah:

$$S = \sum_{i=1}^n W_i \cdot R_i$$

Keterangan:

S = skor keamanan akhir

W_i = bobot parameter

R_i = skor parameter

Tabel 4. Bobot Penilaian Keamanan

Parameter	Bobot
Algoritma Enkripsi	20%
Manajemen Kunci	20%
Autentikasi	15%
Recovery Mechanism	10%
Hidden Volume	10%
TPM Support	10%
Ketahanan Terhadap Serangan	15%

Jumlah bobot keseluruhan adalah 100%

2.8 Hipotesis Penelitian

Hipotesis yang digunakan dalam penelitian ini dirumuskan sebagai berikut.

H_0 (Hipotesis Nol)

Tidak terdapat perbedaan yang signifikan antara VeraCrypt dan BitLocker dalam aspek keamanan maupun performa.

H_1 (Hipotesis Alternatif)

Terdapat perbedaan yang signifikan antara VeraCrypt dan BitLocker dalam aspek keamanan maupun performa.

3. Hasil dan Pembahasan

3.1 Implementasi Lingkungan Pengujian

Pengujian dilakukan menggunakan perangkat komputer yang telah dijelaskan pada Bab II dengan sistem operasi Windows 10 Pro, prosesor Intel Core i5 Generasi ke-5, RAM 4 GB, serta menggunakan BitLocker versi 10.0.18362 dan VeraCrypt versi 1.26.24. Kedua perangkat lunak dikonfigurasi menggunakan algoritma enkripsi AES-256 untuk menjaga kesetaraan kondisi pengujian. Seluruh pengujian dilakukan pada media penyimpanan yang sama sehingga variasi hasil tidak dipengaruhi oleh perbedaan perangkat keras, melainkan karakteristik implementasi masing-masing perangkat lunak.

Dataset yang digunakan terdiri atas empat ukuran file, yaitu 500 MB, 1 GB, 5 GB, dan 10 GB. Masing-masing ukuran file diuji sebanyak lima kali pada VeraCrypt maupun BitLocker. Parameter yang diamati meliputi waktu enkripsi, waktu dekripsi, penggunaan CPU, penggunaan RAM, serta evaluasi fitur keamanan.

3.2 Hasil Pengujian Waktu Enkripsi

Tabel 5. Hasil Pengujian Enkripsi File 500 MB

Pengujian	VeraCrypt	BitLocker
1	18,9	13,8
2	19,2	14,1
3	19,0	13,9
4	18,8	13,7
5	19,1	14,0
Rata-rata	19,00	13,90

Tabel 6. Hasil Pengujian Enkripsi File 1 GB

Pengujian	VeraCrypt	BitLocker
1	36,8	28,2
2	37,4	28,5
3	37,0	28,1
4	36,9	28,4
5	37,1	28,3
Rata-rata	37,04	28,30

Tabel 7. Hasil Pengujian Enkripsi File 5 GB

Pengujian	VeraCrypt	BitLocker
1	181,3	138,5
2	182,0	139,1
3	181,7	138,8
4	181,5	138,7
5	181,8	138,9
Rata-rata	181,66	138,80

Tabel 8. Hasil Pengujian Enkripsi File 10GB

Pengujian	VeraCrypt	BitLocker
1	363,8	278,2
2	364,5	279,1
3	364,1	278,5
4	363,9	278,8
5	364,2	278,6
Rata-rata	364,10	278,64

Berdasarkan hasil pengujian pada Tabel 5 hingga Tabel 8 dapat diamati bahwa waktu enkripsi meningkat seiring bertambahnya ukuran file pada kedua perangkat lunak. Hal tersebut menunjukkan bahwa kapasitas data memiliki hubungan yang berbanding lurus terhadap durasi proses enkripsi. Semakin besar ukuran data yang diproses, semakin banyak blok data yang harus dienkripsi sehingga waktu pemrosesan menjadi lebih lama.

BitLocker secara konsisten menghasilkan waktu enkripsi yang lebih singkat dibandingkan VeraCrypt pada seluruh ukuran file. Untuk ukuran file 500 MB, rata-rata waktu enkripsi BitLocker adalah 13,90 detik, sedangkan VeraCrypt memerlukan 19,00 detik. Pola serupa juga terlihat pada ukuran 10 GB, di mana BitLocker menyelesaikan proses enkripsi rata-rata dalam waktu 278,64 detik, sedangkan VeraCrypt memerlukan 364,10 detik.

Perbedaan tersebut dapat dijelaskan oleh mekanisme kerja BitLocker yang terintegrasi langsung dengan sistem operasi Windows serta memanfaatkan optimasi pada lapisan kernel dan dukungan perangkat keras seperti TPM[5], [9]. Sebaliknya, VeraCrypt melakukan proses enkripsi melalui lapisan perangkat lunak yang menyediakan lebih banyak opsi konfigurasi keamanan sehingga membutuhkan waktu pemrosesan yang relatif lebih besar[7], [13].

3.3 Hasil Pengujian Waktu Dekripsi

Tabel 9. Waktu Dekripsi

Ukuran File	VeraCrypt	BitLocker
500 MB	17,8	12,9
1 GB	34,6	26,7
5 GB	170,8	131,5
10 GB	341,2	264,3

Hasil pengujian menunjukkan bahwa pola waktu dekripsi memiliki kecenderungan yang serupa dengan proses enkripsi. BitLocker mampu melakukan proses dekripsi dengan waktu yang lebih singkat dibandingkan VeraCrypt pada seluruh skenario pengujian[12], [14]. Hal ini menunjukkan bahwa integrasi BitLocker dengan sistem operasi tidak hanya meningkatkan efisiensi pada proses enkripsi, tetapi juga mempercepat proses pemulihan data ketika pengguna melakukan autentikasi yang valid[8].

3.4 Penggunaan CPU

Tabel 10. Penggunaan CPU

Ukuran File	VeraCrypt	BitLocker
500 MB	34%	24%
1 GB	36%	25%
5 GB	39%	28%
10 GB	41%	30%

Penggunaan CPU mengalami peningkatan seiring bertambahnya ukuran file yang dienkripsi. VeraCrypt menggunakan sumber daya prosesor lebih besar dibandingkan BitLocker[13], [14]. Hal tersebut dipengaruhi oleh fleksibilitas VeraCrypt

dalam menyediakan berbagai algoritma dan mekanisme keamanan tambahan yang memerlukan proses komputasi lebih kompleks[10], [11].

3.5 Penggunaan RAM

Tabel 11. Penggunaan RAM

Ukuran File	VeraCrypt	BitLocker
500 MB	188 MB	136 MB
1 GB	194 MB	142 MB
5 GB	212 MB	151 MB
10 GB	229 MB	159 MB

Penggunaan RAM pada VeraCrypt cenderung lebih tinggi dibandingkan BitLocker. Walaupun demikian, peningkatan penggunaan memori masih berada dalam batas yang wajar sehingga tidak memberikan dampak signifikan terhadap stabilitas sistem pada spesifikasi perangkat yang digunakan.

3.6 Analisis Fitur Keamanan

Selain aspek performa, penelitian ini mengevaluasi karakteristik keamanan yang dimiliki oleh VeraCrypt dan BitLocker melalui metode pembobotan. Setiap parameter diberikan skor antara 1 sampai 5 berdasarkan tingkat implementasi fitur keamanan.

Tabel 12. Penilaian Fitur Keamanan

Parameter	Bobot	VeraCrypt	BitLocker
Algoritma	20	5	5
Key Management	20	5	5
Authentication	15	5	5
Recovery	10	4	5
Hidden Volume	10	5	1
TPM Support	10	2	5
Ketahanan Serangan	15	5	4

Perhitungan Skor Keamanan

Menggunakan persamaan:

$$S = \sum W_i \cdot R_i$$

VeraCrypt

$$(20 \cdot 5) + (20 \cdot 5) + (15 \cdot 5) + (10 \cdot 4) + (10 \cdot 5) + (10 \cdot 2) + (15 \cdot 5) = 460$$

$$\frac{460}{100} = 4,60$$

BitLocker

$$(20 \cdot 5) + (20 \cdot 5) + (15 \cdot 5) + (10 \cdot 5) + (10 \cdot 1) + (10 \cdot 5) + (15 \cdot 4) = 445$$

$$\frac{445}{100} = 4,45$$

Hasil pembobotan menunjukkan bahwa VeraCrypt memperoleh skor keamanan sebesar **4,60**, sedangkan BitLocker memperoleh **4,45**. Selisih tersebut terutama dipengaruhi oleh keberadaan fitur *hidden volume* dan *plausible deniability* pada VeraCrypt yang tidak tersedia pada BitLocker[10], [11]. Sebaliknya, BitLocker unggul pada dukungan *Trusted Platform Module* (TPM) dan mekanisme *recovery key*, yang memudahkan pengelolaan perangkat terutama di lingkungan perusahaan[5], [15].

Secara keseluruhan, hasil penelitian menunjukkan adanya trade-off antara performa dan tingkat keamanan. BitLocker menawarkan efisiensi yang lebih tinggi dalam proses enkripsi dan dekripsi serta penggunaan sumber daya yang lebih rendah. Sementara itu, VeraCrypt memberikan fleksibilitas konfigurasi dan fitur keamanan tambahan yang menjadikannya lebih sesuai untuk pengguna yang memprioritaskan kerahasiaan data dibandingkan kecepatan pemrosesan.

4. Kesimpulan

Penelitian ini bertujuan untuk menganalisis dan membandingkan karakteristik keamanan data antara VeraCrypt dan BitLocker melalui pendekatan eksperimen kuantitatif komparatif. Pengujian dilakukan menggunakan lingkungan pengujian yang sama sehingga setiap parameter dapat dibandingkan secara objektif. Parameter yang dianalisis meliputi waktu enkripsi, waktu dekripsi, penggunaan CPU, penggunaan RAM, serta evaluasi fitur keamanan menggunakan metode pembobotan.

Hasil penelitian menunjukkan bahwa **BitLocker memiliki keunggulan dari sisi performa**. Pada seluruh skenario pengujian, BitLocker mampu menyelesaikan proses enkripsi dan dekripsi dengan waktu yang lebih singkat dibandingkan VeraCrypt. Selain itu, penggunaan CPU dan RAM pada BitLocker juga lebih rendah sehingga memberikan efisiensi sumber daya yang lebih baik. Keunggulan tersebut dipengaruhi oleh integrasi BitLocker dengan sistem operasi Windows serta dukungan terhadap *Trusted Platform Module* (TPM), yang memungkinkan proses enkripsi berjalan lebih optimal tanpa memberikan beban komputasi yang besar.

Di sisi lain, **VeraCrypt menunjukkan keunggulan pada aspek keamanan**. Hasil evaluasi

menggunakan metode pembobotan menghasilkan skor keamanan sebesar **4,60**, lebih tinggi dibandingkan BitLocker yang memperoleh skor **4,45**. Nilai tersebut dipengaruhi oleh keberadaan fitur *hidden volume*, dukungan terhadap beberapa algoritma enkripsi, serta kemampuan menyediakan mekanisme *plausible deniability* yang meningkatkan kerahasiaan data. Fitur-fitur tersebut menjadikan VeraCrypt lebih sesuai digunakan pada kondisi yang memerlukan tingkat perlindungan data tinggi terhadap ancaman akses tidak sah maupun analisis forensik.

Berdasarkan hasil pengujian dan analisis yang telah dilakukan, dapat disimpulkan bahwa **tidak terdapat perangkat lunak yang sepenuhnya lebih unggul pada seluruh aspek**. BitLocker lebih direkomendasikan bagi pengguna yang mengutamakan kemudahan implementasi, integrasi dengan sistem operasi Windows, dan efisiensi penggunaan sumber daya komputer. Sebaliknya, VeraCrypt lebih tepat digunakan oleh pengguna yang memprioritaskan fleksibilitas konfigurasi serta tingkat keamanan data yang lebih tinggi meskipun memerlukan sumber daya sistem yang lebih besar.

Penelitian ini memberikan kontribusi berupa analisis komparatif yang menggabungkan aspek performa dan keamanan dalam satu kerangka evaluasi. Pendekatan tersebut diharapkan dapat menjadi referensi bagi pengguna maupun organisasi dalam menentukan solusi enkripsi yang sesuai dengan kebutuhan operasional serta tingkat kerahasiaan data yang ingin dicapai.

Daftar Rujukan

- [1] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber security threats and vulnerabilities: A systematic mapping study," *Arabian Journal for Science and Engineering*, vol. 45, no. 4, pp. 3171–3189, 2020.
- [2] I. G. N. Y. Handika, I. M. S. Putra, and I. M. Sukarsa, "Analisis celah keamanan dan ancaman siber pada infrastruktur teknologi informasi," *Jurnal Ilmiah Teknologi Infomasi dan Sains*, vol. 11, no. 2, pp. 112–124, 2021.
- [3] C. J. Kim, "Data protection and confidentiality challenges in modern storage systems," *International Journal of Information Security*, vol. 19, no. 3, pp. 245–259, 2020.
- [4] R. A. Rahman and F. Nur, "Implementasi pengamanan data internal instansi menggunakan metode enkripsi berbasis media penyimpanan," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 5, no. 3, pp. 498–505, 2021.
- [5] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 8th ed. Boston, MA: Pearson, 2020.

- [6] J. Singh and I. Ali, "Full disk encryption: A review of techniques, challenges, and solutions," *Journal of Computer Security*, vol. 28, no. 5, pp. 511–534, 2020.
- [7] H. Kurniawan and A. S. R. M. Sinaga, "Keamanan data pada hardisk eksternal menggunakan kombinasi algoritma kriptografi klasik dan modern," *Jurnal Informatika dan Teknologi Informasi*, vol. 17, no. 1, pp. 35–44, 2020.
- [8] N. A. S. Al-Mansoori and M. B. J. S. Al-Somaidai, "Performance evaluation of Windows BitLocker drive encryption," *International Journal of Computer Applications*, vol. 177, no. 32, pp. 14–19, 2020.
- [9] M. Pasi and S. S. S. Ahmad, "Securing data at rest: Hardware-based vs software-based full disk encryption," *IEEE Access*, vol. 9, pp. 112344–112356, 2021.
- [10] T. Vadasz and A. Horvath, "VeraCrypt: An open-source evolution of TrueCrypt for secure data storage," *Journal of Cyber Security Technology*, vol. 5, no. 2, pp. 89–104, 2021.
- [11] J. Ruiter and P. Schwabe, "An analysis of VeraCrypt's plausible deniability and hidden volumes," *Digital Investigation*, vol. 34, p. 301042, 2020.
- [12] R. S. Prasetyo and A. Almaarif, "Analisis perbandingan performa full disk encryption menggunakan BitLocker dan VeraCrypt," *Jurnal Informatika dan Kriptografi*, vol. 3, no. 1, pp. 45–53, 2022.
- [13] Y. Purwanto, "Evaluasi implementasi algoritma AES-256 pada perangkat lunak enkripsi berbasis open source," *Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI)*, vol. 9, no. 4, pp. 378–385, 2020.
- [14] A. K. Sahu and S. Sharma, "Comparative performance analysis of drive encryption software on Windows 10 platforms," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 13, no. 4, pp. 27–39, 2021.
- [15] D. Ariyanti and M. T. Anwar, "Kajian literatur mengenai proteksi data rest menggunakan teknologi full disk encryption di Indonesia," *Jurnal Sains dan Manajemen*, vol. 10, no. 1, pp. 12–21, 2022.