Hindawi
Scientific Programming
Volume 2020, Article ID 6132312, 9 pages
https://doi.org/10.1155/2020/6132312

Review Article

Evaluating Encryption Algorithms for Sensitive Data Using Different Storage Devices

Bahman A. Sassani (Sarrafpour),[1] Mohammed Alkorbi,[1] Noreen Jamil ,[2] M. Asif Naeem,[2,3] and Farhaan Mirza[3]

[1]*Department of Computer Science, Unitec Institute of Technology, Auckland, New Zealand*
[2]*Department of Computer Science, National University of Computer & Emerging Sciences, Islamabad, Pakistan*
[3]*School of Engineering, Computer and Mathematical Sciences, Auckland University of Technology, Auckland, New Zealand*

Correspondence should be addressed to Noreen Jamil; noreen.jamil@nu.edu.pk

Received 24 February 2020; Accepted 4 May 2020; Published 31 May 2020

Academic Editor: Iván García-Magariño

Sensitive data need to be protected from being stolen and read by unauthorized persons regardless of whether the data are stored in hard drives, flash memory, laptops, desktops, and other storage devices. In an enterprise environment where sensitive data is stored on storage devices, such as financial or military data, encryption is used in the storage device to ensure data confidentiality. Nowadays, the SSD-based NAND storage devices are favored over HDD and SSHD to store data because they offer increased performance and reduced access latency to the client. In this paper, the performance of different symmetric encryption algorithms is evaluated on HDD, SSHD, and SSD-based NAND MLC flash memory using two different storage encryption software. Based on the experiments we carried out, Advanced Encryption Standard (AES) algorithm on HDD outperforms Serpent and Twofish algorithms in terms of random read speed and write speed (both sequentially and randomly), whereas Twofish algorithm is slightly faster than AES in sequential reading on SSHD and SSD-based NAND MLC flash memory. By conducting full range of evaluative tests across HDD, SSHD, and SSD, our experimental results can give better idea for the storage consumers to determine which kind of storage device and encryption algorithm is suitable for their purposes. This will give them an opportunity to continuously achieve the best performance of the storage device and secure their sensitive data.

1. Introduction

The term cryptography is defined as the encryption of sensitive information such as data, images, and others. The cryptography techniques have changed over the years based on the developments of encryption software and encryption algorithms. Sensitive data needs to be protected from being stolen and read by unauthorized persons regardless of whether this data is stored in hard drives, flash memory, laptops, desktops, or other storage devices. The process of cryptography involves converting standard text (called plain text) into something unintelligible (called cipher text). Decryption is the opposite of encryption; it is the process of changing unintelligible language into plain text.

In 1977, the US government required a method that would store their sensitive information safely. A solution to their problem was found through the release of Data Encryption Standard (DES) in the same year. DES is 56-bit key length with 64-bit block size [1, 2].

An observation of DESs performance revealed that it was defenseless against brute force attacks. For that reason, a public request was made by the National Institute of Standards and Technology to develop a new encryption standard. A total of fifteen algorithms were received and submitted by twelve different countries. Out of these fifteen, only five algorithms were chosen: MARS, RC6, Serpent, Rijndael, and Twofish. Rijndael was the top algorithm and called the Advanced Encryption Standard (AES) [3]. The second best option was the Serpent followed by Twofish [3].

The Solid State Disks (SSDs) are widely used by government and security departments [4]. They mostly utilize NAND-based flash memory in which information is represented by electrons trapped in a floating gate between normal gate and channel of a transistor cell, therefore eliminating the mechanical spinning head in older hard disk drives (HDD). Technology has evolved over the years. Single-Level Cell (SLC) SSD flash memory was the core technology used in the first generation of SSD and is still in use due to its high reliability and wide read margin; it stores single bit (0, 1) on a single cell, where a cell with trapped electron represents "0" and lack of electron indicates "1."

There is also Multilevel cell (MLC) SSD flash memory storing two bits (00, 01, 10. 11) on a single cell [5, 6] and third-generation 3D Triple-Level cell (TLC) SSD flash memory storing three bits (000, 001, ..., 110, 111) on a single cell. While 3D TLC NAND flash SSDs are rapidly gaining ground, currently, SSD-based NAND MLC flash is still dominating on storage market due to its continuously increasing capacity, decreasing price, and high read and write speeds [4].

A hard disk drive (HDD), as the old magnetic field-based technology, uses a write/read head that spans over one or many disks in order to access the stored information. The speed of a hard drive is measured in revolutions per minute (RPM). The RPM of a hard drive can be as low as 5400 PRM and as high as 15000 PRM [5]. The benefit of using a hard drive lies in giving one the ability to store large amount of data and its cheap price compared to SSD.

Solid-state hybrid drive (SSHD) is an integrated technology that combines NAND flash SSD and HDD technology. The purpose of NAND flash SSD on the hybrid drive is to speed up the booting process or, in some rare cases, to act as a cache for the data stored on the HDD.

Since these storage devices are portable and light weight, they are at high risk of being lost or stolen and accessed by unauthorized persons. Encryption will ensure that data in storage devices will remain confidential from unauthorized access and modification of data [7].

Nowadays, several software-based encryption has been developed to ensure the confidentiality of data on storage devices. For instance, TrueCrypt is an open-source software disk encryption. This software can be operated on different operating systems [8]. TrueCrypt has the ability to turn a file into an encrypted virtual disk [8].

On the other hand, BestCrypt is a licensed encryption software that was established by the application developer, Gray [9]. BestCrypt is widely used in government, military agencies, healthcare organizations, insurance vendors, and other organizations [9]. The functionality of BestCrypt is similar to that of the TrueCrypt encryption software in that it is capable of storing files in a container that is similar to a hard drive [9]. Both TrueCrypt and BestCrypt support AES, Serpent, and Twofish 256-bit encryption algorithms.

In 2009, Elminaam et al. have compared different symmetric encryption algorithms' performance including DES, 3DES, AES, RC4, and RC6 [10]. The impact that encryption algorithms have on CPU usage and battery life on laptops was examined as well. Additionally, a comparison of the encryption and decryption time of these algorithms based on different packet size and data type (such as text file and image) was made. The researchers concluded that Blowfish performs better than other algorithms due to the change of packet size. In addition, they determined that RC4, RC6, and Blowfish were more time consuming when encrypting and decrypting images than other algorithms. Finally, they mentioned that changing AES encryption keys to the highest key (256 bits) will increase power and time consumption.

In 2014, Kansal and Mittal mentioned the significant use of encryption in electronic transactions across the internet [11]. The researchers examined the different symmetric encryption algorithms including DES, 3DES, and AES. The examination was based on different parameters and data types such as text file and image on i7 processor. They concluded that AES requires less encryption and decryption time compared with DES and 3DES. However, 3DES utilizes less memory than other algorithms.

In 2018, Slimane et al. [12] proposed a hash-key-based image cryptosystem using 2D logistic maps and cellular automata to ensure the security of multimedia data. Based on data collected on statistical tests, key space, entropy information, and differential attacks, they concluded that their cryptosystem is fast and efficient for encryption. Similarly, in 2018, design and implementation of a high-performance encryption system based on AES algorithm was proposed by Yuan et al. [13]. Their proposed cryptosystem supports all three modes including AES-128, -192, and -256, piped into 4 stages for each round operation for both encryption and decryption. The main advantage of the above proposed cryptosystem is concluded to be the performance and throughput due to 4-stage pipeline implementations.

To further improve the security of data sanitization in low-cost MLC flash memories, Lin et. al. [14] proposed a fast sanitization scheme. The scheme achieves fast sanitization of old data with zero live-data-copy overhead when a new data is created. The design allows sanitizing either upper or lower page without disturbing data on the associated lower or upper page and eliminates the need for backing up the data.

Furthermore, in 2019, researchers Meijer and van Gastel [15] analysed hardware full-disk encryption of several solid-state drives (SSDs) produced by three manufacturers between 2014 and 2018 using internal SATA and NVMe interfaces or external USB interface. The analysis was done by RE (reverse engineering) the firmware of those devices. They concluded that critical security weaknesses on many of those models due to specification, design, or implementation allowing full recovery of data by adversary, even if data was protected by Microsoft Windows Integrated, BitLocker on those models.

Considering the recent evaluations and by focusing on common storage devices, this paper investigates the encryption performance of AES, Serpent, and Twofish 256-bit key on HDD, SSHD, and SSD-based NAND MLC flash using TrueCrypt and BestCrypt. The comprehensive experimental results provided in this paper allow storage solution consumers to determine which encryption algorithm performs the best on these storage devices.

Additionally, it provides them with detailed encryption performance of both software-based encryption products which can enable them to select the right software-based encryption product to secure their storage devices.

The rest of this paper has been organized as follows: Section 2 discusses the performance evaluations in detail within two subsections of system setup and experimental results; this subsection broadly outlines the outcome of the evaluative tests and compares the results, and finally, Section 3 concludes the paper.

2. Performance Evaluation

2.1. Experimental Setup. We built a test bed environment with Western Digital HDD, Seagate SSHD, and Samsung 128 GB flash MLC SSD on a comprehensive system (see Tables 1 and 2). Anvil's Storage Utilities is used to compare the read and write speed of the storage device. The benchmark tool determines the speed of storage device across different disk access patterns including 4 MB sequential read, 4K random read, 4 MB sequential write, and 4K random write. Samsung 128 GB flash MLC SSD has 256 MB of cache to accelerate the read and write speed of the storage device (see Table 2). The size of the test file that is sent by the benchmark measuring tool (Anvil's Storage Utilities) to the storage device is 1 GB to overwrite the cache which will determine the actual storage performance. In order to get more accurate results, each experiment is done 10 times. Afterwards, the average read and write performance of each storage device is determined.

4 MB sequential read speed is a disk access pattern whereby 4 MB blocks of data are read from adjacent locations on the surface of a device. 4K random read speed is a disk access pattern whereby small (4 KB) blocks of data are read from random locations on the surface of the device being tested. They are usually measured in MB/S. 4 MB sequential write is a disk access pattern whereby 4 MB blocks of data are written from adjacent locations on the surface of a device. 4K random write is a disk access pattern whereby small (4 KB) blocks of data are written from random locations on the surface of a storage device.

2.2. Experimental Results. Figure 1 shows, in this experiment, three different encryption algorithms being applied to the HDD storage device using TrueCrypt and BestCrypt in order to test how well they each perform and determine which kind of encryption storage software performs the best. After being applied to the HDD storage device using BestCrypt, AES 256-bit average 4 MB sequential read speed is 58.70 Mb/s. In comparison, AES 256-bit average 4 MB sequential read speed is 59.14 Mb/s when TrueCrypt is applied instead. AES 256-bit 4 MB sequential read speed performs 0.75% better when TrueCrypt is applied than BestCrypt. Similarly, Serpent 256-bit 4 MB sequential read speed is 58.43 Mb/s when BestCrypt is applied and 59.32 Mb/s when TrueCrypt is applied, which indicates that it performs 1.52% better on TrueCrypt than on BestCrypt. Finally, Twofish 256-bit 4 MB sequential read speed is 57.48 Mb/s when BestCrypt is applied and 59.22 Mb/s when TrueCrypt is applied. That is a 3.03% difference.

Table 1: System specifications used in experiment test bed environment.

Item	Description
Motherboard model	F2A88XM-HD3
Processor	AMD-A10 7850k 3.70 GHz
Memory	DDR3 2133 16 GB
DVD/CD writer	24x internal DVD/CD writer
Operating system	Windows 8.1 Professional

Figure 2 shows, in this experiment, three different encryption algorithms being applied to the HDD storage device using TrueCrypt and BestCrypt in order to test how well they each perform and determine which kind of encryption storage software performs the best. After being applied to the HDD storage device using TrueCrypt, AES 256-bit average 4K random read speed is 0.47 Mb/s. In comparison, AES 256-bit average 4K random read speed is 0.50 Mb/s when BestCrypt is applied instead. AES 256-bit 4K random read speed performs 6.38% better when BestCrypt is applied than TrueCrypt. Similarly, Serpent 256-bit 4K random read speed is 0.43 Mb/s when TrueCrypt is applied and 0.49 Mb/s when BestCrypt is applied, which indicates that it performs 13.95% better on BestCrypt than on TrueCrypt.

Finally, Twofish 256-bit 4K random read speed is 0.42 Mb/s when TrueCrypt is applied and 0.49 Mb/s when BestCrypt is applied. That is a 16.67% difference. Figure 3 shows, in this experiment, three different encryption algorithms being applied to the HDD storage device using TrueCrypt and BestCrypt in order to test how well they each perform and determine which kind of encryption storage software performs the best. After being applied to the HDD storage device using BestCrypt, AES 256-bit average 4 MB sequential write speed is 51.13 Mb/s. In comparison, AES 256-bit average 4 MB sequential write speed is 51.64 Mb/s when TrueCrypt is applied instead. AES 256-bit 4 MB sequential write speed performs 1.00% better when TrueCrypt is applied than BestCrypt. Similarly, Serpent 256-bit 4 MB sequential write speed is 51.08 Mb/s when BestCrypt is applied and 51.99 Mb/s when TrueCrypt is applied, which indicates that it performs 1.78% better on TrueCrypt than on BestCrypt. Finally, Twofish 256-bit 4 MB sequential write speed is 51.45 Mb/s when BestCrypt is applied and 52.00 Mb/s when TrueCrypt is applied. That is a 1.07% difference.

Figure 4 shows, in this experiment, three different encryption algorithms being applied to the HDD storage device using TrueCrypt and BestCrypt in order to test how well they each perform and determine which kind of encryption storage software performs the best. After being applied to the HDD storage device using BestCrypt, AES 256-bit average 4K random write speed is 0.93 Mb/s. In comparison, AES 256-bit average 4K random write speed is 1.01 Mb/s when TrueCrypt is applied instead. AES 256-bit 4K random write speed performs 8.60% better when TrueCrypt is applied than BestCrypt. Similarly, Serpent 256-bit 4K random write speed is 0.91 Mb/s when BestCrypt is applied and 0.99 Mb/s when TrueCrypt is applied, which indicates that it performs 8.79%

Table 2: Storage specification used in experiment test bed environment.

Storage type	Manufacturer and model	Interface	Size (GB)	Cache (MB)	Temp (C) performance
HDD	Western Digital (WD5000AAKX)	SATA III 6 Gb/s	500	16	0 60 Data transfer rate 6 Gb/s max. Sustained data host to/ from drive is 126 MB/S max.
SSHD	Seagate (ST1000LM014)	SATA III 6 Gb/s	1	64	0 60 Sustained data transfer max. I/O data transfer rate is 600 MB/S max.

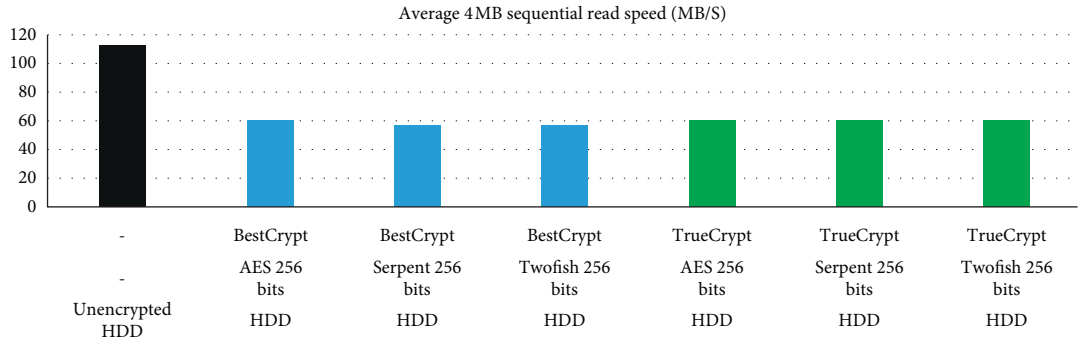

Figure 1: Comparison of the average 4 MB sequential read speed of HDD after applying AES, Serpent, and Twofish 256 bits using BestCrypt and TrueCrypt.

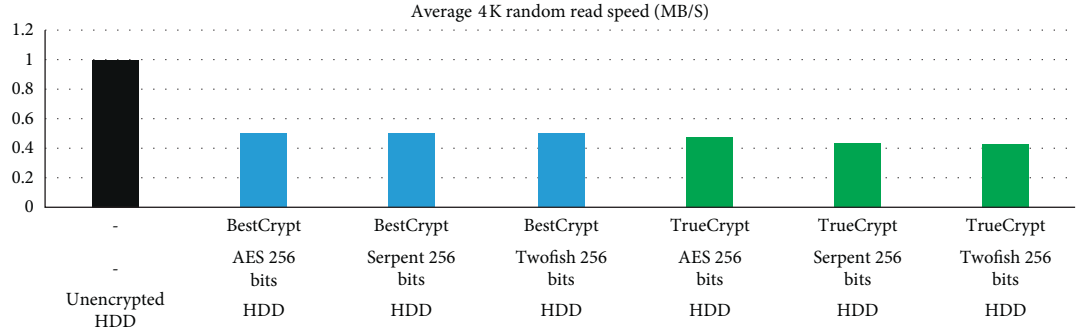

Figure 2: Comparison of the average 4K random read speed of HDD after applying AES, Serpent, and Twofish 256 bits using BestCrypt and TrueCrypt.

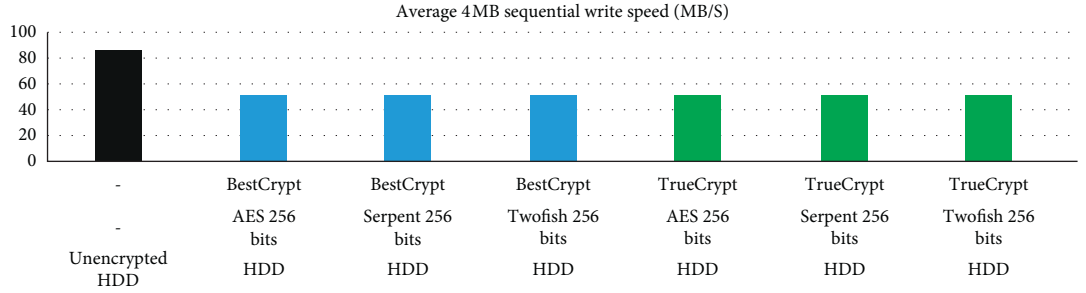

Figure 3: Comparison of the average 4 MB sequential write speed of HDD after applying AES, Serpent, and Twofish 256 bits using BestCrypt and TrueCrypt.

better on TrueCrypt than on BestCrypt. Finally, Twofish 256-bit 4K random write speed is 0.92 Mb/s when BestCrypt is applied and 0.99 Mb/s when TrueCrypt is applied. That is a 7.61% difference.

Figure 5 shows that three different encryption algorithms are applied to the SSHD storage device using True Crypt and BestCrypt in order to test how well they each perform and determine which kind of encryption storage software

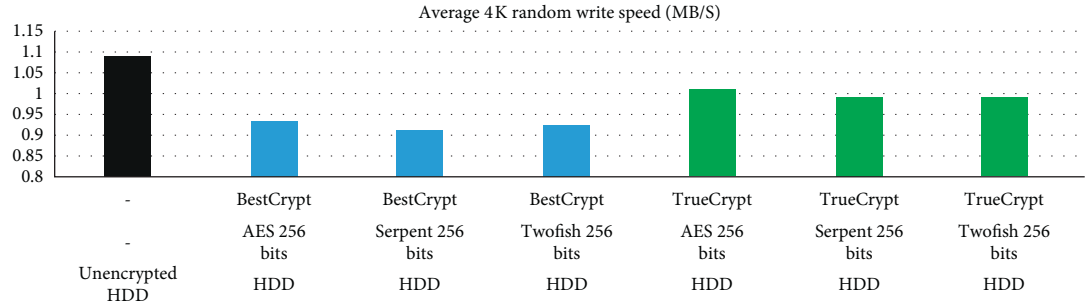

Figure 4: Comparison of the average 4K random write speed of HDD after applying AES, Serpent, and Twofish 256 bits using BestCrypt and TrueCrypt.

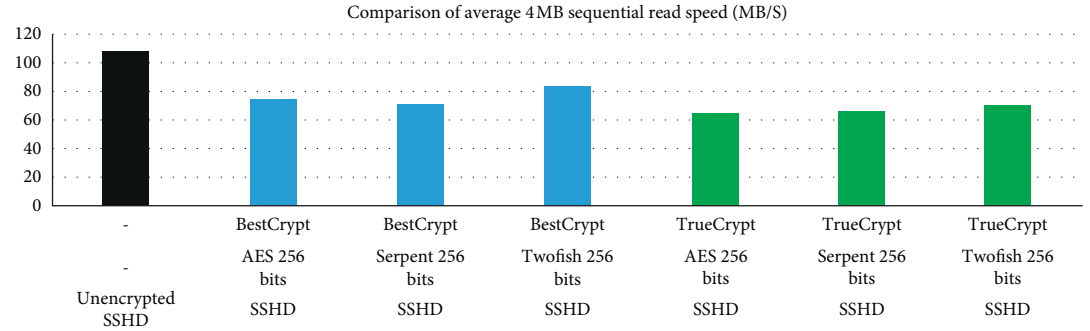

Figure 5: Comparison of the average 4 MB sequential read speed of SSHD after applying AES, Serpent, and Twofish 256 bits using BestCrypt and TrueCrypt.

performs the best. After being applied to the SSHD storage device using TrueCrypt, AES 256-bit average 4 MB sequential read speed is 64.55 Mb/s. In comparison, AES 256-bit average 4 MB sequential read speed is 75.95 Mb/s when BestCrypt is applied instead. AES 256-bit 4 MB sequential read speed performs 17.66% better when BestCrypt is applied than TrueCrypt. Similarly, Serpent 256-bit 4 MB sequential read speed is 65.94 Mb/s when TrueCrypt is applied and 71.90 Mb/s when BestCrypt is applied, which indicates that it performs 9.04% better on BestCrypt than on TrueCrypt. Finally, Twofish 256-bit 4 MB sequential read speed is 68.76 Mb/s when TrueCrypt is applied and 82.24 Mb/s when BestCrypt is applied. That is a 19.60% difference.

Figure 6 shows, in this experiment, three different encryption algorithms being applied to the SSHD storage device using TrueCrypt and BestCrypt in order to test how well they each perform and determine which kind of encryption storage software performs the best. After being applied to the SSHD storage device using TrueCrypt, AES 256-bit average 4K random read speed is 0.65 Mb/s. In comparison, AES 256-bit average 4K random read speed is 0.68 Mb/s when BestCrypt is applied instead. AES 256-bit 4K random read speed performs 4.61% better when BestCrypt is applied than TrueCrypt. Similarly, Serpent 256-bit 4K random read speed is 0.59 Mb/s when TrueCrypt is applied and 0.67 Mb/s when BestCrypt is applied, which indicates that it performs 13.56% better on BestCrypt than on TrueCrypt. Finally, Twofish 256-bit 4K random read speed is 0.70 Mb/s when TrueCrypt is applied and 0.78 Mb/s when BestCrypt is applied. That is an 11.43% difference.

Figure 7 shows, in this experiment, three different encryption algorithms being applied to the SSHD storage device using TrueCrypt and BestCrypt in order to test how well they each perform and determine which kind of encryption storage software performs the best. After being applied to the SSHD storage device using BestCrypt, AES 256-bit average 4 MB sequential write speed is 74.61 Mb/s. In comparison, AES 256-bit average 4 MB sequential write speed is 91.97 Mb/s when TrueCrypt is applied instead. AES 256-bit 4 MB sequential write speed performs 23.27% better when TrueCrypt is applied than BestCrypt. On the other hand, Serpent 256-bit 4 MB sequential write speed is 62.39 Mb/s when TrueCrypt is applied and 73.80 Mb/s when BestCrypt is applied, which indicates that it performs 18.29% better on BestCrypt than on TrueCrypt. Finally, Twofish 256-bit 4 MB sequential write speed is 69.99 Mb/s when BestCrypt is applied and 80.20 Mb/s when TrueCrypt is applied. That is a 14.59% difference.

Figure 8 shows, in this experiment, three different encryption algorithms being applied to the SSHD storage device using TrueCrypt and BestCrypt in order to test how well they each perform and determine which kind of encryption storage software performs the best. After being applied to the SSHD storage device using BestCrypt, AES 256-bit average 4K random write speed is 1.13 Mb/s. In comparison, AES 256-bit average 4K random write speed is 2.28 Mb/s when TrueCrypt is applied instead. AES 256-bit 4K random write speed performs 101.77% better when TrueCrypt is applied than BestCrypt. On the other hand, Serpent 256-bit 4K random write speed is 1.22 Mb/s when

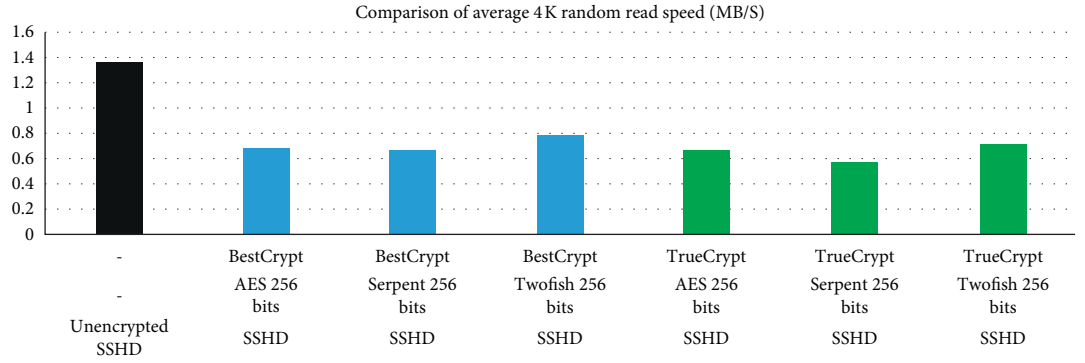

Figure 6: Comparison of the average 4K random read speed of SSHD after applying AES, Serpent, and Twofish 256 bits using BestCrypt and TrueCrypt.

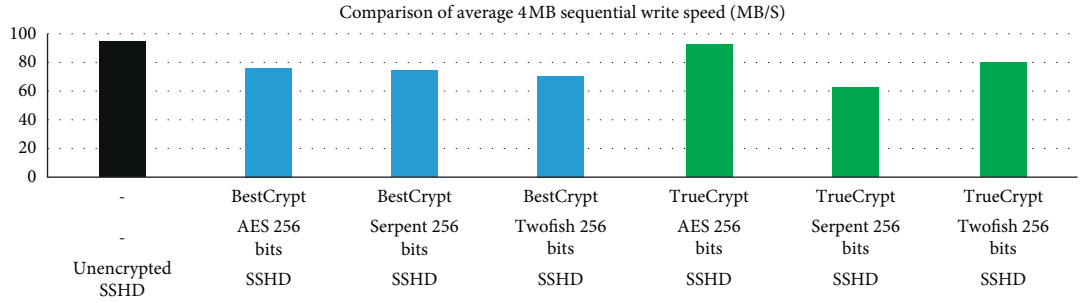

Figure 7: Comparison of the average 4 MB sequential write speed of SSHD after applying AES, Serpent, and Twofish 256 bits using BestCrypt and TrueCrypt.

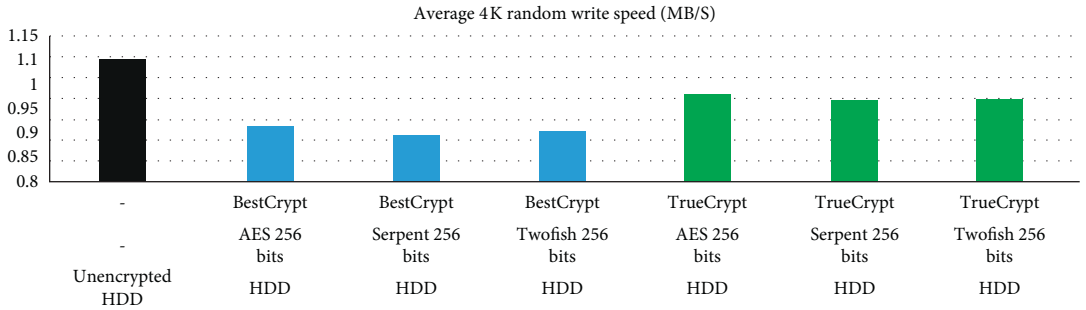

Figure 8: Comparison of the average 4K random write speed of SSHD after applying AES, Serpent, and Twofish 256 bits using BestCrypt and TrueCrypt.

TrueCrypt is applied and 1.46 Mb/s when BestCrypt is applied, which indicates that it performs 19.67% better on BestCrypt than on TrueCrypt. Finally, Twofish 256-bit 4K random write speed is 1.07 Mb/s when BestCrypt is applied and 1.69 Mb/s when TrueCrypt is applied. That is a 57.94% difference.

Figure 9 shows, in this experiment, three different encryption algorithms being applied to the SSD-based NAND MLC flash storage device using TrueCrypt and BestCrypt in order to test how well they each perform and determine which kind of encryption storage software performs the best. After being applied to the SSD-based NAND MLC flash storage device using BestCrypt, AES 256-bit average 4 MB sequential read speed is 389.54 Mb/s. In comparison, AES 256-bit average 4 MB sequential read speed is 410.47 Mb/s when True-Flash after applying AES, Serpent, and Twofish 256 bits using BestCrypt and TrueCrypt.

Crypt is applied instead. AES 256-bit 4 MB sequential read speed performs 5.37% better when TrueCrypt is applied than BestCrypt. On the other hand, Serpent 256-bit 4 MB sequential read speed is 251.00 Mb/s when TrueCrypt is applied and 254.55 Mb/s when BestCrypt is applied, which indicates that it performs 1.41% better on BestCrypt than on TrueCrypt. Finally, Twofish 256-bit 4 MB sequential read speed is 385.73 Mb/s when TrueCrypt is applied and 413.73 Mb/s when BestCrypt is applied. That is a 7.26% difference.

Figure 10 shows, in this experiment, three different encryption algorithms being applied to the SSD-based

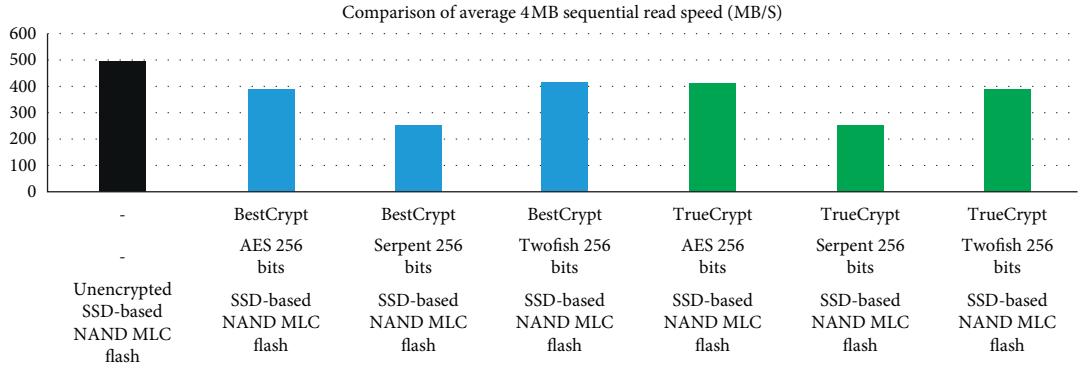

Figure 9: Comparison of the average 4 MB sequential read speed of SSD-based NAND MLC flash after applying AES, Serpent, and Twofish 256 bits using BestCrypt and TrueCrypt.

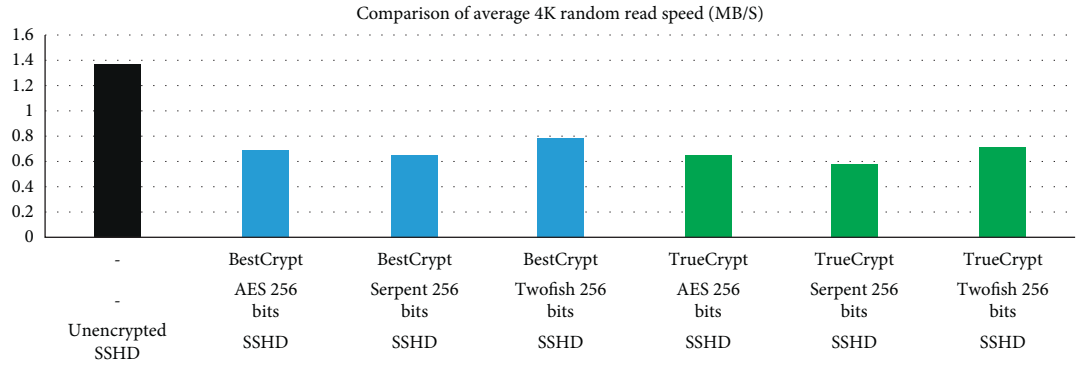

Figure 10: Comparison of the average 4K random read speed of SSD-based NAND MLC.

NAND MLC flash storage device using TrueCrypt and BestCrypt in order to test how well they each perform and determine which kind of encryption storage software performs the best. After being applied to the SSD-based NAND MLC storage device using TrueCrypt, AES 256-bit average 4K random read speed is 13.11 Mb/s. In comparison, AES 256-bit average 4K random read speed is 18.65 Mb/s when BestCrypt is applied instead. AES 256-bit 4K random read speed performs 42.26% better when BestCrypt is applied than TrueCrypt. Similarly, Serpent 256-bits 4K random read speed is 12.95 Mb/s when TrueCrypt is applied and 16.09 Mb/s when BestCrypt is applied, which indicates that it performs 24.25% better on BestCrypt than on TrueCrypt. Finally, Twofish 256-bit 4K random read speed is 13.01 Mb/s when TrueCrypt is applied and 17.88 Mb/s when BestCrypt is applied. That is a 37.43% difference.

Figure 11 shows, in this experiment, three different encryption algorithms being applied to the SSD-based NAND MLC flash storage device using TrueCrypt and BestCrypt in order to test how well they each perform and determine which kind of encryption storage software performs the best. After being applied to the SSD-based NAND MLC flash storage device using BestCrypt, AES 256-bit average 4 MB sequential write speed is 360.89 Mb/s. In comparison, AES 256-bit average 4 MB sequential write speed is 399.23 Mb/s when TrueCrypt is applied instead. AES 256-bit 4 MB sequential write speed performs 53.03% better when TrueCrypt is applied than BestCrypt. Similarly, Serpent 256-bit 4 MB sequential write speed is 212.64 Mb/s when BestCrypt is applied and 231.77 Mb/s when TrueCrypt is applied, which indicates that it performs 9% better on TrueCrypt than on BestCrypt. Finally, Twofish 256-bit 4 MB sequential write speed is 346.96 Mb/s when TrueCrypt is applied and 386.45 Mb/s when BestCrypt is applied. That is an 11.38% difference.

Figure 12 shows, in this experiment, three different encryption algorithms being applied to the SSD-based NAND MLC flash storage device using TrueCrypt and BestCrypt in order to test how well they each perform and determine which kind of encryption storage software performs the best. After being applied to the SSD-based NAND MLC storage device using BestCrypt, AES 256-bit average 4K random write speed is 36.20 Mb/s. In comparison, AES 256-bit average 4K random write speed is 36.24 Mb/s when TrueCrypt is applied instead. AES 256-bit 4K random read speed performs 0.11% better when TrueCrypt is applied than BestCrypt. On the other hand, Serpent 256-bit 4K random write speed is 26.21 Mb/s when TrueCrypt is applied and 33.52 Mb/s when BestCrypt is applied, which indicates that it performs 27.89% better on BestCrypt than on TrueCrypt. Finally, Twofish 256-bit 4K random write speed is 31.11 Mb/s when TrueCrypt is applied and 34.91 Mb/s when BestCrypt is applied. That is a 12.21% difference.

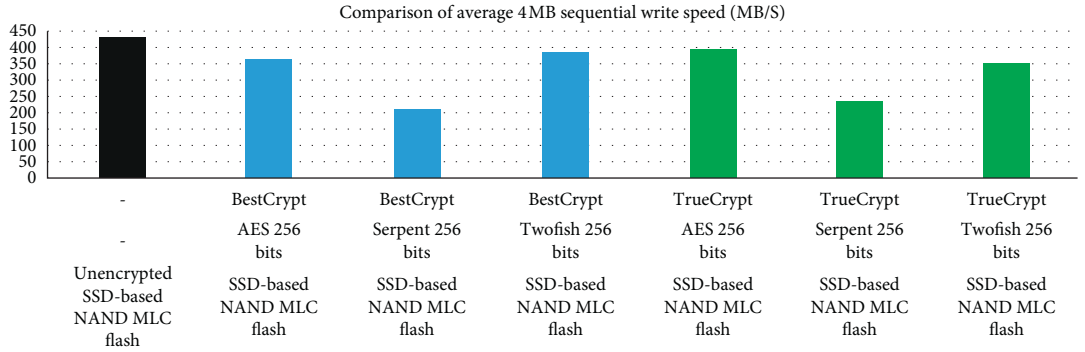

Figure 11: Comparison of the average 4 MB sequential write speed of SSD-based NAND MLC flash after applying AES, Serpent, and Twofish 256 bits using BestCrypt and TrueCrypt.

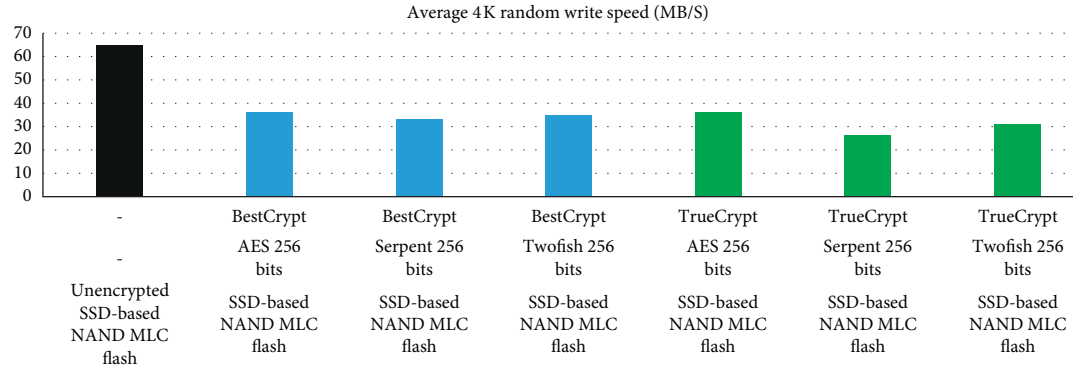

Figure 12: Comparison of the average 4K random write speed of SSD-based NAND MLC flash after applying AES, Serpent, and Twofish 256 bits using BestCrypt and TrueCrypt.

3. Conclusions

Data can be processed, transferred, and stored. In order to secure data in storage devices, this research paper studies in depth the performance of symmetric encryption algorithms on three different storage devices using BestCrypt (commercial storage encryption software) and TrueCrypt (open-source storage encryption software software). The three storage devices examined in this research paper are HDD, SSHD, and SSD-based NAND MLC flash memory. HDD and SSHD are forms of old storage technology, whereas SSD-based NAND MLC (SATA III interface) is form of current storage technology.

The research reveals that SSD-based NAND MLC flash (SATA III interface) has the highest level of performance before and after applying AES, Serpent, and Twofish 256-bit key using BestCrypt and TrueCrypt compared to HDD and SSHD. The research determined what kind of symmetric encryption algorithms, including AES, Serpent, and Twofish, performs the best on each storage device tested in this research paper. The encryption algorithm that performs best on HDD is AES 256-bit key compared to Serpent and Twofish 256-bit key using BestCrypt. However, Twofish 256 bits performs better on SSHD and SSD-based NAND MLC flash compared to AES and Serpent 256-bit key using BestCrypt. On the other hand, AES 256-bit key has the highest level of encryption performance on SSHD and SSD-based NAND MLC flash compared to Serpent and Twofish 256-bit key using TrueCrypt. Additionally, when Twofish 256 bits is used to encrypt HDD using TrueCrypt, Twofish 256-bit key performs the best compared to AES and Serpent 256 bits using the same storage encryption software. Overall, AES, Serpent, and Twofish 256-bit key perform the best on HDD using TrueCrypt compared to BestCrypt. On other hand, AES, Serpent, and Twofish 256-bit key have performed better on SSHD and SSD-based NAND MLC flash (SATA III interface) using BestCrypt compared to TrueCrypt. However, the research proves that AES and Twofish 256 bits consistently perform better across different storage devices than Serpent 256 bits using BestCrypt and TrueCrypt.

Choosing the right encryption algorithm will have a significant impact on the performance of a storage device. Careful evaluation and selection of encryption algorithms is especially essential when using SSD-based NAND flash memory and SSHD as the performance of each algorithm varies greatly depending on which device it is applied to. On the other hand, the performance of different encryption on HDD remains reasonably consistent across different disk access patterns.

Data Availability

The data used in this research will be provided upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] Z. P. Buba and G. M. Wajiga, "Cryptographic algorithms for secure data communication," *International Journal of Computer Science and Security (IJCSS)*, vol. 5, no. 2, pp. 227–243, 2011.

[2] Y. Kumar, R. Munjal, and H. Sharma, "Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures," *International Journal of Computer Science and Management Studies*, vol. 11, no. 3, pp. 60–63, 2011.

[3] H. B. Pethe and S. Pande, "A survey on different secret key cryptographic algorithms," *IBMRD's Journal of Management & Research*, vol. 3, no. 1, pp. 142–150, 2014.

[4] F. Wu, L. Wang, and J. Wan, "A low cost and inner-round pipelined design of ecb-aes-256 crypto engine for solid state disk," in *Proceedings of the Fifth International Conference on Networking, Architecture, and Storage*, pp. 485–491, IEEE, Macau, China, July 2010.

[5] S. Jung and Y. H. Song, "Data loss recovery for power failure in flash memory storage systems," *Journal of Systems Architecture*, vol. 61, no. 1, pp. 12–27, 2015.

[6] S. S. Rizvi and T. S. Chung, "Flash ssd vs hdd: high performance oriented modern embedded and multimedia storage systems," in *Proceedings of the 2nd International Conference on Computer Engineering and Technology*, vol. 7, pp. V7–V297, IEEE, Chengdu, China, April 2010.

[7] W. Stallings, Network and Internetwork Security: *Principles and Practice*, vol. 1, Prentice-Hall, Englewood Cliffs, NJ, USA, 1995.

[8] Q. x. Miao, "Research and analysis on encryption principle of truecrypt software system," in *Proceedings of the 2nd International Conference on Information Science and Engineering*, pp. 1409–1412, IEEE, Hangzhou, China, December 2010.

[9] J. Gray, "Jetico's BestCrypt container encryption," 2017.

[10] A. Elminaam, A. Kader, and M. Hadhoud, "Performance evaluation of symmetric encryption algorithms," *Communications of the IBIMA*, vol. 8, pp. 58–64, 2009.

[11] S. Kansal and M. Mittal, "Performance evaluation of various symmetric encryption algorithms," in *Proceedings of the International Conference on Parallel, Distributed and Grid Computing*, pp. 105–109, IEEE, Solan, India, December 2014.

[12] N. B. Slimane, N. Aouf, K. Bouallegue, and M. Machhout, "Hash key-based image cryptosystem using chaotic maps and cellular automata," in *Proceedings of the 15th International MultiConference on Systems, Signals & Devices (SSD)*, pp. 190–194, IEEE, Hammamet, Tunisia, March 2018.

[13] Y. Yuan, Y. Yang, L. Wu, and X. Zhang, "A high performance encryption system basedon AES algorithm with novel hardware implementation," in *Proceedings of the International Conference on Electron Devices and Solid State Circuits (EDSSC)*, pp. 1-2, IEEE, Shenzhen, China, June 2018.

[14] P. Lin, Y. Chang, Y. Li, W. Wang et al., "Achieving fast sanitization with zero live data copy for MLC flash memory," in *Proceedings of the 2018 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, San Diego, CA, USA, February 2018.

[15] C. Meijer and B. Van Gastel, "Self-encrypting deception: weaknesses in the encryption of solid state drives," in *Proceedings of the Symposium on Security and Privacy (SP)*, pp. 72–87, IEEE, San Francisco, CA, USA, May 2019.