Just IT : Jurnal Sistem Informasi, Teknologi Informasi dan Komputer
Vol. 14, No. 2, Januari 2024, pp. 80-149
P-ISSN: 2089 – 0256, e-ISSN: 2598 – 3016

TEKNIK PENGAMANAN DATA *AT REST* MENGGUNAKAN BITLOCKER DAN VERACRYPT

Akhmad Nur Ghazi[1], Ghofar Taufiq[2]
[1]Teknologi Informasi Fakultas Teknik dan Informatika Universitas Bina Sarana Informatika
17190401@bsi.ac.id[1]

Abstrak

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. Penelitian ini bertujuan untuk memberikan informasi mengenai cara melakukan pengamanan data at rest dengan menggunakan Bitlocker dan Veracrypt. Hasil penelitian menunjukkan bahwa BitLocker dan VeraCrypt masing-masing memiliki kelebihan dan kekurangan. BitLocker menawarkan integrasi yang baik dengan sistem operasi Windows dan memiliki dukungan resmi, sementara VeraCrypt adalah perangkat lunak sumber terbuka yang memberikan fleksibilitas dan keandalan. Namun, BitLocker memiliki beberapa keterbatasan dalam hal dukungan platform dan kontrol pengguna, sedangkan VeraCrypt memiliki antarmuka yang lebih kompleks. Temuan penelitian ini dapat memberikan wawasan bagi pengguna dan organisasi dalam memilih solusi enkripsi yang sesuai dengan kebutuhan keamanan data mereka.
Kata Kunci: *Pengamanan data, Bitlocker, Veracrypt*

Abstract

Recently, there have been numerous cases of data leaks, such as the Twitter source code being spread on GitHub, Meta's leaked AI on internet forums, and suspected data leaks of Indihome customers. These incidents can occur due to security vulnerabilities in data storage. Therefore, data security becomes an important effort to safeguard personal or company data from unauthorized access. This research aims to provide information on how to secure data at rest using BitLocker and VeraCrypt. The research findings show that BitLocker and VeraCrypt each have their own advantages and disadvantages. BitLocker offers good integration with Windows operating systems and has official support, while VeraCrypt is an open-source software that provides flexibility and reliability. However, BitLocker has some limitations in terms of platform support and user control, while VeraCrypt has a more complex interface. The research findings can provide insights for users and organizations in choosing encryption solutions that meet their data security needs.
Keywords: *Data security, Bitlocker, Veracrypt*

1. 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

p-ISSN 2089-0265
e-ISSN 2598-3016

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).

2. 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.

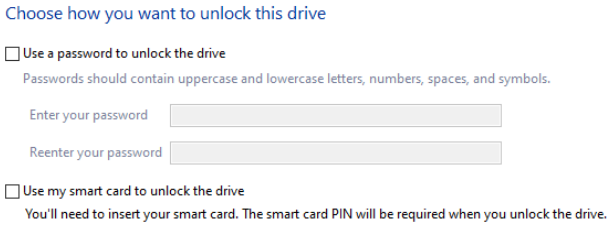
3. Hasil dan Pembahasan

A. Melakukan pengamanan data dengan BitLocker

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 terdapat beberapa proses / tahapan yakni : pemberian *password* enkripsi, penyalinan kunci Recovery, pemilihan metode enkripsi dan pemilihan versi enkripsi.

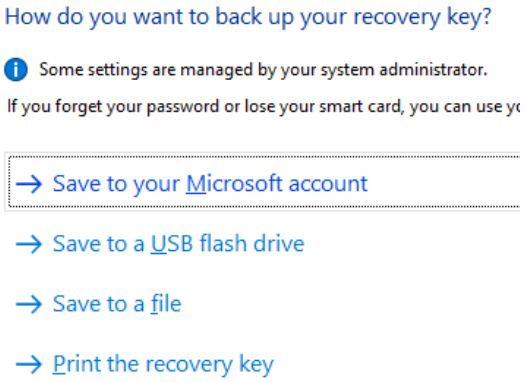
Gambar. 1. Tampilan bitlocker pada *Control Panel*

Pada tahap pertama merupakan proses pemilihan dalam mengamankan partisi yakni dapat menggunakan password / 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*

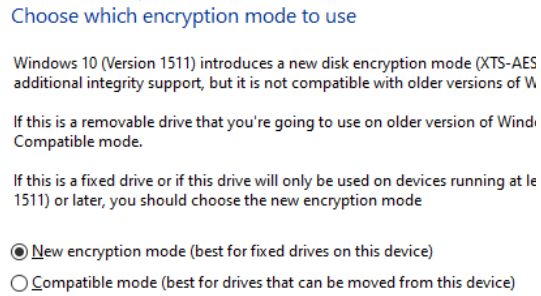
Pada tahap ketiga di gambar 4 berikut, merupakan pemilihan metode enkripsi pada

p-ISSN 2089-0265
e-ISSN 2598-3016

disk, apakah ingin mengenkripsi data yang terpakai saja di drive atau ingin mengenkripsi satu drive penuh.

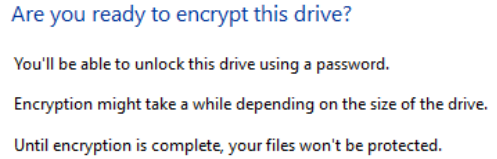
Gambar. 4. Tampilan pemilihan metode enkripsi

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).



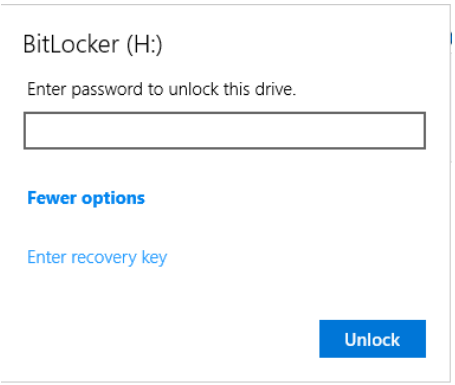
Gambar. 5. Tampilan pemilihan versi enkripsi

Pada gambar 6 berikut merupakan jendela konfirmasi sebelum melakukan proses enkripsi. Perlu diingat durasi proses enkripsi ini akan ditentukan oleh seberapa besar ukuran partisi yang dienkripsi.



Gambar. 6. Tampilan Konfirmasi sebelum memulai proses Enkripsi

Dan setelah proses enkripsi tersebut selesai, partisi sudah diamankan dengan enkripsi bitlocker. Untuk membuka partisi yang telah diamankan pada gambar 7 berikut, masukkan password enkripsi atau jika lupa dengan passwordnya akses menu "*Enter recovery key*".

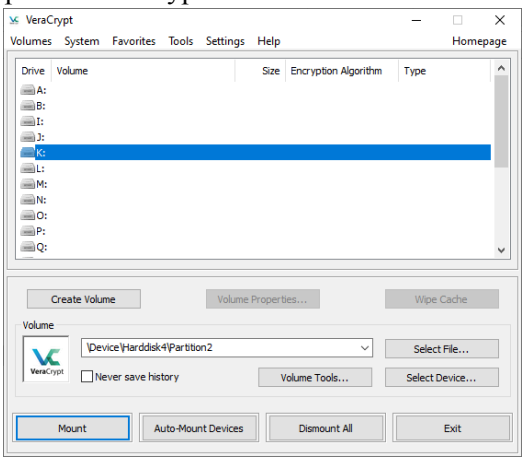


Gambar. 7. Tampilan *Input password* untuk melakukan dekripsi partisi Bitlocker

B. 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.

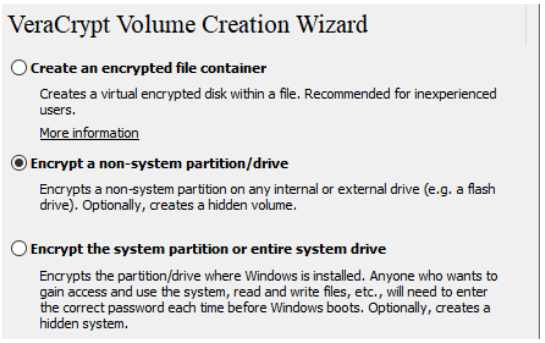
Berikut merupakan tampilan awal aplikasi Veracrypt



Gambar. 8. Tampilan awal Veracrypt

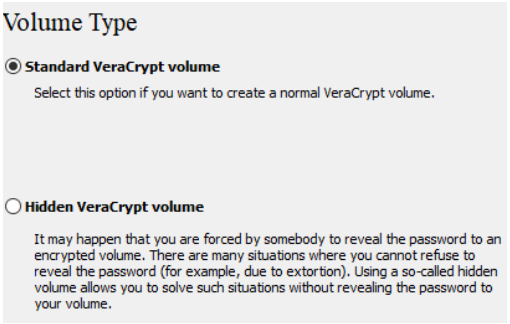
Tahap pertama pada gambar 9 merupakan proses pemilihan pembuatan enkripsi, terdapat 3 pilihan yakni membuat *file container* baru dengan ekstensi veracrypt, menggunakan partisi non sistem dan menggunakan partisi sistem.

p-ISSN 2089-0265
e-ISSN 2598-3016



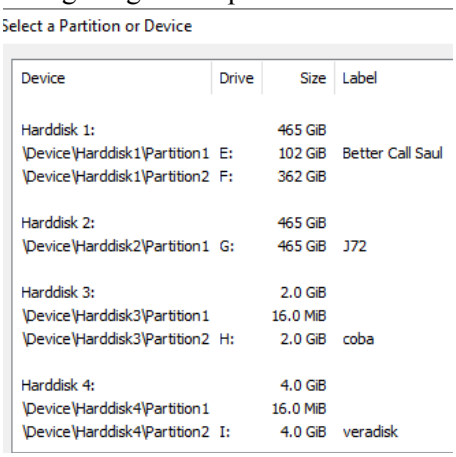
Gambar. 9. Tampilan pemilihan pembuatan enkripsi

Tahap kedua pada gambar 10 adalah pemilihan jenis volume yang akan dibuat, yakni *standard* dan *hidden*.



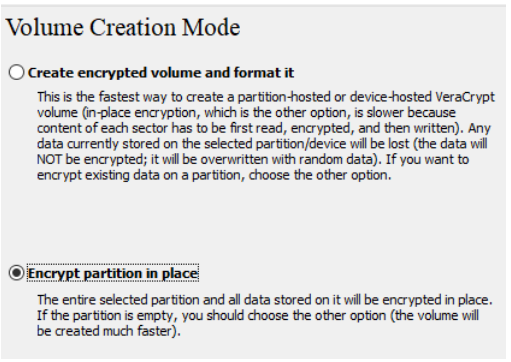
Gambar. 10. Tampilan pemilihan jenis volume

Pada tahap ketiga di gambar 11, merupakan tampilan untuk memilih partisi yang ingin dienkripsi. Pada gambar 11 ini juga ditunjukkan semua partisi yang terhubung dengan komputer kita.



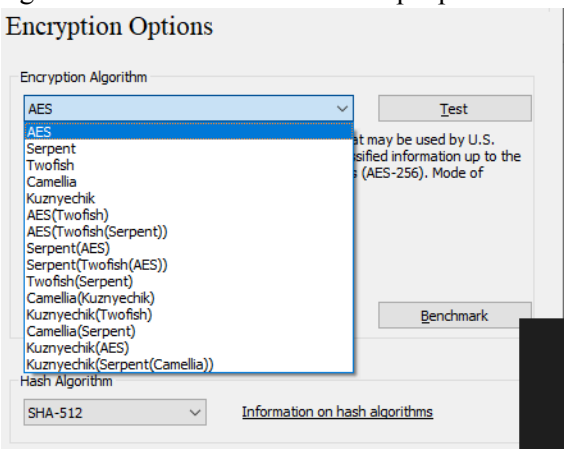
Gambar. 11. Tampilan pemilihan partisi yang ingin dienkripsi

Pada tahap keempat di gambar 12, merupakan tampilan untuk memilih pembuatan mode enkripsi, yang pertama enkripsi lalu *format* yang kedua hanya mengenkripsi saja.



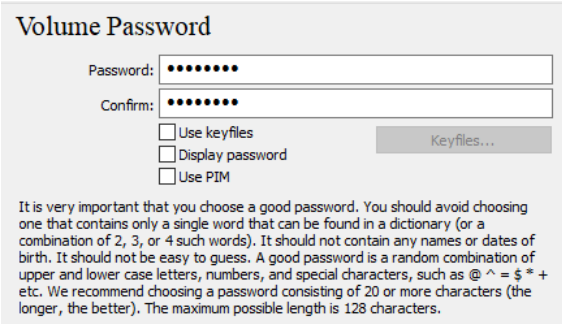
Gambar. 12. Tampilan pemilihan pembuatan mode enkripsi

Pada tahap kelima di gambar 13, merupakan tampilan pemilihan Algoritma enkripsi dan Algoritma *hash* yang akan digunakan untuk melakukan enkripsi partisi.



Gambar. 13. Tampilan pemilihan Algoritma enkripsi dan Algoritma *hash*

Pada tahap keenam di gambar 14, adalah tampilan pemberian password untuk enkripsi, selain itu kita juga dapat menambahkan kunci *file.*

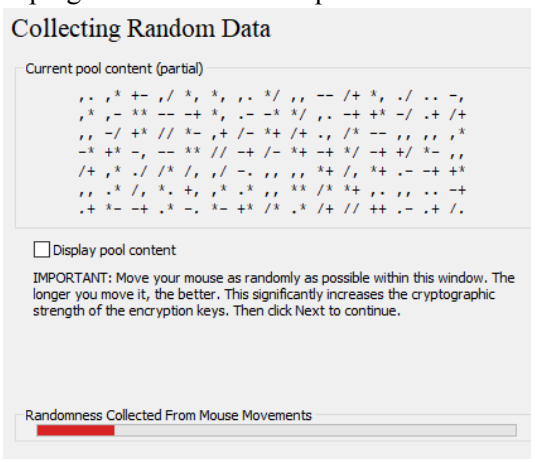


Gambar. 14. Tampilan pemberian *password* enkripsi

Pada tahap ketujuh di gambar 15, adalah tampilan untuk mengumpulkan data acak yang dihasilkan oleh pergerakan *mouse*

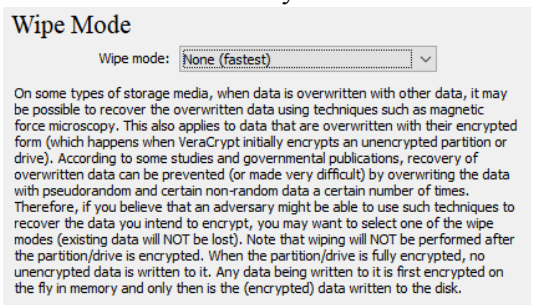
p-ISSN 2089-0265
e-ISSN 2598-3016

yang berfungsi untuk meningkatkan kekuatan kriptografi dari kunci enkripsi.



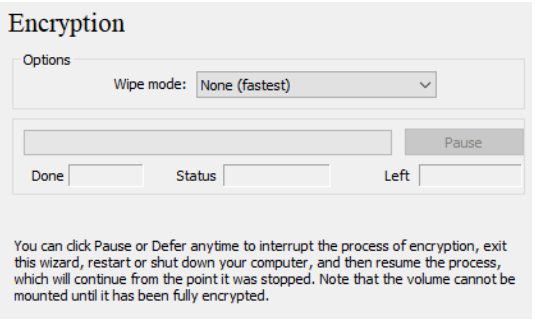
Gambar. 15. Tampilan pengumpulan data acak

Pada tahap kedelapan di gambar 16, merupakan tampilan pemilihan mode *wipe*. Mode wipe ini digunakan untuk mencegah atau mempersulit recovery dari data yang telah dienkripsi, karena terdapat kemungkinan bagi data yang telah dienkripsi untuk dilakukan recovery.



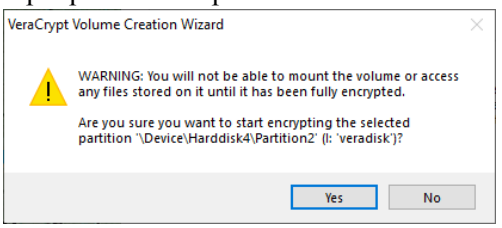
Gambar. 16. Tampilan pemilihan mode *wipe*

Pada tahap terakhir di gambar 17, merupakan tampilan status enkripsi dan juga merupakan tampilan sebelum memulai proses enkripsi.



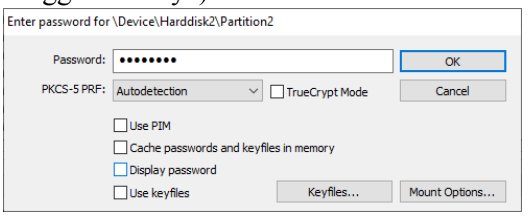
Gambar. 17. Tampilan status proses enkripsi

Sebelum memulai proses enkripsi akan muncul tampilan konfirmasi untuk memulai enkripsi pada gambar 18, perlu diingat partisi yang sedang dienkripsi tidak dapat diakses sampai proses enkripsi selesai.



Gambar. 18. Tampilan konfirmasi sebelum proses enkripsi

Proses enkripsi telah selesai dan partisi yang dienkripsi pun dapat diakses, tetapi harus menggunakan aplikasi Veracrypt untuk melakukan *mounting* partisi. Setelah *mounting* partisi akan muncul tampilan pada gambar 19 untuk memasukkan password enkripsi dan kunci *file* (jika menggunakannya).



Gambar. 19. Tampilan *Input password* untuk dekripsi partisi

C. 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

p-ISSN 2089-0265
e-ISSN 2598-3016

enkripsi yang dapat digunakan seperti: 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.

D. Kelebihan dan Kekurangan masing-masing Program

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.

4. Simpulan dan Saran

Dari hasil penelitian dapat disimpulkan bahwa pada segi dukungan operasi sistem bitlocker cocok digunakan pengguna yang hanya memakai windows OS saja sedangkan Veracrypt untuk pengguna yang menggunakan beberapa operasi sistem. Walau bitlocker dapat digunakan di Windows OS, namun hanya varian windows tertentu saja yang terdapat bitlocker, sehingga 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.

Terdapat beberapa saran untuk pengembangan penelitian selanjutnya: penelitian lebih lanjut mengenai performa enkripsi dan dekripsi, pengaruh enkripsi pada sistem, pengujian keamanan, dampak penggunaan enkripsi yang berbeda dan melakukan perbandingan dengan aplikasi pengamanan data lainnya seperti FileVault di MacOS atau LUKS di Linux.

Daftar Pustaka

Addlesee, A. (2022). Securely Capturing People's Interactions with Voice Assistants at Home: A Bespoke Tool for Ethical Data Collection. *Proceedings of the Second Workshop on NLP for Positive Impact (NLP4PI)*, 25–30. https://aclanthology.org/2022.nlp4pi-1.3/

Fathiyana, R. Z. (2021). Analisis Keamanan Perangkat Lunak Enkripsi Media Penyimpanan DiskCryptor. *Journal of Informatics and Communication Technology (JICT)*, *3*(1), 20–30. https://doi.org/10.52661/j_ict.v3i1.64

IDRIX. (2022). *Home*. Veracrypt. https://veracrypt.fr/en/Home.html

Ocenas, M., Homoliak, I., Hanacek, P., & Malinka, K. (2020). Security and Encryption at Modern Databases. *Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy*, 19–23. https://doi.org/10.1145/3377644.3377662

Tan, C., Zhang, L., & Bao, L. (2020). A Deep Exploration of BitLocker Encryption and Security Analysis. *2020 IEEE 20th*

p-ISSN 2089-0265
e-ISSN 2598-3016

International Conference on Communication Technology (ICCT), *2020-Octob*, 1070–1074. https://doi.org/10.1109/ICCT50939.2020.9295908

Yusroni, Y., & Anton, A. (2022). Implementasi Teknologi Cloud Computing Pada PT Zurich Topas Life Jakarta. *Simpatik: Jurnal Sistem Informasi dan Informatika*, *2*(1), 11–20. https://doi.org/10.31294/simpatik.v2i1.1110