advances in Technology

Adv. Technol. ***2024****, 3(2), 75-96*

Secure Cloud Storage Solution with "Seafile" & "NextCloud": A Resilient Efficiency Assessment

Gavin Dutcher[1], Koku Azianyo[1], Thivanka P.B. M. Dissanayake[1], and Akalanka B. Mailewa[2,*]

[1]Department of Information Assurance, College of Business, St. Cloud State University, Minnesota, USA
[2]Department of Computer Science & Information Technology, St. Cloud State University, St. Cloud, Minnesota, USA

Corresponding Author: amailewa@stcloudstate.edu

Received: 16 January 2023; Revised: 17 July 2023; Accepted: 06 March 2024; Published: 02 April 2024

Abstract
Storage and file synchronization have become increasingly important services in our everyday lives. With cloud storage providers giving users access to file space in the cloud, one might wonder how efficient these cloud storage providers are with their encryption methods. There are many different cloud storage providers and programs to set up a cloud storage solution. This paper focuses on two secure cloud storage solutions, Seafile, and NextCloud, and determines the efficiency of these cloud storage solutions' encryption methods. By determining the efficiency of these secure cloud storage providers' encryption methods, it can help others determine which of these providers will fit their needs. To determine efficiency, the CPU, memory, and network usage of these cloud storage solutions will be measured at idle and when files are being uploaded to them. To measure the CPU, memory, and network usage, 'dstat' will be used to capture their usages and record them to a CSV file. It is expected that both cloud solutions will have better performance when they have files being uploaded to them with no encryption. However, with the encryption methods of both cloud solutions being lightweight, that was not the case.

Keywords: attacks, cloud efficiency, data encryption, Google cloud, Seafile cloud, security and privacy

Introduction

Today with the rapid development of technology commonly known as Information Technology (IT), we can do things that before were difficult if not impossible. IT through its advanced developments we have what we also call Cloud Storage. Cloud storage in its basic term would be defined as being a cloud computing model that stores data on the internet through a cloud computing provider who manages and operates data storage as a service [1]. By this definition, we can understand several things. Cloud storage has evolved over time. Initially, the cloud storage can only be used through a third person which can be a person, an individual, or an organization [1]. Today, this is no longer the case, cloud storage can be put into use by anyone who wishes to have one. Therefore, we have a multitude of cloud storage available to any individual, without payment. As said, cloud storage has become popular, we can distinguish them like Dropbox, Azure, NextCloud, Google Drive, etc [2-4]. But our work concerns particularly two of these cloud storages mentioned namely NextCloud [5] and Seafile. Seafile is a cloud storage just like the others

which can be used to store data, encrypt data in transit as in rest [6]. In this study, we are going to compare these two cloud storages in terms of efficiency, security, and storage capacity [7, 8]. We first discuss of IT in general and cloud computing as information technology has always evolved, in line with new technologies but also to meet new demands. The first computers used by companies, the mainframes, were dethroned by the mini computing which bowed before the microcomputer but today, they compute with the PDAs (personal digital assistant) and smartphones [9, 10]. Computing mechanisms are always changing as those are centralized most of the time with the advent of data centers and things mentioned before, it goes dematerialized and becomes cloud computing [11]. Computing power is virtualized and consumed where and when it is needed and becomes extensible, all thanks to the Internet. Whenever we use an application like Facebook, LinkedIn, Gmail, or Hotmail, we are involved in cloud computing. Cloud Computing is a major concept in the evolution of computing in recent years. This concept refers to the use of the computing and storage capacities of computers and servers distributed around the world provided as a service through internet technologies to a multitude of external users [12]. Cloud Computing is therefore a concept of deportation to remote servers from computer processing traditionally carried out on local computers. Thus, the end users or companies are no longer the managers of their own IT capacities but can access many online services without having to manage the underlying, often complex infrastructure. Also, data and applications no longer reside on the local computer, but in a cloud of remote servers interconnected with the excellent bandwidth essential to the fluidity of the system [13, 14] [15]. Therefore, it is certain that there is no any "cloud computing" without having a solid, efficient, and reliable "cloud storage" mechanism which reads and writes the data and *vice versa* to/from the storage and cloud applications.

Cloud Storage

Cloud storage is a place where we can store data and this data is accessible wherever it is called by the cloud-networked application [16]. Some cloud providers are not demanding as to the amount of data you want to store [17]. These providers give users the choice to increase their memory capacity at their convenience, at any time, and with some patience, it is possible to build your own super cloud with more than 100 GB of free storage. In addition, with a lot of patience (and pestering of user's plans), it is possible to nab more than 225 GB of storage [18]. The research question here is "RQ: Is it possible to continuously accommodate user's demand by all cloud service providers equally in a reliable and secure manner such as NextCloud and Seafile otherwise how effective is one versus the other?

Cloud Storage Comparison

NextCloud is one of the most successful cloud storage providers [5, 19]. The effectiveness of NextCloud is proven through user reviews around the world. NextCloud is among the providers that ensure that your files or documents are protected, NextCloud ensures your identity or your sensitive document is encrypted to ensure your privacy. Once your files are in the NextCloud, you are guaranteed security. NextCloud server is an efficient, easy-to-use interface is one of the main things that sets NextCloud apart from the competition, according to NextCloud. But our goal here with NextCloud efficiency is a little

different. By the way, our objective is to see or measure its efficiency in relation to its capacity, i.e., CPU usage, network usage, in short, to what extent its efficiency can be demonstrated. Therefore, in our testing, we will demonstrate this by a series of tests with different capacities of files and consider when files are encrypted and when they are not. We will observe the behavior or variation of CPUs, network usage, etc. for this purpose.

Seafile, like NextCloud, is an open-source cloud server that can be used to store data where it is not popular like NextCloud, but has the same services and features that other cloud storage providers can offer [6, 20] . In this precise research study, it is demonstrated how efficient Seafile is compared to NextCloud. According to the results we obtained in our pre-testing of two servers, Seafile is ahead when it comes to CPUs usage efficiency, network usage, and capacity to name a few and we provide much more detail in the testing section with supporting figures and numbers which will be able to help people including businesses, education, and other target fields to understand how the concept of cloud computing is closely related with the cloud storage.

When choosing a cloud storage provider, two important aspects are security and efficiency [21, 22]. Therefore, by evaluating the encryption and non-encryption efficiency of NextCloud and Seafile, it can help users decide which provider to choose. It also can help give users insight as to how efficient the encryption methods used are compared to using no encryption depending on the amount and size of files being uploaded to the server. In the background section of this article discuss the literature review to give a better understanding of the research. Thereafter authors address methodology, which explains how the experiment was done. Finally, in the results section, the authors describe the findings from the research experiments.

Background and Related Work

Cloud computing is a buzzword in today's IT environment as Cloud computing keeps seeing new faces every day while maintaining its principles. Cloud computing is the fact of having IT services virtually, that is to say, everything is controlled by the network or the internet. But, to have a good internet connection, you also need a good quality of hardware and software [23]. The hardware is extended here by peripheral devices like CPUs, RAM memory, routers, switches, etc. which ensure the connection [24]. This research consists of measuring these tools in order to ensure the smooth running of cloud computing, in this specific case, we are planning to collect data that demonstrates the role that these tools play in the cloud computing environment. As nobody is aware that good management of these tools will make it possible to have sufficient space to store more data, and the data center which stores this data can function effectively but is not the case. The data centers continue to operate at low resource utilization [25]. This prior work has determined that data centers are struggling with data that are too heavy, making them too under-operated, thus the resources are in turn underutilized. Based on our work, we have determined that the idle CPU usage is greater than any results from our testing. In our research, we also noticed that encrypted files use more memory and network than non-encrypted files, but that is something normal since files are encrypted, they use more time, or it takes more to be encrypted and

something will happen when trying to decrypt those files. Table 1, below shows basically the results of the prior work done by Wang et. al (2021).

Table 1: Average CPU stats in the number of cores [25].

Parameter	IndexServe (500QPS)	Memeached (40KQPS)	moses (400QPS)	img-dnn (2000QPS)
CPU usage	1.3	2.3	1.5	1.7
Peak CPU usage	7	7.7	5.2	6.9

Having efficient cloud servers is extremely important, especially when there are many users accessing the server at once. Olakanmi and Odeyemi, (2021) propose a novel scheme that has a faster server-aided de-duplication scheme with an efficient authenticated key agreement [26]. The de-duplication in this scheme is performed by the server to remove multiple copies of the same outsourced data. The authenticated key agreement also makes the scheme capable of thwarting any attacks related to confidentiality [26, 27]. Compared to other state-of-the-art de-duplication schemes, a security, computational, and communication cost analysis shows that the proposed scheme has a high performance at low complexity and cost [26, 28].

Cloud servers are used in many different fields and one of those fields is healthcare. A security scheme proposed by Olakanmi and Odeyemi (2020) provides effective health information management and secure access to patients' health information in an e-health system [29]. The purpose for this is to reduce information management bottlenecks, security, and privacy challenges in the e-health environment [29, 30]. Reduced access time through hierarchical storage is another benefit of the proposed scheme. The scheme works by having a two-layer security where the first layer uses symmetric encryption to secure the exchange of PHI (personal health information) between the MSP (middle-security provider) and the patient and the second layer uses a modified CP-ABE (public encryption scheme) to enforce fine-grained access control on the uploaded PHI. In this scenario, the patient has a wearable medical device with low computational power. Due to the low computational power, the attribute-based encryption is pushed to the MSP. The work is then further subdivided into two parts, the framework for effective management of PHI in the e-health system and the expressible access control scheme for fog-enhanced e-health systems [29, 31].

Many cloud servers must process large amounts of data and having an efficient computation offloading scheme is vital for this as it can speed up tasks and save energy. A computation offloading scheme in Fog-Cloud-IoT environments (SecOFF-FCIoT) proposed by Alli and Alam (2019) makes use of machine learning strategies to accomplish efficient, secure offloading in a FoG-IoT setting [32]. The scheme is also secure and if effective in balancing the trade-off between latency and energy consumption. In the implementation, the scheme was also shown to have a marginal delay and negligible energy consumption, making the scheme robust.

With the growth of the vehicular cloud, cloud servers will need to keep up with the growth to efficiently compute the data. Mistareehi et al., (2021) propose a secure and distributed architecture for the vehicular cloud [33]. This architecture uses cloud servers to give vehicles services such as parking management,

accident alert, traffic updates, and cooperative driving. The architecture ensures the privacy of vehicles and supports scalable and secure message dissemination using the vehicular infrastructure. The distributed architecture for the vehicular cloud is hierarchical and it consists of vehicles, RSUs (roadside units), regional clouds, and the central cloud. The vehicles and RSUs communicate with each other and from the results, it show the RSUs has less computation overhead as compared to the vehicles. With respect to energy consumption and throughput, when messages are encrypted, they have little overhead.

When using cloud servers, it is important to reduce data redundancies and bandwidth for users as much as possible. Zhang et al. (2021) propose a secure and efficient data deduplication scheme (SED) in a joint cloud storage system without depending on the help of a trusted key server (KS) [34]. SED is shown to effectively eliminate data redundancies with low computational complexity and communication and storage overhead but with SED, the usability of the client-side is increased. The proposed SED is made up of five components: system setup, data outsourcing, data access, data update, and data sharing. In the system setup, users and the cloud servers perform the initialization and mutual authentication. The data outsourcing phase is where the data is encrypted and stored in cloud storage providers hence data access is the phase where users can retrieve their data and the last two phases, data update and data sharing is where the users can respectively update and share their data in the cloud [34, 35].

Methodology

In this research, our technique for testing encryption performance for these cloud servers is by running tests that capture the Central Processing Unit (CPU), network, and memory usage of the server computer. We will run seven different tests for each server. The first test is an idle run for five minutes, to see the CPU, network, and memory usage while the server is running, and nothing is being uploaded. The next two tests measure the performance of many small files being uploaded to the server. There will be 10,000 files of 5 kilobytes each uploaded to the server in first an encrypted folder and then a folder that has no encryption. After that, the next two tests will be 100 files of 20 megabytes each in both an encrypted folder and a folder with no encryption. The last two tests will be 2 files of 1 gigabyte each in an encrypted folder and a folder that is not encrypted. While each of these tests are being performed, we will be using a Linux command line tool called "dstat" to measure the server computer's CPU, network, and memory usage. We will then export the results to a CSV file to analyze the results. Once we collect all the results from "dstat", we will take the average of the CPU user percentage, CPU system percentage, CPU idle percentage, CPU wait percentage, network receive, network send, memory used, and memory free. With that data we will compare these averages against the idle test of the same server and encryption and decryption performance of the same test (i.e., comparing Seafile 100 20 MB file encryption against Seafile 100 20 MB file no encryption). This project the experiment testbed is running on Ubuntu 18.0.4 with 4GB of memory and an Intel i7 processor (CPU). Figure 2 depicts the methodology testing process. There will be a total of 14 tests, 7 on Seafile and 7 on NextCloud in the states shown in Figure 1.

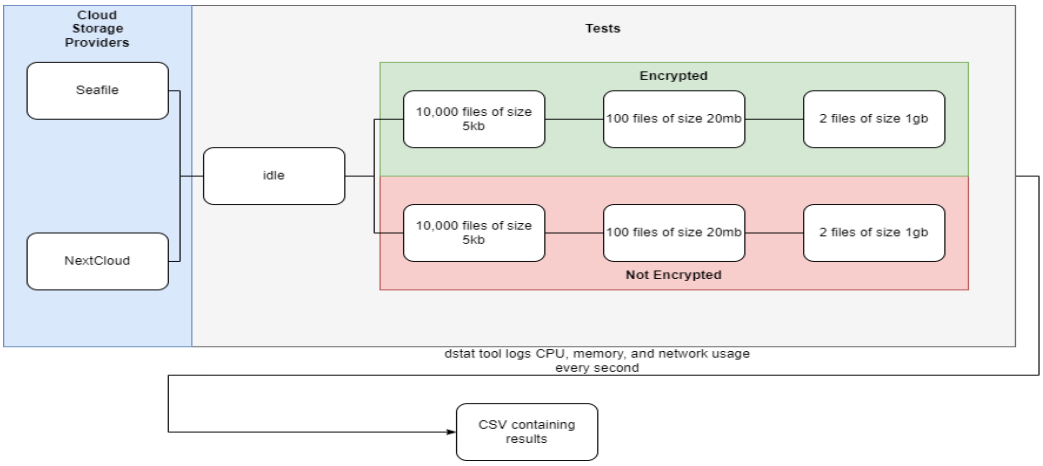

Figure 1: Methodology testing process

Results

This section present excremental results to evaluate and compare the Seafile cloud based solutions with NextCloud cloud based solutions.

Seafile Idle Results

Table 2 presents the CPU, network, and memory usage of the server computer with no files being uploaded to it. This is done as a baseline test for the Seafile server.

Table 2: Seafile idle results

CPU User Avg	**CPU Sys Avg**	**CPU Idle Avg**	**CPU Wait Avg**
8.3%	.427%	90%	1.2%
Network Receive Avg	**Network Send Average**		
364.4 Bytes/Second	26.01 Bytes/Second		
Memory Used Avg	**Memory Free Avg**		
3154 Megabytes	1757 Megabytes		

Seafile 10,000, 5 KB File Encryption Results

Table 3 shows the CPU, network, and memory usage of the server computer with 10,000, 5 KB files being uploaded into an encrypted folder. These results show increased usage in CPU, network, and memory compared to the idle test, as expected.

Table 3. Seafile 10,000, 5 KB file encryption results

CPU User Avg	**CPU Sys Avg**	**CPU Idle Avg**	**CPU Wait Avg**
30.39%	1.96%	59.11%	9.92%
Network Receive Avg		**Network Send Average**	
26.518 Kilobytes/Second		25.84 Kilobytes/Second	
Memory Used Avg		**Memory Free Avg**	
3529 Megabytes		1374 Megabytes	

Seafile 10,000, 5 KB File No Encryption Results

Table 4 explains the CPU, network, and memory usage of the server computer with 10,000, 5 KB files being uploaded into a non-encrypted folder. The results are like Table II, and it shows that there is little difference in terms of efficiency of encryption verses no encryption when 10,000 files of 5 KB each are uploaded to Seafile.

Table 4. Seafile 10,000, 5 KB file no encryption results

CPU User Avg	**CPU Sys Avg**	**CPU Idle Avg**	**CPU Wait Avg**
30.95%	2.05%	57.06%	9.92%
Network Receive Avg		**Network Send Average**	
26.489 Kilobytes/Second		25.83 Kilobytes/Second	
Memory Used Avg		**Memory Free Avg**	
3492 Megabytes		1579 Megabytes	

Seafile 100, 20 MB File Encryption Results

Table 5 presents the CPU, network, and memory usage of the server computer with 100, 20 MB files being uploaded into an encrypted folder. CPU usage is down compared to Table II and Table III, but the network and memory usage is up.

Table 5. Seafile 100, 20 MB file encryption results

CPU User Avg	**CPU Sys Avg**	**CPU Idle Avg**	**CPU Wait Avg**
12.95%	2.98%	78.87%	5.17%
Network Receive Avg	**Network Send Average**		
685 Kilobytes/Second	12.58 Kilobytes/Second		
Memory Used Avg	**Memory Free Avg**		
3610 Megabytes	1304 Megabytes		

Seafile 100, 20 MB File No Encryption Results

Table V shows the CPU, network, and memory usage of the server computer with 100, 20 MB files being uploaded into a non-encrypted folder. The results are like Table IV, and it shows that there is little difference in terms of efficiency of encryption verses no encryption when 100 files of 20 MB each are uploaded to Seafile.

Table 6. Seafile 100, 20 MB file no encryption results

CPU User Avg	**CPU Sys Avg**	**CPU Idle Avg**	**CPU Wait Avg**
13.69%	2.91%	79.11%	4.27%
Network Receive Avg	**Network Send Average**		
700 Kilobytes/Second	12.74 Kilobytes/Second		
Memory Used Avg	**Memory Free Avg**		
3707 Megabytes	1291 Megabytes		

Seafile 2, 1 GB File Encryption Results

Table 7 explains the CPU, network, and memory usage of the server computer with 2, 1 GB files being uploaded into an encrypted folder. CPU and memory usage is down compared to Table IV and Table V, but network usage is up.

Table 7. Seafile 2, 1 GB file encryption results

CPU User Avg	**CPU Sys Avg**	**CPU Idle Avg**	**CPU Wait Avg**
9.42%	3.03%	85.5%	2.03%
Network Receive Avg	**Network Send Average**		
837 Kilobytes/Second	15 Kilobytes/Second		
Memory Used Avg	**Memory Free Avg**		
2049 Megabytes	1302 Megabytes		

Seafile 2, 1 GB File No Encryption Results

Table 8 presents the CPU, network, and memory usage of the server computer with 2, 1 GB files being uploaded into a non-encrypted folder. The results show a slight increase in CPU, memory, and network usage but not by a significant amount.

Table 8. Seafile 2, 1 GB file no encryption results

CPU User Avg	**CPU Sys Avg**	**CPU Idle Avg**	**CPU Wait Avg**
9.98%	3.28%	84.63%	2.1%
Network Receive Avg	**Network Send Average**		
919 Kilobytes/Second	16 Kilobytes/Second		
Memory Used Avg	**Memory Free Avg**		
2126 Megabytes	1402 Megabytes		

NextCloud Idle Results

Table 9 shows the CPU, network, and memory usage of the server computer with no files being uploaded to it. This test is a baseline test for the NextCloud server.

Table 9. NextCloud idle results

CPU User Avg	**CPU Sys Avg**	**CPU Idle Avg**	**CPU Wait Avg**
6.9%	.87%	91.94%	.27%
Network Receive Avg	**Network Send Average**		
422.3 Bytes/Second	103.13 Bytes/Second		
Memory Used Avg	**Memory Free Avg**		
2024 Megabytes	2878 Megabytes		

NextCloud 10,000, 5 KB File Encryption Results

Table 10 presents the CPU, network, and memory usage of the server computer with 10,000, 5 KB files being uploaded into an encrypted folder. The results show nearly all the CPU was used.

Table 10. NextCloud 10,000, 5 KB file encryption results

CPU User Avg	**CPU Sys Avg**	**CPU Idle Avg**	**CPU Wait Avg**
96.59%	2.57%	.82%	.009%
Network Receive Avg	**Network Send Average**		
8.8 Kilobytes/Second	9.08 Kilobytes/Second		
Memory Used Avg	**Memory Free Avg**		
2157 Megabytes	7672 Megabytes		

NextCloud 10,000, 5 KB File No Encryption Results

Table 11 explains the CPU, network, and memory usage of the server computer with 10,000, 5 KB files being uploaded into a non-encrypted folder. The results are like Table IX, and it shows that there is little difference in terms of efficiency of encryption verses no encryption when 10,000 files of 5 KB each are uploaded to NextCloud.

Table 11. NextCloud 10,000, 5 KB file no encryption results

CPU User Avg	**CPU Sys Avg**	**CPU Idle Avg**	**CPU Wait Avg**
96.93%	2.39%	.66%	.006%
Network Receive Avg	**Network Send Average**		
9.17 Kilobytes/Second	9.54 Kilobytes/Second		
Memory Used Avg	**Memory Free Avg**		
1856 Megabytes	1271 Megabytes		

NextCloud 100, 20 MB File Encryption Results

Table 12 shows the CPU, network, and memory usage of the server computer with 100, 20 MB files being uploaded into an encrypted folder. The results show significantly less CPU is used compared to Table 10-11.

Table 12. NextCloud 100, 20 MB file encryption results

CPU User Avg	**CPU Sys Avg**	**CPU Idle Avg**	**CPU Wait Avg**
10.14%	1.39%	86.35%	2.1%
Network Receive Avg	**Network Send Average**		
634.97 Kilobytes/Second	12.95 Kilobytes/Second		
Memory Used Avg	**Memory Free Avg**		
2098 Megabytes	2316 Megabytes		

NextCloud 100, 20 MB File No Encryption Results

Table 13 presents the CPU, network, and memory usage of the server computer with 100, 20 MB files being uploaded into a non-encrypted folder. The results show that there is slightly less CPU, network, and memory used as compared to Table 12.

Table 13. NextCloud 100, 20 MB file no encryption results

CPU User Avg	**CPU Sys Avg**	**CPU Idle Avg**	**CPU Wait Avg**
8.51%	1.16%	88.88%	1.42%
Network Receive Avg	**Network Send Average**		
597 Kilobytes/Second	11.96 Kilobytes/Second		
Memory Used Avg	**Memory Free Avg**		
1775 Megabytes	3351 Megabytes		

NextCloud 2, 1 GB File Encryption Results

Table 14 explains the CPU, network, and memory usage of the server computer with 2, 1 GB files being uploaded into an encrypted folder. As compared to Table 12-13, there is less CPU usage in Table XIII, but more network and memory usage.

Table 14. NextCloud 2, 1 GB file encryption results

CPU User Avg	**CPU Sys Avg**	**CPU IdleAvg**	**CPU Wait Avg**
6.76%	1.17%	90.9%	1.145%
Network Receive Avg	**Network Send Average**		
627 Kilobytes/Second	12.89 Kilobytes/Second		
Memory Used Avg	**Memory Free Avg**		
2000 Megabytes	1654 Megabytes		

NextCloud 2, 1 GB File No Encryption Results

Table 15 shows the CPU, network, and memory usage of the server computer with 2, 1 GB files being uploaded into a non-encrypted folder. In every category, Table 15 is more efficient than its encrypted counterpart, Table 14, but not by a significant amount.

Table 15. NextCloud 2, 1 GB file no encryption results

CPU User Avg	**CPU Sys Avg**	**CPU IdleAvg**	**CPU Wait Avg**
4.8%	.94%	93.2%	.97%
Network Receive Avg	**Network Send Average**		
536 Kilobytes/Second	10.77 Kilobytes/Second		
Memory Used Avg	**Memory Free Avg**		
1657 Megabytes	1376 Megabytes		

Comparisons

We will first start out by comparing Seafile 10,000, 5 KB file encryption efficiency and 10,000, 5 KB file no encryption efficiency in Figure 2-4.

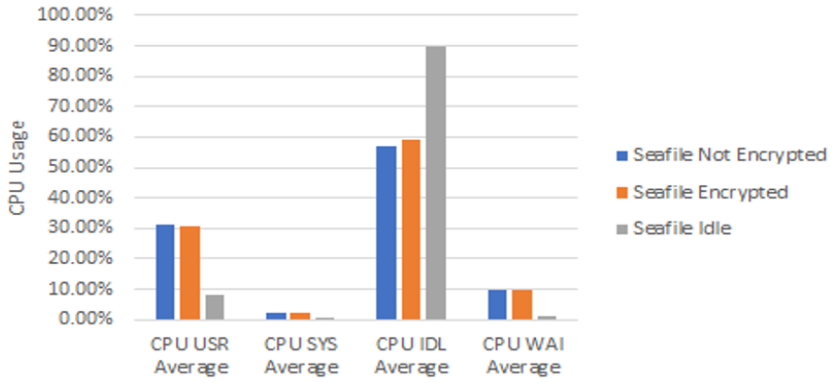

Figure 2. Seafile 10,000 5 KB files CPU usage

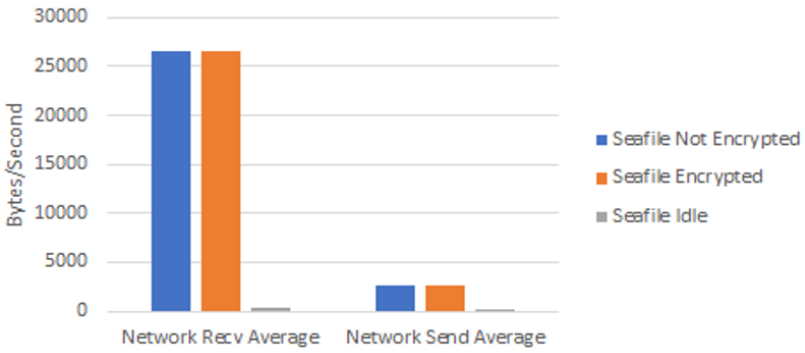

Figure 3. Seafile 10,000 5 KB files network usage

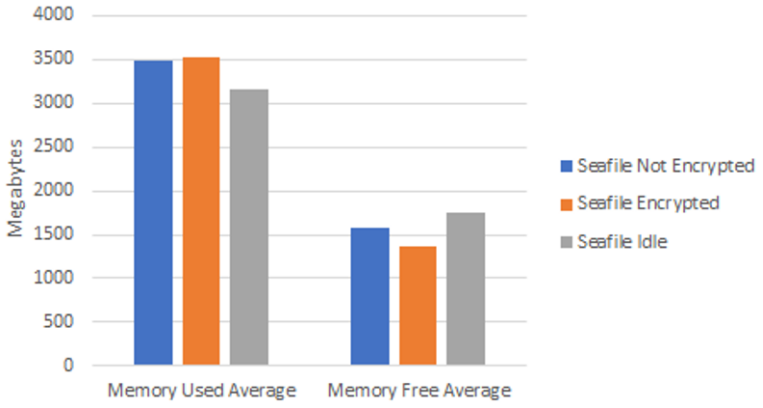

Figure 4. Seafile 10,000 5 KB files memory usage

We can see from Figure 2-4 that the performance between the encrypted and not encrypted is similar. The encryption did use slightly more memory on average than having no encryption. Next, we will compare Seafile 100, 20 MB encryption efficiency and 100, 20 MB no encryption efficiency in Figure 5-7.

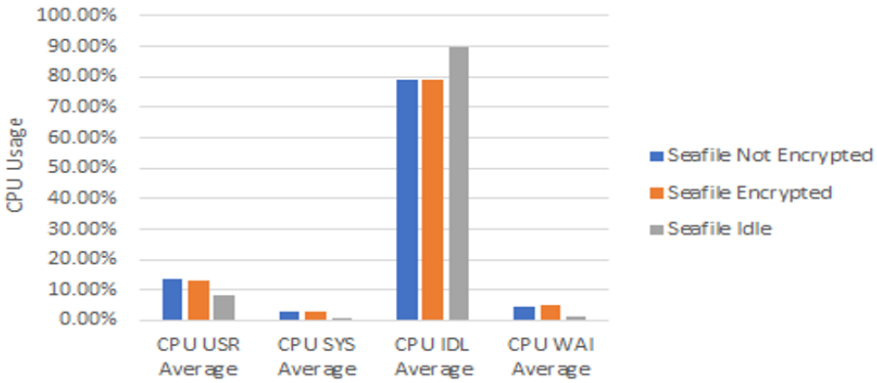

Figure 5. Seafile 100 20 MB files CPU usage

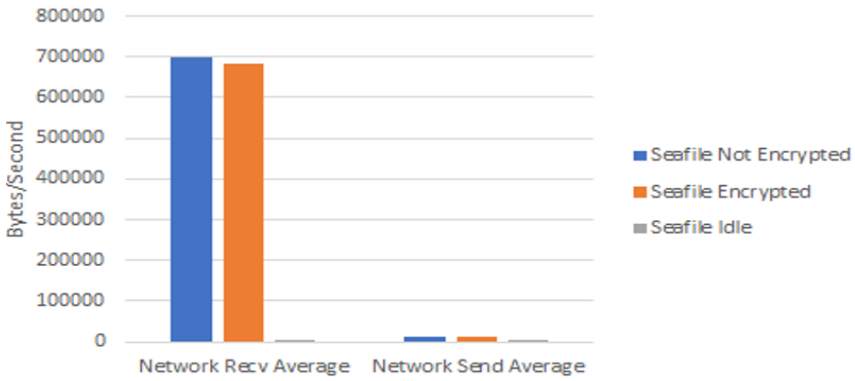

Figure 6. Seafile 100 20 MB files network usage

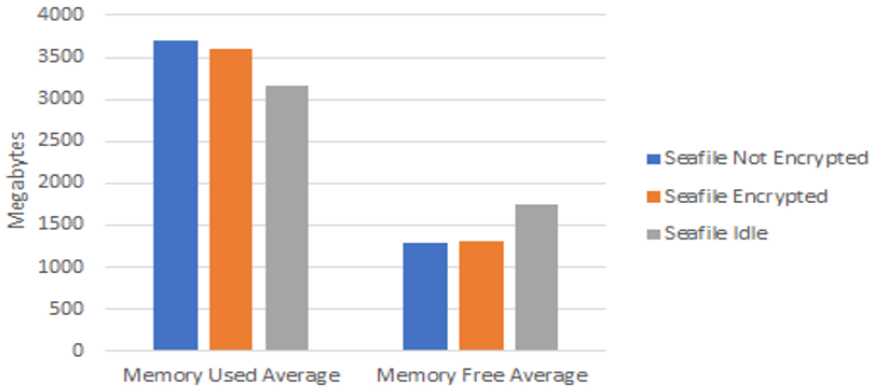

Figure 7. Seafile 100 20 MB files memory usage

Figure 5-7 show that the average between the encryption efficiency and no encryption efficiency is similar. Overall, the no encryption efficiency is slightly less than the encryption efficiency. Next, we have compared Seafile 2, 1 GB encryption efficiency and 2, 1 GB no encryption efficiency in Figure 8, Figure 9, and Figure 10.

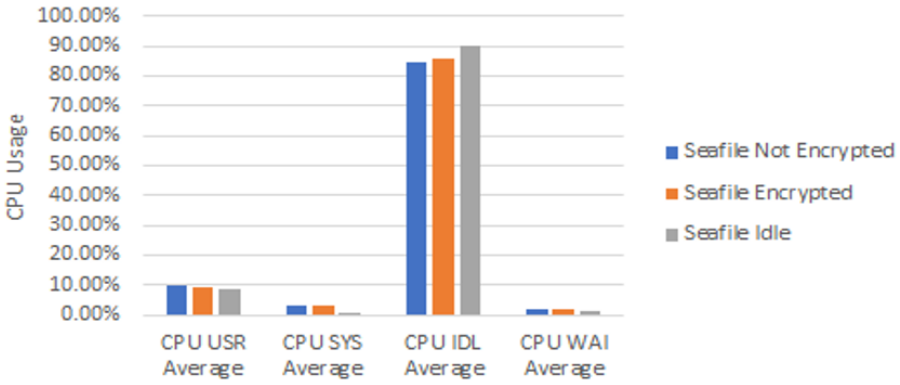

Figure 8. Seafile 2 1 GB files CPU usage

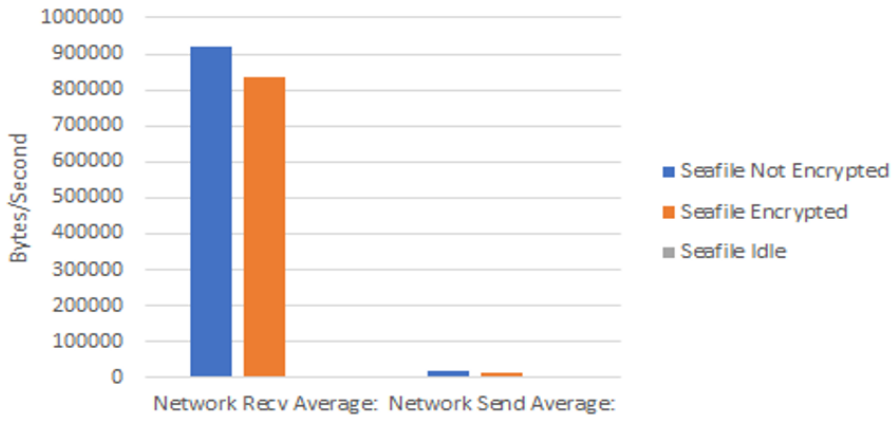

Figure 9. Seafile 2 1 GB files network usage

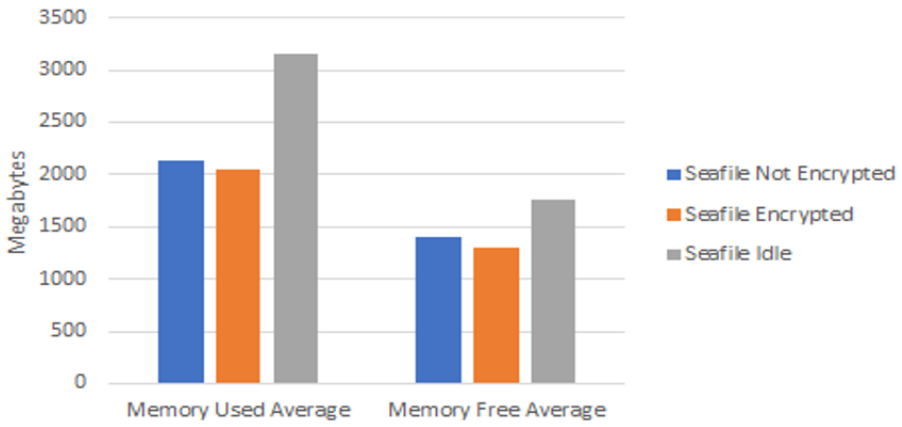

Figure 10. Seafile 2 1 GB files memory usage

Figure 8-10 shows that the average between the encryption efficiency and no encryption efficiency is similar. Overall, the no encryption efficiency is slightly less than the encryption efficiency. Thereafter we have compared NextCloud 10,000, 5 KB file encryption efficiency and 10,000, 5 KB file no encryption efficiency in Figure 11- 13.

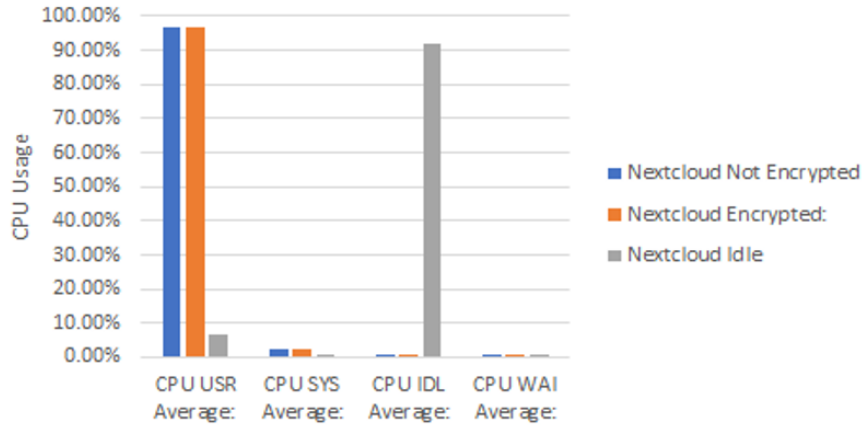

Figure 11. Seafile 10,000 5 KB files CPU usage

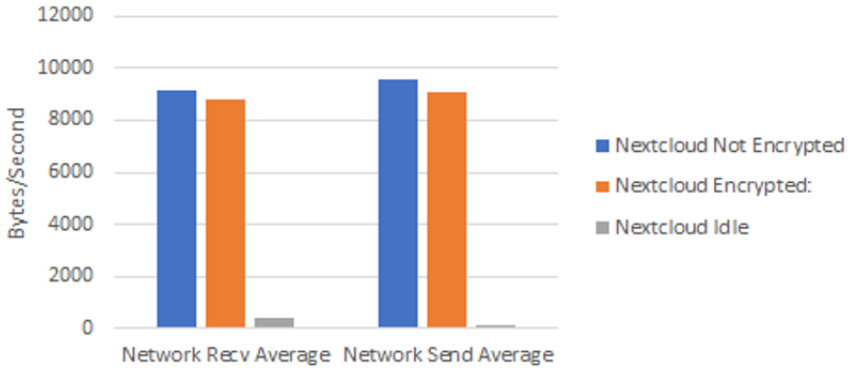

Figure 12. Seafile 10,000 5 KB files network usage

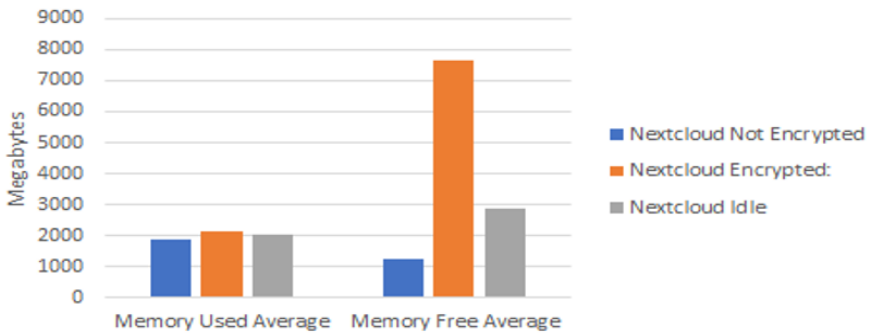

Figure 13. Seafile 10,000 5 KB files memory usage

Figure 11, Figure 12, and Figure 13 explain that there is not much of a difference between encryption efficiency and no encryption efficiency. On average, the memory usage of encryption is slightly more than that of no encryption and the CPU usage on average is very similar between the two.

Further we have compared NextCloud 100, 20 MB encryption efficiency and 100, 20 MB no encryption efficiency in Figure 14- 16.

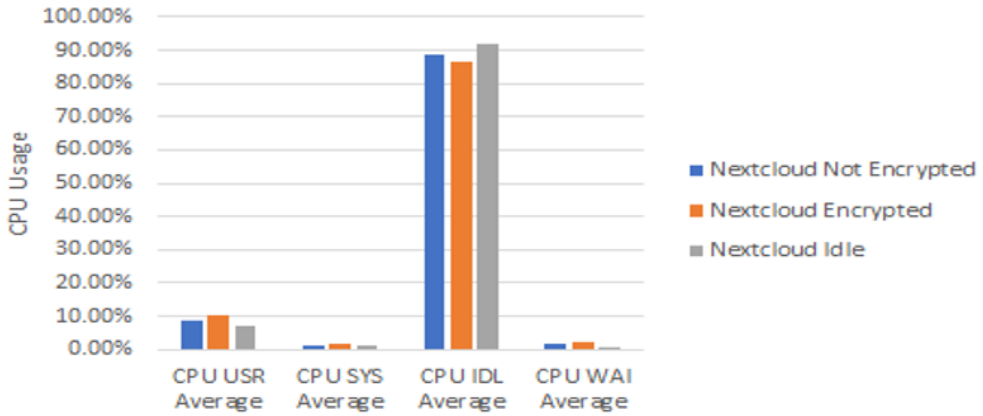

Figure 14. NextCloud 100 20 MB files CPU usage

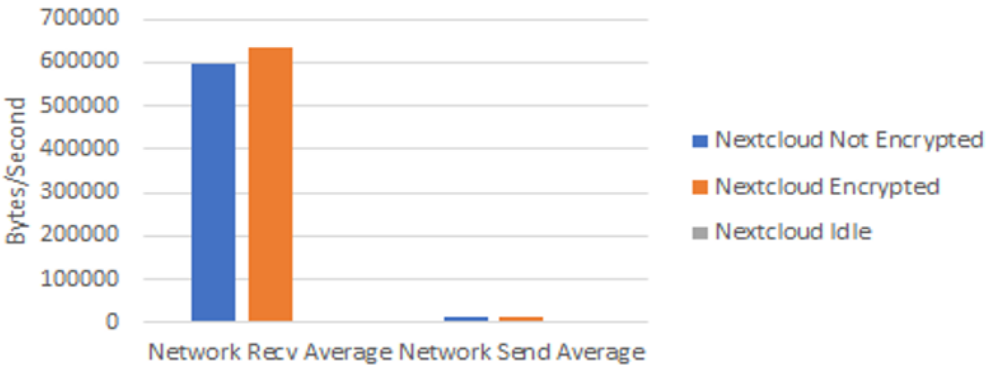

Figure 15. NextCloud 100 20 MB files network usage

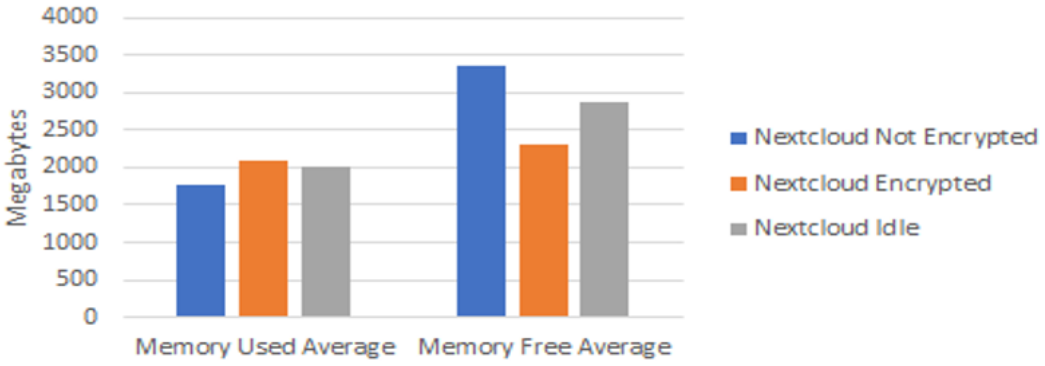

Figure 16. NextCloud 100 20 MB files memory usage

From Figure 14-16, we can see that the no encryption efficiency is slightly more than the encryption efficiency overall between CPU, network, and memory usage.

Finally, we have compared NextCloud 2, 1 GB encryption efficiency and 2, 1 GB no encryption efficiency in Figure 17-19.

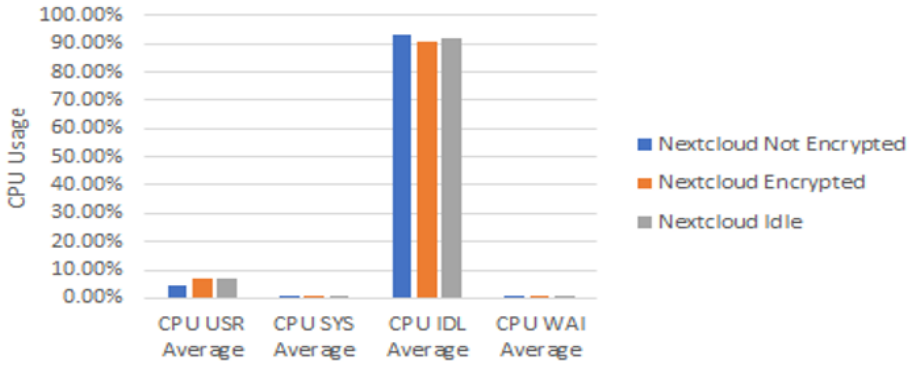

Figure 17. NextCloud 2 1 GB files CPU usage

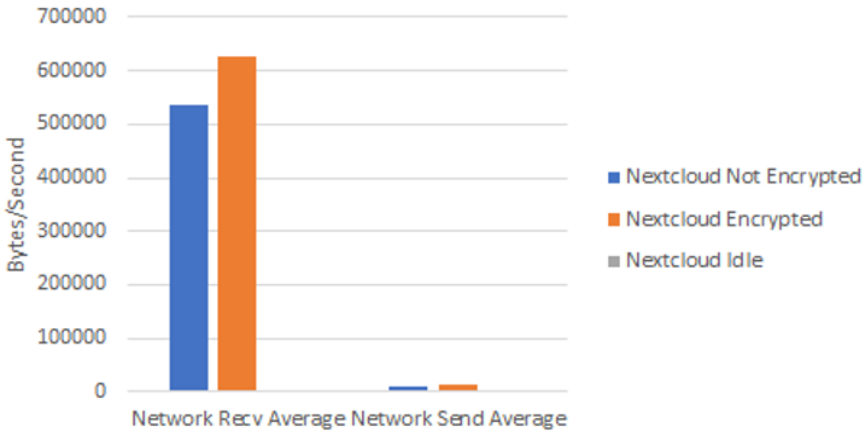

Figure 18. NextCloud 2 1 GB files network usage

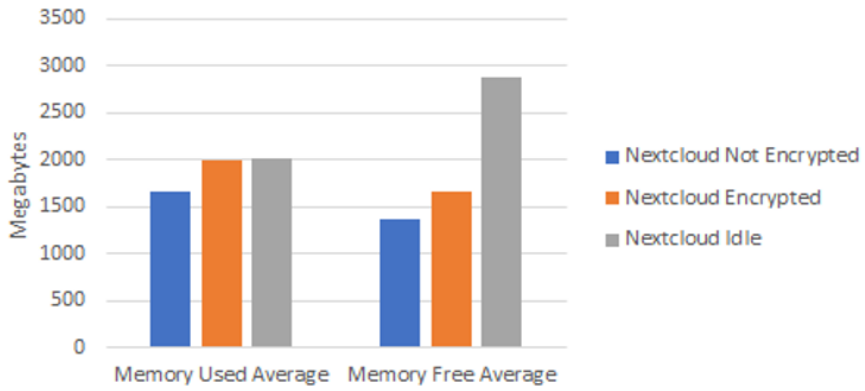

Figure 19. NextCloud 2 1 GB files memory usage

Overall, Figure 17-19 show that no encryption efficiency is slightly more than the encryption efficiency overall between CPU, network, and memory usage.

Conclusion

The efficiency and strength of encryption is constantly improving and for cloud storage, it is a necessity to have server-side encryption. Many big cloud storage providers such as Google Drive have many files being uploaded at once and if there was an inefficient encryption mechanism, it would overload the server. By doing these tests on encryption efficiency, we can help to see how well these server programs would perform in a bigger cloud storage environment with many users. Results that we got from this project were not what we expected, we thought that overall, the encryption efficiency would be less than the no encryption efficiency. However, some tests showed that encryption was more efficient than no encryption. The reason is probably because the encryption algorithm for both server programs is very lightweight and non-resource intensive. Overall, Seafile was much more efficient than NextCloud in this environment. While the original goal of this project was not to compare NextCloud and Seafile against each other, it became obvious through CPU usage that Seafile is much more efficient overall. From this research experiment, we can conclude that efficiency of the server-side encryption is similar to the efficiency of no server-side encryption. We also found that Seafile is higher in overall efficiency than NextCloud in the environment we did the experiment in. While the goal of this experiment wasn't to compare the two, it is an experiment that can be done in the future. In addition, this research can also be expanded in the future by running more test cases and running the experiment in a different environment (such as having different hardware components for the server). It could even be expanded to test more cloud storage server software.

References

[1] U. Warrier, Singh, P., Jien, C.W., Kee, D.M.H., Yi, G.Z., Jiann, T.W., Liang, T.Y., Sb, G., Nair, S., Nair, R.K., Lokhande, S.D., and Ganatra, V., Factors that Lead Amazon.com to A Successful Online Shopping Platform. *International Journal of Tourism and Hospitality in Asia Pasific*, **2021**. *4(1)*,7-17.DOI: 10.32535/ijthap.v4i1.1017.

[2] KamalaKannan, T., K.S., C. Shanthi, and Devi., R., Energy-Efficient Heterogeneous Multi-Processor Environment in Cloud using Modern Artificial BEE Colony. *International Journal of Engineering and Advanced Technology*, **2019**. *9(2)*,976-981.DOI: 10.35940/ijeat.b2835.129219.

[3] V. Yatskiv, Kulyna, S., Yatskiv, N., and Kulyna, H. *Protected Distributed Data Storage Based on Residue Number System and Cloud Services*. in *2020 10th International Conference on Advanced Computer Information Technologies (ACIT)*. **2020**. IEEE.

[4] I. Ihsan, Zulkarnain, Z., and Amsal, A.Y., Perancangan Dan Implementasi Cloud Storage Menggunakan NextCloud Pada Smk YPP Pandeglang. *Jurnal Pengembangan Riset dan Observasi Sistem Komputer*, **2019**. *6(2)*.

[5] N. Singh, Bui, K. and Mailewa, A. *Robust Efficiency Evaluation of NextCloud and GoogleCloud*. *Advances in Technology,* **2021**. 536-545

[6] S. Yang, Jiang, L., Zhu, S., and Dai, L. *Research and Application of Private Cloud Storage Platform in High Schools Based on Seafile*. in *2013 6th International Conference on Intelligent Networks and Intelligent Systems*. **2013**. IEEE.

[7] A.M. Dissanayaka, Mengel, S., Gittner, L., and Khan, H. *Dynamic & portable vulnerability assessment testbed with Linux containers to ensure the security of MongoDB in Singularity LXCs.* in *Companion Conference of the Supercomputing-2018 (SC18)*. **2018**.

[8] X. Lu, Pan, Z., and Xian, H., An integrity verification scheme of cloud storage for internet-of-things mobile terminal devices. *Computers & Security*, **2020**. *92*,101686.DOI: 10.1016/j.cose.2019.101686.

[9] Initials. Last Name of M. Oppitz and Tomsu, P.(s), Book Inventing the Cloud Century, Springer International Publishing Location, Springer International Publishing, 2018, pp. Page

[10] T. Coughlin, Digital Storage in Smartphones and Wearables [The Art of Storage]. *IEEE Consumer Electronics Magazine*, **2018**. *7(2)*,108-120.DOI: 10.1109/mce.2017.2773361.

[11] K. Karthiban and Smys, S. *Privacy preserving approaches in cloud computing*. in *2018 2nd International Conference on Inventive Systems and Control (ICISC)*. **2018**. IEEE.

[12] A.M. Dissanayaka, Mengel, S., Gittner, L., and Khan, H. *Vulnerability Prioritization, Root Cause Analysis, and Mitigation of Secure Data Analytic Framework Implemented with MongoDB on Singularity Linux Containers*. in *Proceedings of the 2020 4th International Conference on Compute and Data Analysis*. **2020**. ACM.

[13] H. Hammami, Yahia, S.B., and Obaidat, M.S., A lightweight anonymous authentication scheme for secure cloud computing services. *The Journal of Supercomputing*, **2020**. *77(2)*,1693-1713.DOI: 10.1007/s11227-020-03313-y.

[14] D. Milojicic, Faraboschi, P., Dube, N., and Roweth, D. *Future of HPC: Diversifying Heterogeneity*. in *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. **2021**. IEEE.

[15] S.S. Khan, and Mailewa, A.B., *Detecting network transmission anomalies using autoencoders-svm neural network on multi-class NSL-KDD Dataset*." **in** 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0835-0843. **2023**. IEEE.

[16] A. Rahman, Jin, J., Rahman, A., Cricenti, A., Afrin, M., and Dong, Y.-n., Energy-efficient optimal task offloading in cloud networked multi-robot systems. *Computer Networks*, **2019**. *160*,11-32.DOI: 10.1016/j.comnet.2019.05.016.

[17] M. Jebalia, Asma Ben Letaïfa, Mohamed Hamdi, and Tabbane., S. *A Fair Resource Allocation Approach in Cloud*

Computing Environments. in *2018 IEEE 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*. **2018**. IEEE.

[18] H. González Labrador, Mościcki, J.T., Lamanna, M., and Pace, A., Increasing interoperability for research clouds: CS3APIs for connecting sync&share storage, applications and science environments. *EPJ Web of Conferences*, **2020**. *245*,07041.DOI: 10.1051/epjconf/202024507041.

[19] J.B. Nurdin, and Mulyana, E., NextCeph: Nextcloud Platform Based Application for Ceph Cluster Management. **in** 2019 IEEE 13th International Conference on Telecommunication Systems, Services, and Applications (TSSA), pp. 25-30. **2019**. IEEE.

[20] Initials. Last Name of Y.-Y. Teing, Homayoun, S., Dehghantanha, A., Choo, K.-K.R., Parizi, R.M., Hammoudeh, M., and Epiphaniou, G.(s), Book Private Cloud Storage Forensics: Seafile as a Case Study, Springer International Publishing Location, Springer International Publishing, 2019, pp. Page

[21] M. Akintaro, Teddy Pare, and Dissanayaka, A.M. *Darknet and black market activities against the cybersecurity: a survey*. in *n The Midwest Instruction and Computing Symposium.(MICS), North Dakota State University, Fargo*. **2019**.

[22] J.A. Alzubi, Manikandan, R., Alzubi, O.A., Qiqieh, I., Rahim, R., Gupta, D., and Khanna, A., Hashed Needham Schroeder Industrial IoT based Cost Optimized Deep Secured data transmission in cloud. *Measurement*, **2020**. *150*,107077.DOI: 10.1016/j.measurement.2019.107077.

[23] S. Sahmim and Gharsellaoui, H., Privacy and Security in Internet-based Computing: Cloud Computing, Internet of Things, Cloud of Things: a review. *Procedia Computer Science*, **2017**. *112*,1516-1522.DOI: 10.1016/j.procs.2017.08.050.

[24] A. Mailewa and Herath., J. *Operating systems learning environment with VMware*. in *The Midwest Instruction and Computing Symposium. Retrieved from http://www. micsymposium. org/mics2014/ProceedingsMICS_2014/mics2014_submission_14. pdf.* . **2014.**

[25] Y. Wang, Arya, K., Kogias, M., Vanga, M., Bhandari, A., Yadwadkar, N.J., Sen, S., Elnikety, S., Kozyrakis, C., and Bianchini, R. *SmartHarvest*. in *Proceedings of the Sixteenth European Conference on Computer Systems*. **2021**. ACM.

[26] O.O. Olakanmi and Odeyemi, K.O., Faster and efficient cloud-server-aided data de-duplication scheme with an authenticated key agreement for Industrial Internet-of-Things. *Internet of Things*, **2021**. *14*,100376.DOI: 10.1016/j.iot.2021.100376.

[27] H. Mazi, Foka Ngniteyo Arsene, and Dissanayaka, A.M. *The influence of black market activities through dark web on the economy: a survey*. in *The Midwest Instruction and Computing Symposium.(MICS), Milwaukee School of Engineering and Northwestern Mutual, Milwaukee, Wisconsin*. **2020**.

[28] A.M. Dissanayaka, Susan Mengel, L.G., and Khan., H. *Dynamic & portable vulnerability assessment testbed with Linux containers to ensure the security of MongoDB in Singularity LXCs.* in *Companion Conference of the Supercomputing-2018 (SC18).* . **2018**.

[29] O. Olakanmi and Odeyemi, K., FEACS: A fog enhanced expressible access control scheme with secure services delegation among carers in E-health systems. *Internet of Things*, **2020**. *12*,100278.DOI: 10.1016/j.iot.2020.100278.

[30] R.R. Shetty, Akalanka Mailewa Dissanayaka, Susan Mengel, L.G., Ravi Vadapalli, and Khan., H. *Secure NoSQL based medical data processing and retrieval: the exposome project.* in *Companion Proceedings of the10th International Conference on Utility and Cloud Computing,* . **2017**. ACM.

[31] A. Mailewa Dissanayaka, Shetty, R.R., Kothari, S., Mengel, S., Gittner, L., and Vadapalli, R. *A review of MongoDB and singularity container security in regards to hipaa regulations*. in *Companion Proceedings of the10th International*

Conference on Utility and Cloud Computing. **2017**. ACM.

[32] A.A. Alli and Alam, M.M., SecOFF-FCIoT: Machine learning based secure offloading in Fog-Cloud of things for smart city applications. *Internet of Things*, **2019**. *7*,100070.DOI: 10.1016/j.iot.2019.100070.

[33] H. Mistareehi, Islam, T., and Manivannan, D., A secure and distributed architecture for vehicular cloud. *Internet of Things*, **2021**. *13*,100355.DOI: 10.1016/j.iot.2020.100355.

[34] D. Zhang, Le, J., Mu, N., Wu, J., and Liao, X., Secure and Efficient Data Deduplication in JointCloud Storage. *IEEE Transactions on Cloud Computing*, **2023**. *11(1)*,156-167.DOI: 10.1109/tcc.2021.3081702.

[35] A. Mailewa, Jayantha Herath, and Susantha Herath. *A survey of effective and efficient software testing*. in *The Midwest Instruction and Computing Symposium.(MICS), Grand Forks.* **2015**.