JOURNAL OF INFORMATION SYSTEMS AND TECHNOLOGY

**Journal of Information Systems and Technology**
Vol., No. (2025), 80-91
e-ISSN: 3110-4096
Journal homepage: https://athallahpublishing.com/index.php/jistech

*Research Paper*

# Implementasi dan Evaluasi Keamanan Data at Rest Menggunakan BitLocker dan VeraCrypt

Erina Malinda Lubis
Institut Teknologi Sepuluh Nopember, Indonesia
*Corresponding author: lubismlnd@gmail.com

**ARTICLE INFO**

**Kata Kunci**
Bitlocker
Data At Rest
Enkripsi Disk
Keamanan Data
Veracrypt

**Article history**
Received: 12 Agustus 2025
Revised: 25 September 2025
Accepted: 15 Oktober 2025
Available online: 14 Desember 2025

**ABSTRACT**

Keamanan data at rest merupakan aspek krusial dalam perlindungan informasi digital, khususnya pada perangkat penyimpanan yang rentan terhadap akses tidak sah akibat pencurian, kehilangan perangkat, maupun serangan siber. Enkripsi disk penuh menjadi salah satu solusi utama untuk menjaga kerahasiaan dan integritas data. Penelitian ini bertujuan untuk mengimplementasikan serta mengevaluasi tingkat keamanan data at rest menggunakan dua teknologi enkripsi populer, yaitu BitLocker dan VeraCrypt. Metode penelitian yang digunakan meliputi implementasi BitLocker dan VeraCrypt pada media penyimpanan dengan skenario pengujian yang sama, diikuti dengan evaluasi keamanan dan kinerja sistem. Parameter evaluasi mencakup mekanisme enkripsi, autentikasi, manajemen kunci, dampak terhadap performa sistem, serta ketahanan terhadap upaya akses tidak sah. Pengujian dilakukan melalui simulasi serangan dasar dan analisis akses data tanpa kredensial yang sah. Hasil penelitian menunjukkan bahwa baik BitLocker maupun VeraCrypt mampu memberikan perlindungan yang efektif terhadap data at rest. BitLocker unggul dalam kemudahan integrasi dan efisiensi kinerja pada sistem operasi Windows, sedangkan VeraCrypt menawarkan fleksibilitas konfigurasi dan opsi keamanan yang lebih beragam. Temuan ini menegaskan bahwa pemilihan teknologi enkripsi data at rest perlu disesuaikan dengan kebutuhan keamanan, lingkungan sistem, dan tingkat kontrol pengguna. Penelitian ini diharapkan dapat menjadi referensi dalam penerapan enkripsi data at rest untuk meningkatkan keamanan informasi.

## Pendahuluan

Belum lama ini terjadi banyak kasus kebocoran data seperti source code Twitter yang disebar di github, AI milik Meta yang bocor di forum internet hingga data pelanggan indihome yang diduga bocor. Hal ini dapat terjadi karena adanya celah keamanan dalam penyimpanan data. Oleh karenanya pengamanan data menjadi salah satu usaha yang penting untuk menjaga data pribadi / perusahaan sehingga tidak dapat diakses oleh pihak yang tak berwenang. Salah satu usaha yang dapat dilakukan untuk mengamankan data ialah dengan melakukan enkripsi (Fathiyana, 2021). Penggunaan Enkripsi yang tepat dapat membuatnya tidak dapat dilihat konten datanya (Ocenas et al., 2020). Salah satu aplikasi yang dapat dipakai adalah Bitlocker dan VeraCrypt. BitLocker sendiri merupakan sebuah fitur enkripsi full-disk yang telah tersedia dalam sistem operasi Microsoft Windows, baik versi Ultimate maupun Enterprise yang didesain untuk melindungi data dengan melakukan enkripsi terhadap keseluruhan partisi (Yusroni & Anton, 2022). 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. (IDRIX, 2022). VeraCrypt juga memiliki peningkatan keamanan yang signifikan berdasarkan TrueCrypt, yang meningkatkan kompleksitas dalam memecahkan kata sandi sebesar 10 hingga sekitar 300 kali lipat (Tan et al., 2020).

Perkembangan teknologi informasi dan komunikasi yang sangat pesat telah mendorong meningkatnya ketergantungan individu maupun organisasi terhadap data digital. Data tidak hanya menjadi aset strategis dalam mendukung pengambilan keputusan, operasional bisnis, dan layanan publik, tetapi juga menyimpan informasi sensitif yang bernilai tinggi, seperti data pribadi, data keuangan, serta informasi rahasia institusi. Seiring dengan meningkatnya volume dan nilai data, risiko terhadap ancaman keamanan informasi juga semakin kompleks dan beragam. Salah satu aspek penting dalam keamanan informasi adalah perlindungan data at rest, yaitu data yang tersimpan pada media penyimpanan seperti hard disk, solid state drive, maupun media eksternal. Data at rest menjadi target yang rentan terhadap berbagai ancaman, terutama ketika perangkat penyimpanan hilang, dicuri, atau diakses oleh pihak yang tidak berwenang. Tanpa mekanisme pengamanan yang memadai, data yang tersimpan dapat dengan mudah dieksploitasi, dimodifikasi, atau disalahgunakan, sehingga menimbulkan kerugian finansial, pelanggaran privasi, dan penurunan kepercayaan terhadap sistem informasi.

Berbagai standar dan regulasi keamanan informasi, baik di tingkat nasional maupun internasional, menekankan pentingnya perlindungan data at rest sebagai bagian dari strategi keamanan menyeluruh. Enkripsi menjadi salah satu metode paling efektif dalam menjaga kerahasiaan data, karena mampu mengubah data menjadi bentuk yang tidak dapat dibaca tanpa kunci atau kredensial yang sah. Oleh karena itu, penerapan enkripsi pada media penyimpanan merupakan langkah strategis untuk mencegah akses tidak sah terhadap data sensitif. Di lingkungan sistem operasi modern, terdapat berbagai teknologi enkripsi disk yang dirancang untuk melindungi data at rest. Dua di antaranya yang banyak digunakan adalah BitLocker dan VeraCrypt. BitLocker merupakan solusi enkripsi bawaan dari sistem operasi Windows yang menawarkan integrasi erat dengan sistem, kemudahan implementasi, serta dukungan terhadap modul keamanan perangkat keras seperti Trusted Platform Module (TPM). Sementara itu, VeraCrypt merupakan perangkat lunak enkripsi sumber terbuka yang dikenal dengan fleksibilitas konfigurasi, pilihan algoritma enkripsi yang beragam, serta kemampuan lintas platform.

Meskipun keduanya memiliki tujuan yang sama, yaitu melindungi data at rest, BitLocker dan VeraCrypt memiliki karakteristik, mekanisme keamanan, serta implikasi kinerja yang berbeda. Perbedaan ini menimbulkan kebutuhan untuk melakukan kajian yang komprehensif mengenai implementasi dan tingkat keamanan masing-masing teknologi, khususnya dalam konteks penggunaan nyata pada sistem penyimpanan. Evaluasi terhadap aspek keamanan, kemudahan penggunaan, dan dampak terhadap performa sistem menjadi penting agar pengguna dan organisasi dapat menentukan solusi enkripsi yang paling sesuai dengan kebutuhan dan lingkungan operasional mereka. Berdasarkan latar belakang tersebut, penelitian ini difokuskan pada implementasi dan evaluasi keamanan data at rest menggunakan BitLocker dan VeraCrypt. Penelitian ini bertujuan untuk memberikan gambaran yang mendalam mengenai mekanisme kerja kedua teknologi enkripsi, menilai efektivitasnya dalam melindungi data dari akses tidak sah, serta menganalisis kelebihan dan keterbatasan masing-masing solusi. Dengan demikian, hasil penelitian ini diharapkan dapat menjadi referensi akademik dan praktis dalam pengambilan keputusan terkait penerapan enkripsi data at rest guna meningkatkan keamanan informasi secara menyeluruh.

## Metode

Pada pengumpulan data dalam penelitian ini, penulis menggunakan metode observasi dan studi pustaka.Dalam Observasi, penulis melakukan pengamatan dan melakukan enkripsi secara langsung dengan menggunakan perangkat lunak BitLocker dan Veracrypt yang terdapat pada laptop penulis, untuk mendapatkan informasi mengenai perbedaan serta kelebihan dan kekurangan kedua perangkat lunak tersebut. Pada pengumpulan data dengan studi pustaka, penulis menggunakan sumber referensi berupa artikel internet, prosiding seminar dan jurnal penelitian terkait judul yang diangkat. Penelitian ini menggunakan pendekatan eksperimental dan deskriptif-analitis yang bertujuan untuk mengimplementasikan serta mengevaluasi keamanan data at rest menggunakan teknologi enkripsi BitLocker dan VeraCrypt. Metode penelitian disusun

secara sistematis agar mampu memberikan gambaran yang komprehensif mengenai mekanisme, tingkat keamanan, dan dampak penerapan kedua solusi enkripsi tersebut pada media penyimpanan.

Tahap awal penelitian diawali dengan studi literatur yang mendalam terhadap konsep keamanan informasi, khususnya perlindungan data at rest, prinsip enkripsi disk, serta karakteristik teknis BitLocker dan VeraCrypt. Literatur yang digunakan meliputi buku teks, artikel jurnal ilmiah, standar keamanan informasi, dan dokumentasi resmi dari masing-masing teknologi. Studi literatur ini bertujuan untuk membangun landasan teoretis, menentukan parameter evaluasi, serta merumuskan skenario pengujian yang relevan. Selanjutnya, dilakukan perancangan lingkungan pengujian yang mencakup penyiapan perangkat keras dan perangkat lunak. Lingkungan uji dirancang menggunakan sistem operasi yang kompatibel dengan BitLocker dan VeraCrypt, serta media penyimpanan yang sama untuk memastikan kesetaraan kondisi pengujian. Pada tahap ini juga ditentukan konfigurasi enkripsi, termasuk metode autentikasi, algoritma enkripsi, dan skema manajemen kunci yang akan digunakan pada masing-masing teknologi.

Tahap berikutnya adalah implementasi enkripsi data at rest. BitLocker dan VeraCrypt diterapkan secara terpisah pada media penyimpanan dengan mengikuti prosedur standar dan praktik terbaik yang direkomendasikan. Proses implementasi mencakup aktivasi enkripsi, pengaturan kata sandi atau kunci pemulihan, serta verifikasi keberhasilan enkripsi. Setiap tahapan implementasi didokumentasikan untuk memudahkan analisis perbandingan. Setelah implementasi selesai, penelitian dilanjutkan dengan pengujian keamanan dan kinerja sistem. Pengujian keamanan dilakukan dengan mensimulasikan skenario akses tidak sah, seperti upaya membaca data tanpa kredensial yang valid dan percobaan pemulihan data secara ilegal. Sementara itu, pengujian kinerja difokuskan pada pengamatan dampak enkripsi terhadap waktu akses data, kecepatan baca-tulis, serta respons sistem selama penggunaan normal.

Data yang diperoleh dari proses pengujian kemudian dianalisis menggunakan pendekatan analisis deskriptif-komparatif. Hasil pengujian BitLocker dan VeraCrypt dibandingkan berdasarkan parameter keamanan, kemudahan penggunaan, fleksibilitas konfigurasi, dan pengaruh terhadap performa sistem. Analisis ini bertujuan untuk mengidentifikasi kelebihan dan keterbatasan masing-masing teknologi dalam konteks pengamanan data at rest. Tahap akhir penelitian adalah evaluasi dan penarikan kesimpulan. Pada tahap ini dilakukan sintesis hasil analisis untuk menjawab tujuan penelitian serta memberikan rekomendasi terkait pemilihan teknologi enkripsi data at rest yang sesuai dengan kebutuhan pengguna atau organisasi. Metode penelitian ini diharapkan mampu menghasilkan temuan yang objektif dan aplikatif dalam meningkatkan praktik keamanan data melalui penerapan enkripsi disk yang efektif.

## Hasil dan Pembahasan

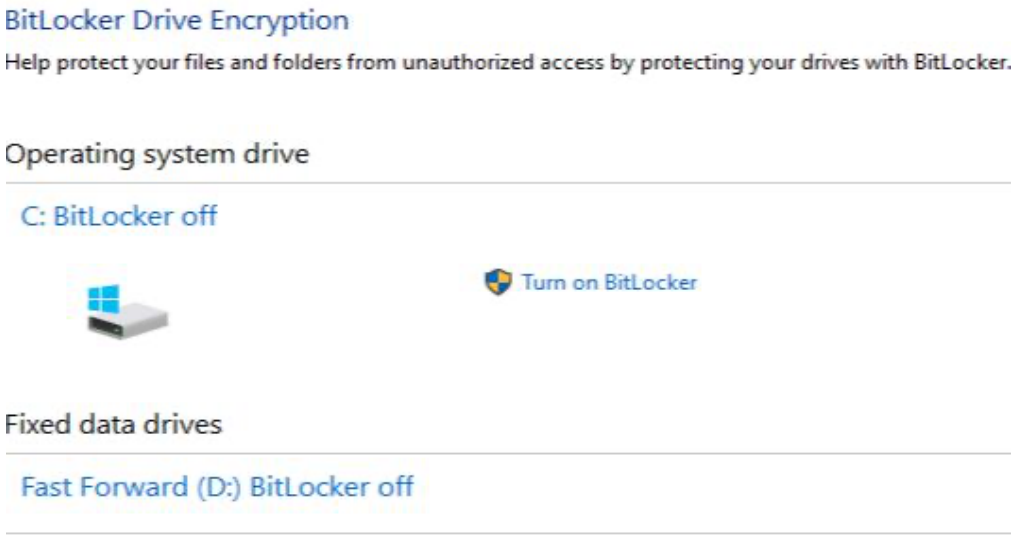
### Melakukan pengamanan data dengan BitLocker

BitLocker merupakan fitur enkripsi bawaan pada sistem operasi Windows yang dirancang untuk melindungi data dengan cara mengenkripsi seluruh isi media

penyimpanan. Pengamanan data dengan BitLocker bertujuan untuk mencegah akses tidak sah terhadap informasi, khususnya ketika perangkat hilang, dicuri, atau diakses oleh pihak yang tidak berwenang. Dengan enkripsi penuh pada drive, data yang tersimpan akan tetap aman meskipun media penyimpanan dilepas dan dihubungkan ke perangkat lain. Proses pengamanan data dengan BitLocker dimulai dengan aktivasi fitur BitLocker pada drive sistem maupun drive penyimpanan lainnya. BitLocker menggunakan algoritma enkripsi yang kuat, seperti Advanced Encryption Standard (AES), untuk mengamankan data. Kunci enkripsi disimpan dan dikelola secara aman, baik melalui Trusted Platform Module (TPM) pada perangkat keras maupun melalui metode autentikasi tambahan seperti kata sandi atau kunci pemulihan. Penggunaan TPM memungkinkan BitLocker memverifikasi integritas sistem saat proses booting, sehingga mencegah manipulasi sistem sebelum sistem operasi dijalankan.

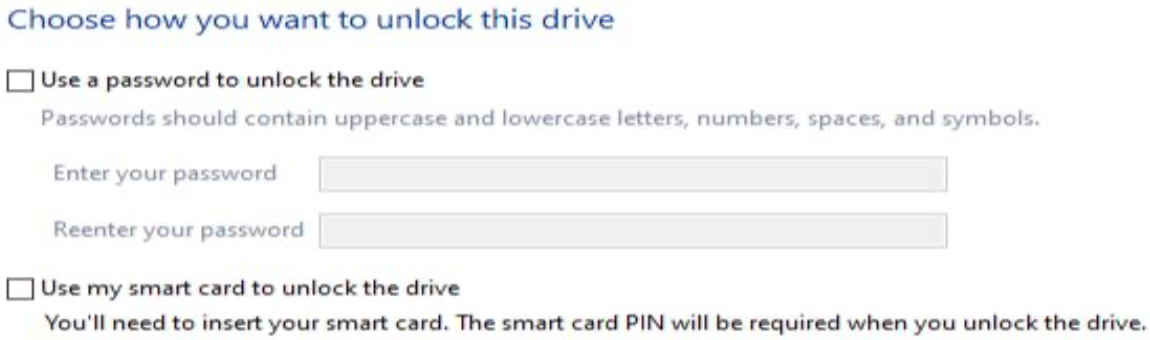
Setelah BitLocker diaktifkan, seluruh data pada drive akan dienkripsi secara otomatis tanpa mengganggu aktivitas pengguna secara signifikan. Proses enkripsi berjalan di latar belakang dan hanya memerlukan waktu awal hingga seluruh data terlindungi. Selanjutnya, pengguna dapat mengakses data seperti biasa selama autentikasi berhasil, sementara pihak yang tidak memiliki kredensial yang sah tidak akan dapat membaca atau memodifikasi data tersebut. Dengan menerapkan BitLocker, organisasi maupun individu dapat meningkatkan tingkat keamanan data at rest secara signifikan. Selain melindungi kerahasiaan data, BitLocker juga membantu memenuhi standar dan kebijakan keamanan informasi yang menuntut perlindungan data sensitif. Oleh karena itu, pengamanan data menggunakan BitLocker menjadi solusi praktis dan efektif dalam menjaga keamanan informasi pada perangkat berbasis Windows.

Bitlocker dapat diakses pada Control Panel > System and Security > BitLocker Drive Encryption atau menggunakan search bawaan windows dengan kata kunci BitLocker. Dalam melakukan pengamanan data dengan Bitlocker setidaknya terdapatbeberapa proses /tahapan yakni pemberian *password* enkripsi, penyalinan kunci Recovery, pemilihan metode enkripsi dan pemilihan versi enkripsi.




Gambar. 1. Tampilan Bitlocker pada *Control Panel*

Pada tahap pertama merupakan proses pemilihan dalam mengamankan partisi yakni dapat menggunakan password atau smartcard.




Gambar. 2. Tampilan Penginputan Password dan Penggunaan Smartcard

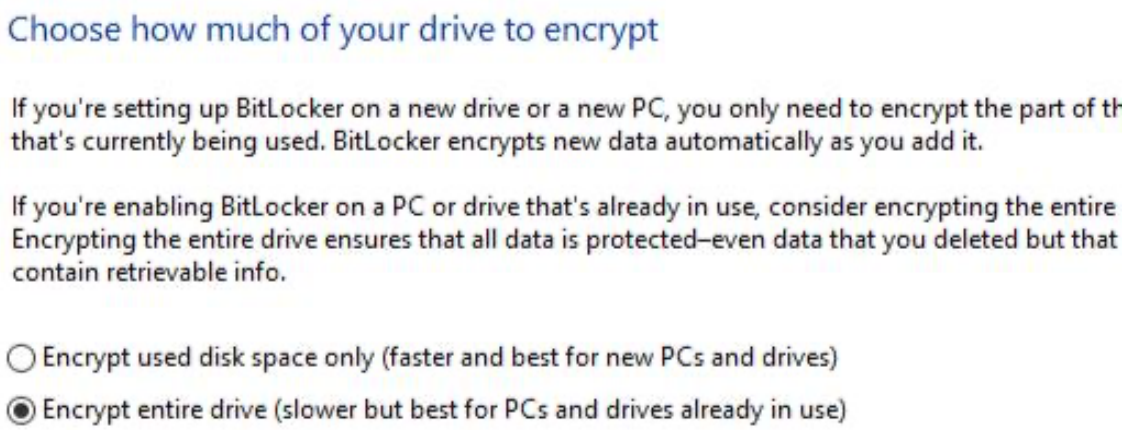
Pada tahap kedua di gambar 3 adalah proses untuk menyimpan salinan kunci *Recovery* untuk dapat melakukan *reset password* ketika lupa dengan *password* yang telah ditentukan sebelumnya.


Gambar. 3. Tampilan Penyalinan Kunci *Recovery*

Pada tahap ketiga di gambar 4 berikut, merupakan pemilihan metode enkripsi pada disk, apakah ingin mengenkripsi data yang terpakai saja di drive atau ingin mengenkripsi satu drive penuh. Tampilan penyalinan kunci pemulihan (Recovery Key) pada BitLocker merupakan tahap penting dalam proses pengamanan data. Kunci pemulihan ini berfungsi sebagai cadangan akses apabila pengguna tidak dapat membuka drive terenkripsi melalui metode autentikasi utama, misalnya karena lupa kata sandi, perubahan perangkat keras, atau kegagalan sistem. Pada saat BitLocker diaktifkan, sistem akan menampilkan halaman yang meminta pengguna untuk menyimpan atau menyalin kunci Recovery. Kunci ini biasanya berupa deretan angka unik yang bersifat rahasia dan hanya dapat digunakan oleh pemilik yang sah. Tampilan ini memberikan beberapa opsi penyimpanan, seperti

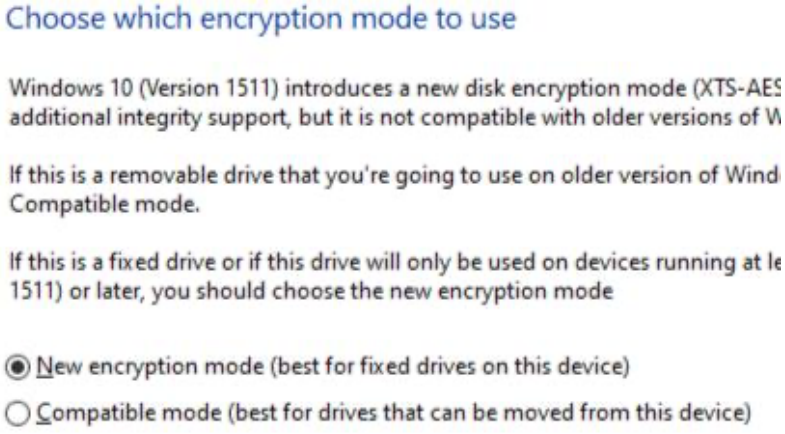
menyimpan ke akun Microsoft, menyimpan ke file, mencetak kunci, atau menyalinnya secara manual ke media yang aman.

Penyalinan kunci Recovery bertujuan untuk memastikan bahwa data tetap dapat diakses dalam kondisi darurat tanpa mengorbankan keamanan. Pada tahap ini, pengguna dianjurkan untuk menyimpan kunci tersebut di lokasi yang terpisah dari perangkat yang dienkripsi, seperti penyimpanan eksternal atau sistem manajemen kunci yang aman. Hal ini mencegah pihak tidak berwenang memperoleh akses ke data jika perangkat utama jatuh ke tangan yang salah. Dengan adanya tampilan penyalinan kunci Recovery, BitLocker menekankan keseimbangan antara keamanan dan ketersediaan data. Pengguna tetap mendapatkan perlindungan maksimal melalui enkripsi, sekaligus memiliki mekanisme pemulihan yang andal apabila terjadi gangguan akses. Oleh karena itu, tahap ini tidak boleh dilewati dan harus dilakukan dengan penuh kehati-hatian untuk menjaga keamanan data secara menyeluruh.




Gambar. 4. Tampilan Pemilihan Metode Enkripsi

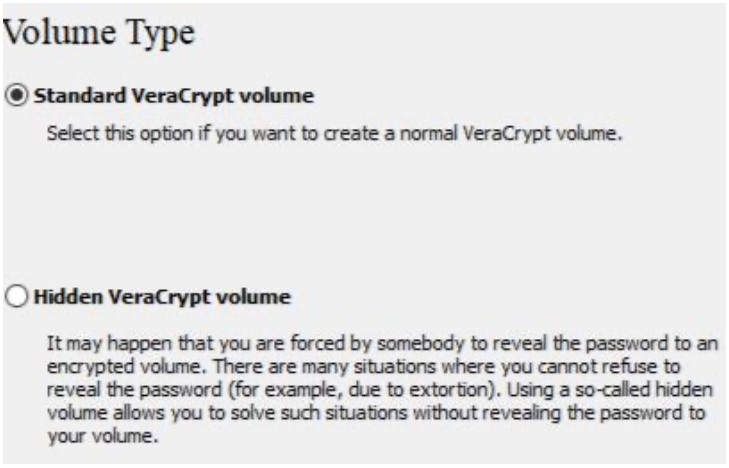
Dalam tahap terakhir sebelum memulai proses enkripsi, pada gambar 5 yakni untuk memilih versi enkripsi versi baru (yang dapat dipakai Windows 10 versi 1511 keatas) atau versi kompatibilitas (versi windows sebelum windows 10).




Gambar. 5. Tampilan Pemilihan Versi Enkripsi

**Melakukan pengamanan data dengan VeraCrypt**

Dalam melakukan pengamanan data pada VeraCrypt setidaknya terdapat 9 tahapan yang harus dilalui, mulai dari Pemilihan pembuatan enkripsi, pemilihan jenis volume, memilih partisi atau volume yang ingin di enkripsi, pemilihan mode enkripsi, pemilihan algoritma enkripsi dan algoritma hash, pemilihan dalam mengamankan enkripsi (password atau file kunci), pengumpulan data acak, penggunaan mode wipe serta yang terakhir konfirmasi sebelum memulai proses enkripsi.Berikut merupakan tampilan awal aplikasi Veracrypt**.** Tahap pertama pada gambar 6 merupakan proses pemilihan pembuatan enkripsi, terdapat 3 pilihan yakni membuat *file container* baru dengan ekstensi veracrypt, menggunakan partisi non sistem dan menggunakan partisi sistem.




Gambar 6. Tampilan pemilihan jenis volume

Pada tahap keempat di gambar 6, merupakan tampilan untuk memilih pembuatan mode enkripsi, yang pertama enkripsi lalu *format* yang kedua hanya mengenkripsi saja.

**Perbedaan Bitlocker dengan VeraCrypt**

Setelah melakukan pengamanan data dengan kedua perangkat lunak BitLocker dan VeraCrypt. Terdapat beberapa perbedaan yakni:

1. Pada dukungan Sistem Operasi, BitLocker hanya dapat dipakai di Windows OS pada edisi Pro, education dan Enterprise untuk windows 8, 8.1, 10 dan 11; pada edisi Ultimate dan Enterprise untuk windows 7 dan vista; dan pada edisi windows server 2008 keatas. Sedangkan VeraCrypt dapat digunakan pada Windows, Mac OS dan Linux.

2. Pada sisi Source code, VeraCrypt bersifat open source (Addlesee, 2022), sehingga komunitas atau siapa saja dapat berkontribusi dalam pengembangan VeraCrypt. Sedangkan BitLocker bersifat closed source.

3. Pada Algoritma enkripsi, VeraCrypt memberikan banyak pilihan algoritma. AES, Serpent, Twofish, Carnellia, Kuznyechik, AES(TwoFish) dan lain-lain. Sedangkan BitLocker hanya memberikan 2 pilihan algoritma saja yakni AES dan XTS-AES.

4. Dalam melakukan penguncian enkripsi, BitLocker dapat menggunakan password atau pun smartcard. Sedangkan VeraCrypt menggunakan password atau pun file kunci.
5. Dalam melakukan tahapan enkripsi pada partisi atau disk, VeraCypt memiliki tahapan yang panjang serta memiliki banyak pilihan pada saat melakukan enkripsi. Sedangkan BitLocker memiliki tahapan yang sedikit serta pilihan yang tidak terlalu banyak.

Pada Bitlocker sendiri memiliki kelebihan yakni berupa *tool* resmi bawaan windows, memiliki kunci Recovery untuk melakukan reset jika lupa dengan password enkripsi serta memiliki tahapan proses yang lebih cepat dan mudah. Untuk kekurangannya sendiri walau tool ini bawaan windows namun tidak dapat dipakai di Sistem operasi lain dan tidak dapat juga dipakai disemua edisi windows, memiliki pilihan algoritma enkripsi yang sedikit serta jika kunci recovery ditempatkan di folder yang rentan, maka partisi yang dienkripsi oleh BitLocker dapat dibuka dengan mudah. Sedangkan pada VeraCrypt unggul dalam dukungan operasi sistem yang berbeda (Linux, MacOS, windows), Source code aplikasi bersifat open source serta memiliki banyak pilihan algoritma enkripsi. Namun Veracrypt juga memiliki kekurangan dalam hal tahapan proses enkripsi yang panjang dan banyak pilihan, tidak memiliki kunci recovery seperti bitlocker serta partisi / disk yang telah dienkripsi oleh Veracrypt tidak bisa diakses langsung oleh OS namun harus melalui perantara aplikasi Veracrypt.

**Pembahasan**

Pembahasan dalam penelitian ini difokuskan pada analisis hasil implementasi dan evaluasi keamanan data at rest menggunakan BitLocker dan VeraCrypt sebagai solusi enkripsi disk penuh. Kedua teknologi tersebut diuji dalam lingkungan dan skenario yang setara untuk memperoleh gambaran yang objektif mengenai tingkat keamanan, kemudahan penggunaan, serta dampaknya terhadap kinerja sistem. Hasil implementasi menunjukkan bahwa BitLocker menawarkan kemudahan integrasi yang tinggi, khususnya pada sistem operasi Windows. Sebagai fitur bawaan, BitLocker dapat diaktifkan dengan relatif cepat dan minim konfigurasi tambahan. Dukungan terhadap Trusted Platform Module (TPM) memberikan lapisan keamanan ekstra melalui penyimpanan kunci enkripsi berbasis perangkat keras, sehingga mengurangi risiko pencurian kunci. Dari sisi manajemen, BitLocker juga menyediakan mekanisme pemulihan yang terstruktur, yang memudahkan administrator dalam mengelola keamanan perangkat dalam skala organisasi.

Di sisi lain, VeraCrypt menampilkan fleksibilitas yang lebih luas dalam konfigurasi enkripsi. Pengguna diberikan kebebasan untuk memilih berbagai algoritma enkripsi, metode hashing, serta skema autentikasi sesuai dengan kebutuhan tingkat keamanan yang diinginkan. Selain itu, VeraCrypt mendukung penggunaan lintas platform, sehingga menjadi solusi yang menarik bagi lingkungan sistem yang heterogen. Keunggulan ini menjadikan VeraCrypt lebih adaptif bagi pengguna yang membutuhkan kontrol penuh atas

proses enkripsi data at rest. Dari aspek keamanan, kedua teknologi terbukti efektif dalam melindungi data dari akses tidak sah. Pengujian menunjukkan bahwa data yang tersimpan pada media penyimpanan terenkripsi tidak dapat diakses tanpa kredensial yang valid. BitLocker menunjukkan keunggulan dalam keamanan berbasis sistem dengan memanfaatkan integrasi TPM, sementara VeraCrypt unggul dalam keamanan berbasis pengguna melalui konfigurasi enkripsi yang lebih kompleks. Perbedaan pendekatan ini menunjukkan bahwa keamanan data at rest tidak hanya bergantung pada algoritma enkripsi, tetapi juga pada strategi manajemen kunci dan autentikasi.

Pembahasan mengenai kinerja sistem menunjukkan bahwa penerapan enkripsi data at rest memberikan dampak yang relatif kecil terhadap performa, terutama pada perangkat keras modern. BitLocker cenderung memiliki overhead kinerja yang lebih rendah karena optimasi sistem dan dukungan perangkat keras. Sebaliknya, VeraCrypt menunjukkan sedikit penurunan performa pada konfigurasi enkripsi tingkat tinggi, namun hal ini sebanding dengan peningkatan tingkat keamanan yang ditawarkan. Dengan demikian, terdapat trade-off antara kinerja dan fleksibilitas keamanan yang perlu dipertimbangkan.
Selain itu, aspek kemudahan penggunaan dan administrasi juga menjadi faktor penting dalam pembahasan. BitLocker lebih sesuai untuk lingkungan enterprise yang membutuhkan pengelolaan terpusat dan penerapan kebijakan keamanan secara konsisten. Sementara itu, VeraCrypt lebih cocok bagi pengguna individu atau organisasi kecil yang mengutamakan transparansi, kontrol konfigurasi, dan independensi dari platform tertentu. Secara keseluruhan, pembahasan ini menunjukkan bahwa baik BitLocker maupun VeraCrypt memiliki keunggulan dan keterbatasan masing-masing dalam mengamankan data at rest. Pemilihan teknologi enkripsi yang tepat sangat dipengaruhi oleh kebutuhan keamanan, lingkungan sistem, serta tingkat kontrol yang diinginkan oleh pengguna. Hasil penelitian ini menegaskan pentingnya pendekatan yang kontekstual dalam penerapan enkripsi data at rest sebagai bagian dari strategi keamanan informasi yang komprehensif.

**Kesimpulan**

Hasil penelitian ini menunjukkan bahwa bahwa penerapan enkripsi data at rest menggunakan BitLocker dan VeraCrypt merupakan langkah yang efektif dalam meningkatkan keamanan informasi pada media penyimpanan. Kedua teknologi tersebut terbukti mampu melindungi data dari akses tidak sah, khususnya dalam kondisi kehilangan perangkat atau upaya pelanggaran keamanan secara langsung terhadap media penyimpanan. BitLocker menunjukkan keunggulan dalam hal kemudahan implementasi, integrasi dengan sistem operasi Windows, serta dukungan manajemen kunci berbasis perangkat keras melalui Trusted Platform Module (TPM). Karakteristik ini menjadikan BitLocker lebih sesuai untuk lingkungan enterprise yang membutuhkan pengelolaan keamanan terpusat, efisiensi operasional, dan performa sistem yang stabil. Sementara itu, VeraCrypt menawarkan fleksibilitas dan kontrol konfigurasi yang lebih tinggi, dengan pilihan algoritma enkripsi dan metode autentikasi yang beragam, sehingga cocok digunakan pada lingkungan yang membutuhkan tingkat keamanan khusus dan sistem lintas platform.

Dari sisi kinerja, penerapan enkripsi data at rest pada kedua teknologi menunjukkan dampak yang relatif minimal terhadap performa sistem, terutama pada perangkat dengan spesifikasi modern. Perbedaan kinerja yang muncul mencerminkan adanya trade-off antara efisiensi sistem dan tingkat fleksibilitas keamanan yang dipilih. Oleh karena itu, pemilihan solusi enkripsi perlu mempertimbangkan keseimbangan antara kebutuhan keamanan, kemudahan penggunaan, dan kinerja sistem. Secara keseluruhan, penelitian ini menegaskan bahwa tidak terdapat satu solusi enkripsi yang sepenuhnya unggul untuk semua kondisi. BitLocker dan VeraCrypt sama-sama memiliki peran strategis dalam pengamanan data at rest, dengan keunggulan yang saling melengkapi. Hasil penelitian ini diharapkan dapat menjadi referensi bagi pengguna dan organisasi dalam menentukan strategi enkripsi data at rest yang tepat sebagai bagian dari upaya menjaga keamanan informasi secara menyeluruh.

**Referensi**


Barker, E. (2020). *Recommendation for key management: Part 1—General* (NIST SP 800-57 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-57pt1r5

Behl, A., & Behl, K. (2017). *Cyberwar: The next threat to national security and what to do about it*. Oxford University Press.

Bertino, E., & Sandhu, R. (2019). Database security—Concepts, approaches, and challenges. *IEEE Transactions on Dependable and Secure Computing*, 16(1), 1–17. https://doi.org/10.1109/TDSC.2017.2768094

Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014). Cryptanalysis of disk encryption systems. *IEEE Symposium on Security and Privacy*, 18–34. https://doi.org/10.1109/SP.2014.14

Creswell, J. W. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638

Ferguson, N., Schneier, B., & Kohno, T. (2011). *Cryptography engineering: Design principles and practical applications*. Wiley.

Garfinkel, S. L., & Shelat, A. (2003). Remembrance of data passed: A study of disk sanitization practices. *IEEE Security & Privacy*, 1(1), 17–27. https://doi.org/10.1109/MSECP.2003.1176992

Gollmann, D. (2011). *Computer security* (3rd ed.). Wiley.

Green, M., & Smith, M. (2016). Cryptopals crypto challenges: Applied cryptography in practice. *Journal of Cybersecurity Education*, 1(2), 45–59.

ISO/IEC. (2018). *ISO/IEC 27001: Information security management systems—Requirements*. International Organization for Standardization.

ISO/IEC. (2022). *ISO/IEC 27002: Information security controls*. International Organization for Standardization.

Kahn Academy. (2022). Disk encryption and data-at-rest security. https://www.khanacademy.org/computing/computer-security

Kahn, A., & Kahn, M. (2019). Data security and privacy in information systems. *Information Systems Frontiers*, 21(4), 801–813. https://doi.org/10.1007/s10796-019-09906-3

Microsoft. (2023). *BitLocker drive encryption overview*. https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview

NIST. (2018). *Digital identity guidelines* (SP 800-63). National Institute of Standards and Technology.

NIST. (2020). *Security and privacy controls for information systems and organizations* (SP 800-53 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in computing* (5th ed.). Pearson Education.

Ristenpart, T., & Shacham, H. (2016). Cryptographic techniques for data storage security. *Communications of the ACM*, 59(2), 80–89. https://doi.org/10.1145/2817744

Schneier, B. (2015). *Applied cryptography* (2nd ed.). Wiley.

Sharma, S., & Chen, J. (2020). Performance analysis of full disk encryption techniques. *Journal of Information Security and Applications*, 52, 102465. https://doi.org/10.1016/j.jisa.2020.102465

Singh, J., & Kumar, R. (2021). Comparative analysis of disk encryption tools for data-at-rest security. *International Journal of Information Security Science*, 10(3), 45–56.

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.

VeraCrypt. (2023). *VeraCrypt documentation*. https://www.veracrypt.fr/en/Documentation.html

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.

Zhang, Y., & Chen, X. (2022). Secure data storage and encryption mechanisms in modern operating systems. *IEEE Access*, 10, 55421–55434. https://doi.org/10.1109/ACCESS.2022.3178456