

Full Paper

Analyzing Data Encryption Efficiencies for Secure Cloud Storages: A Case Study of Pcloud vs OneDrive vs Dropbox

Steven Gamnis, Matthew VanderLinden, and Akalanka B. Mailewa*

Department of Computer Science & Information Technology, St. Cloud State University, St. Cloud, Minnesota, USA

E-mail Correspondence: amailewa@stcloudstate.edu (A. B. Mailewa)

Received: 31 January 2022; Revised: 26 April 2022; Accepted: 02 May 2022; Published: 7 May 2022

Abstract

Now more than ever has it become important to keep the information confidential in an age that is losing its value of individual privacy. In this cloud computing era, regardless of the power of the cloud computing concept, many people do not know that their information can be used and sent to third parties from their cloud storage provider. Today the use of cloud storage is well established however the security of protecting the data on the cloud is a limited thought for most users. Therefore, this study aims to experimentally research which encryption program works best when storing data onto three of the main cloud storage providers currently available on the market. This study will go over the hardware and network impact as well as the time to encrypt and decrypt the data. This study will determine if “7zip” or “rclone” encryption programs work best with these three cloud storage. The data will be collected using NetData tool and accordingly determine which encryption application works best with which cloud storage provider. Thereafter, based on the data analysis, it is recommended that experimental outcomes to all users to keep their sensitive data secured and safe from snooping or prevent private information from being collected and sold to third parties with the help of black market.

Keywords: Cloud Computing, Data Encryption, Pcloud, OneDrive, Dropbox, Security, and Privacy

Introduction

In today's world of technology, there has been immense improvement in the mobile technologies like smartphones, tablets and owing to their popularity due to their affordability and convenience in usage and the wide range of applications that they offer to accomplish huge tasks in a simpler way. However, these devices which are based on mobile technology, although provide effortless benefits, have few constraints in terms of storage space, power source and processing speed, and power [1]. In order to overcome these constraints, the Cloud technology has been developed which allows the users to access their data on various devices on various applications from anywhere in the world with the help of the internet. The mobile cloud computing is built on three essential components such as the mobile device which acts as a medium to use the cloud technology, the wireless communication channel for providing the mobility, and the cloud technology which is responsible for accessing data from anywhere in the world [2][3][4]. The cloud storage cannot use the data as plaintext as the data will be needed to be transferred over a network and if it is transferred as plaintext, it gives rise to security issues. Hence, Cloud technology has an approach of employing multiple third-party servers for the data storage instead of using a single dedicated server as used in traditional data storage networks [3][4][5]. In this, the location of data storage is not known to the

data owner or the actual data user and it is only the concern of the cloud storage provider, and the provider alone can secure the data which is not completely trusted by the users. Hence, in order to gain trust and provide much-enhanced security to the mobile cloud computing technology to overcome these drawbacks, the data must be encrypted even before storing the data in the cloud [6][7][8]. For the above-mentioned reasons, it is certain that there is a dire need for a mechanism to promote Data security in cloud computing. Therefore, encrypted storage for sensitive data is a must [9]. Today, more and more cloud service providers are entering the market and they advertise scalability and affordability but miss another key component, upload speeds and CPU demand [10][11]. This may not seem as important, but time is money; especially for corporations dealing with terabits of data as upload speeds can take days, time that could be spent analyzing and reporting trends or completing collaborative works and it is very obvious how easy it is to fill up gigabytes of storage [12][13]. This is even an issue that extends to everyday users with videos and photos filling up storage rapidly. All this data can be considered sensitive as well and that is why encryption services are becoming more popular [14]. Therefore, this experimental research project examines three popular service providers: 1. Pcloud [15], 2. OneDrive [16], and 3. Dropbox [17] with encryption software to determine what pairing will give users the fastest upload speed and least CPU usage.

Cloud computing has an enormous influence on all aspects of our lives and businesses. Various scholars have explored different architectures and implementations in relation to other frameworks, as well as how different software design approaches can be applied in cloud technology. As a result, the key issue in preserving our data protection is cloud storage reliability [18][19][20]. We look at security issues for cloud computing applications that are just getting started. Since Cloud Computing refers to both applications that provide services over the Internet and infrastructures (i.e., hardware and network software in data centers) that provide these services, additional security concerns, like variability, confidentiality, honesty protection, authorization, and so on, should be addressed [21]. In addition, the cloud computing is based on utility which provides infrastructure services on demand. All a cloud provider's tools, including infrastructure, network, software, and customer data, must be safe. That cloud service providers use a proper algorithm to encrypt data in the cloud [22].

Cloud Storage Services, Tools, and Experiments

The following sections go over the overview of the selective services of this study as well as the setup required to implement the testing environment.

Pcloud

Pcloud is a personal favorite for storing personal and other files. It has a user-friendly interface that clearly shows where all files are located. Being a free service for the first 10 GB is an attractive feature but by far the most attractive feature is the creation of a virtual drive. This drive works just like the C: or any USB drive, where it is manageable from the file explorer. As the Pcloud is available on Windows, Linux, and Mac, the user will be able to access the data in any environment. Pcloud Drive provides a number of additional functionalities, such as integrated file sharing and synchronization through the computer. [23]. The setup for Pcloud is simple and is like how Dropbox and OneDrive are setup. Once the installation is complete then want to sign into the newly created account or an account that may already have. Once signed into the account the user will be linked to the Pcloud storage and will have completed to the setup process for Pcloud. To use Pcloud the user will navigate to the Pcloud folder that was created in the

installation process and then simply add files to the folder to have it synced to the account which can be accessed from any device that the user sign in to with his/her Pcloud account.

OneDrive

Microsoft's OneDrive is very popular cloud storage. 1TB of space is included with a subscription or 5GB for a free plan. OneDrive does what all the other cloud storage services do — it gives a place to put the files on the Internet. To access it, the user needs to log in to OneDrive with his/her Microsoft account (or, equivalently, log in to Windows with the Microsoft account) to access the user's data. If the user logs into a different Windows 10 computer using the same Microsoft account, the user has access to all user's OneDrive data through the web but, surprisingly, not necessarily through File Explorer. In fact, if the user looks only at Windows File Explorer, he/she might not even know what data is sitting in the OneDrive storage [24]. OneDrive works well with Microsoft files, automatically saving and recovering files from any device. OneDrive is quickly becoming one of the top personal cloud storage providers.

The setup for OneDrive, First, go to the OneDrive website and then will create an account with a valid email. Once an account is created, next the user will then proceed to download and install the OneDrive. Once installation is complete the user will then have to sign into the newly created account or an account that may already have. Once signed in the user will be linked to the OneDrive storage and will have completed the setup process for OneDrive. To use OneDrive, the user will navigate to the OneDrive folder that was created in the installation process and then simply add files to the folder to have it synced to the account which can be accessed from any device that the user signs into with his/her OneDrive account.

Dropbox

Probably the most well-known cloud storage provider as it has been around the longest is Dropbox. Dropbox is a home for all the most valuable files of a particular user. To keep the files safe, Dropbox is designed with multiple layers of protection, distributed across a scalable, secure infrastructure [25]. Dropbox has good security to keep the information safe. However, it is always a good idea to encrypt the files since nobody knows if someone can get the user's login credentials. Also, no one should ever trust anyone with a user's information including Dropbox which is why it is important to add extra steps to add more security for the user with some other security mechanisms. The seamless interface on both mobile and laptop is superb; other than that, its name is pulling the weight. Controversy has plagued this titan for years. This is a lack of storage for free subscriptions and only 2GB is the maximum limit to test large volumes of data.

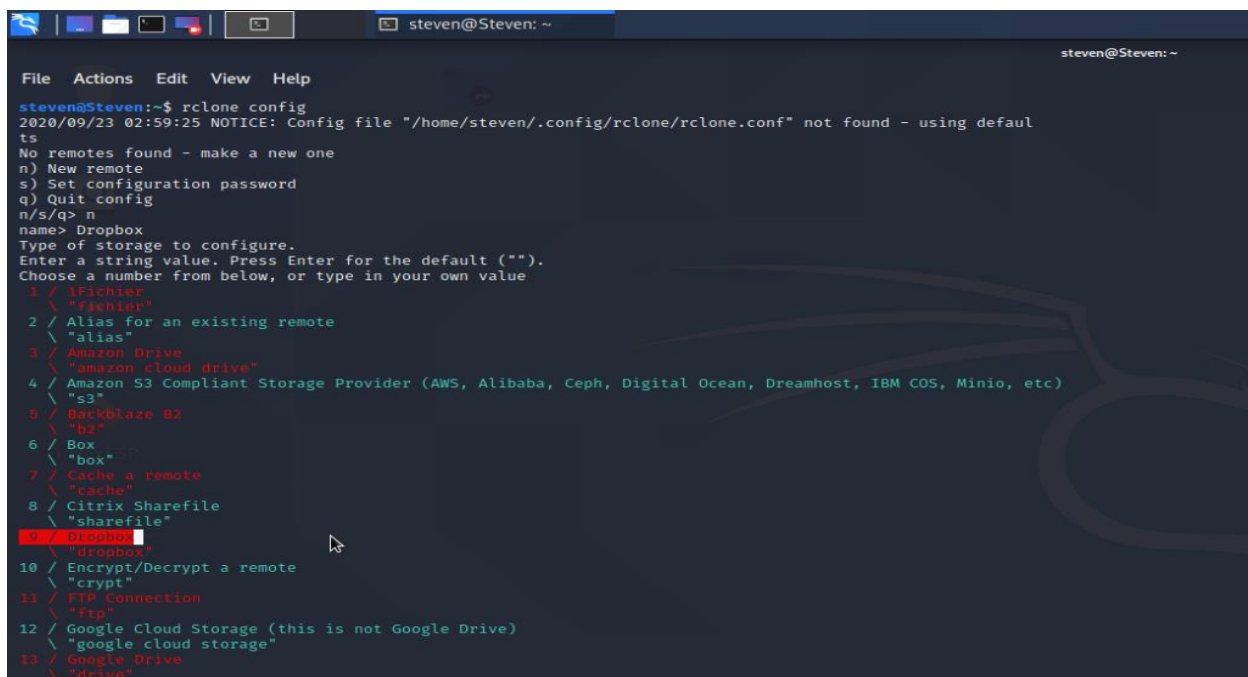
For setup Dropbox, first, go to the Dropbox website and hereafter will create an account with a valid email. Once an account is created then proceed to download and install. After the installation is completed sign into the user's newly created account or an account that may already have. Once signed in the user will be linked to the OneDrive storage and will have completed the setup process for Dropbox. To use Dropbox, make sure to navigate to the Dropbox folder that was created in the installation process and then simply add files to the folder to have it synced to the account which can be accessed from any device that the user signs into with his/her Dropbox account.

Encryption with Rclone

Initial setup

After creating and setting up all three of the test cloud storage services, then want to begin to setup the encryption programs to encrypt the data safely to the cloud. The first encryption program used in this study is rclone and it is a command-line program to manage files on cloud storage. It is a feature-rich

alternative to cloud vendors' web storage interfaces. Over 40 cloud storage products support rclone including S3 object stores, business & consumer file storage services, as well as standard transfer protocols [26]. Rclone has an encryption option that allows for encryption with EME using AES with 256 bit key [27][28]. AES 256 is virtually impenetrable using brute-force methods. While a 56-bit DES key can be cracked in less than a day, AES would take billions of years to break using current computing technology. Hackers would be foolish to even attempt this type of attack [29][30]. This gives the files powerful encryption that will keep the online data safe. This means that even if someone was able to gain access to the cloud data the attacker would not be able to access the data due to it all being encrypted. This powerful tool allows for high customization and has many other features not covered in this report. Because of the high potential for this software to be used in multiple environments to meet the needs of most cloud users in this study to use rclone as one of the encryption tools. The steps for setup will be show setup for DropBox however process for the other cloud storage is a similar setup so will not be repeated for each individual cloud storage in the report so use DropBox setup as a reference when doing the setup for OneDrive and Pcloud. The setup first begins with opening the terminal. Type 'sudo apt-get install rclone'. After the installation, the user will need to create buckets for all three cloud services and another 3 buckets for the encryption of each cloud service. The next steps will create a bucket in Rclone for Dropbox. In the first step type "rclone config" then click "n" for the new remote and then name the bucket "Dropbox" (Figure 1). A list will show a variety of options with each number having a different option. For the setup, select "9" and then select "n" for Edit advanced config. Next select "y" to use auto-config. The web browser will open and ask to sign in to the specific Dropbox account (Figure 1). After successful login to Dropbox the user will get a successful user screen (Figure 2). The last step of this part is it will grab the code and then ask if the setup is ok and respond "y" for "Yes this is OK". After that the Dropbox setup in rclone, press "q" for quit config because the setup has finished. For this section make sure the setup follows similarly to figures (1)-(3) and use these figures for reference if stuck on an aforementioned step.



```

steven@Steven:~$ rclone config
2020/09/23 02:59:25 NOTICE: Config file "/home/steven/.config/rclone/rclone.conf" not found - using default
ts
No remotes found - make a new one
n) New remote
s) Set configuration password
q) Quit config
n/s/q> n
name> Dropbox
Type of storage to configure.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value
 1 / rFichier
   \ "rFichier"
 2 / Alias for an existing remote
   \ "alias"
 3 / Amazon Drive
   \ "amazon cloud drive"
 4 / Amazon S3 Compliant Storage Provider (AWS, Alibaba, Ceph, Digital Ocean, Dreamhost, IBM COS, Minio, etc)
   \ "s3"
 5 / Backblaze B2
   \ "b2"
 6 / Box
   \ "box"
 7 / Cache a remote
   \ "cache"
 8 / Citrix Sharefile
   \ "sharefile"
 9 / Dropbox
   \ "dropbox"
10 / Encrypt/Decrypt a remote
   \ "crypt"
11 / FTP Connection
   \ "ftp"
12 / Google Cloud Storage (this is not Google Drive)
   \ "google cloud storage"
13 / Google Drive
   \ "drive"

```

Figure 1. DropBox Setup_Stage-01

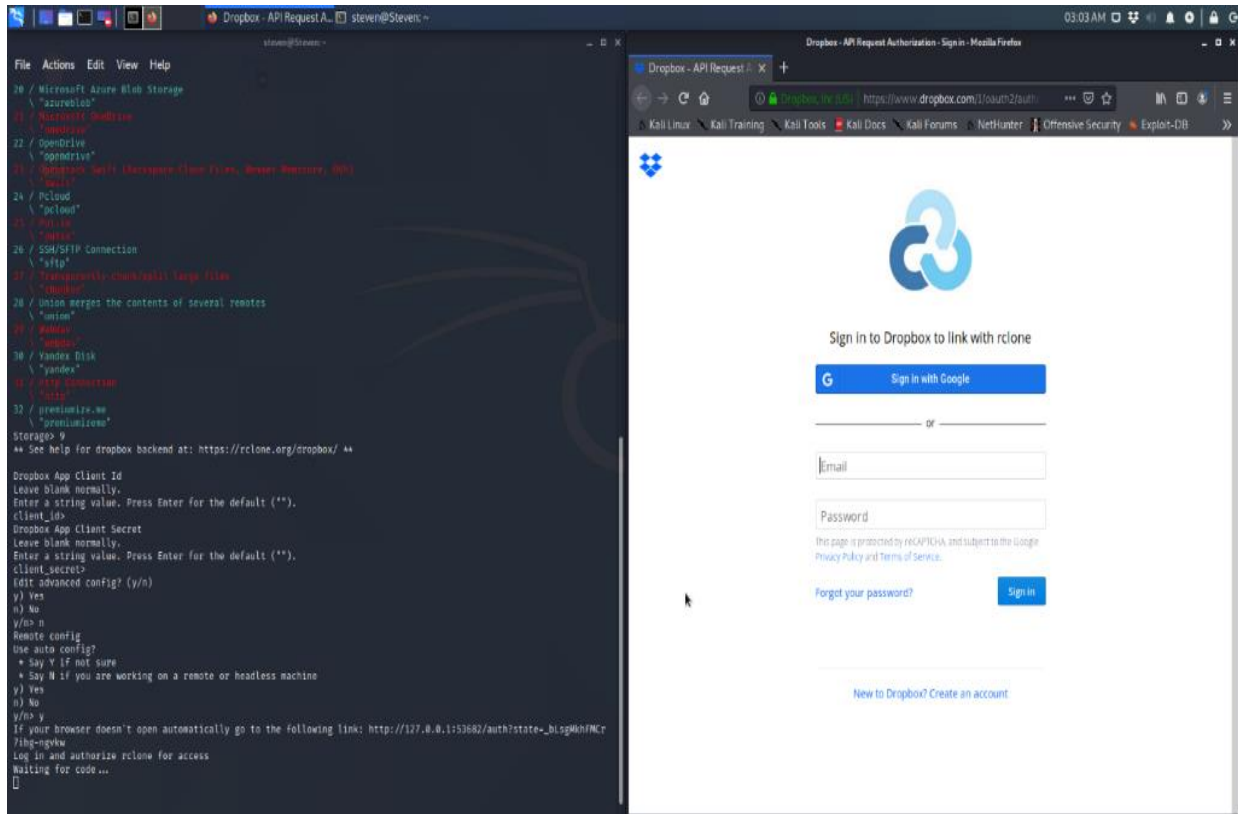


Figure 2. DropBox Setup_Stage-02

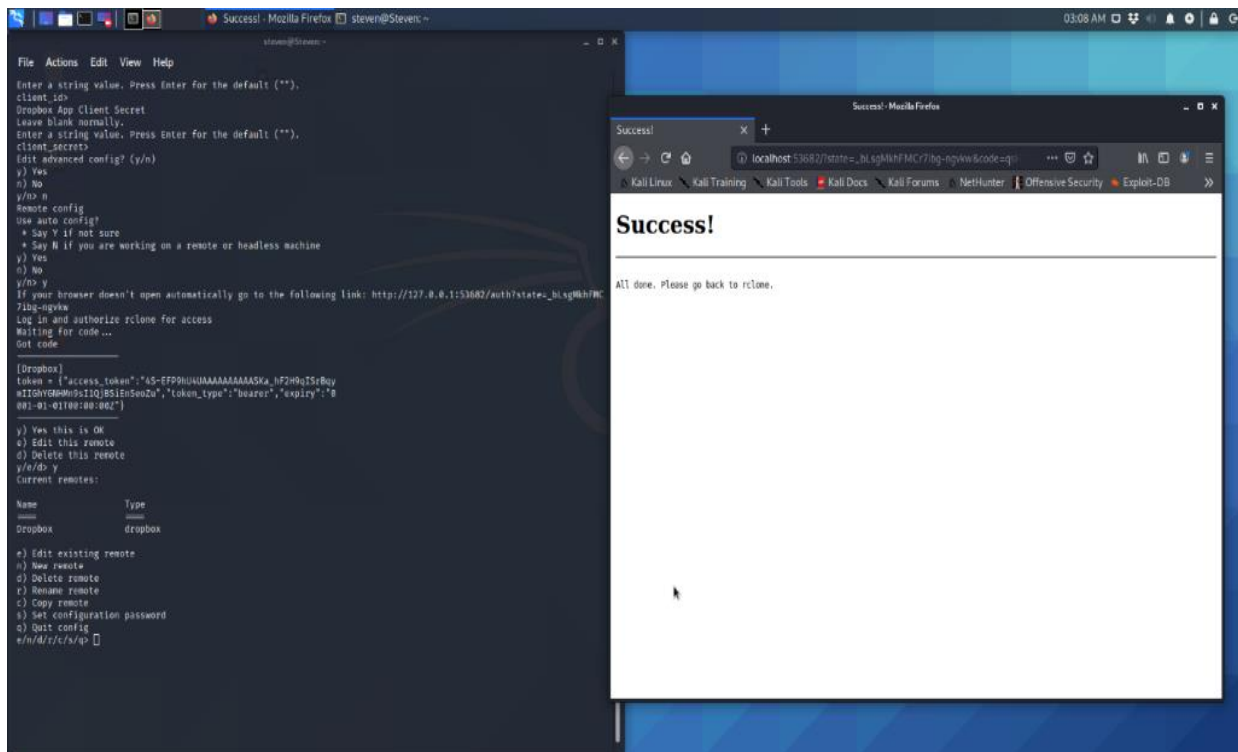
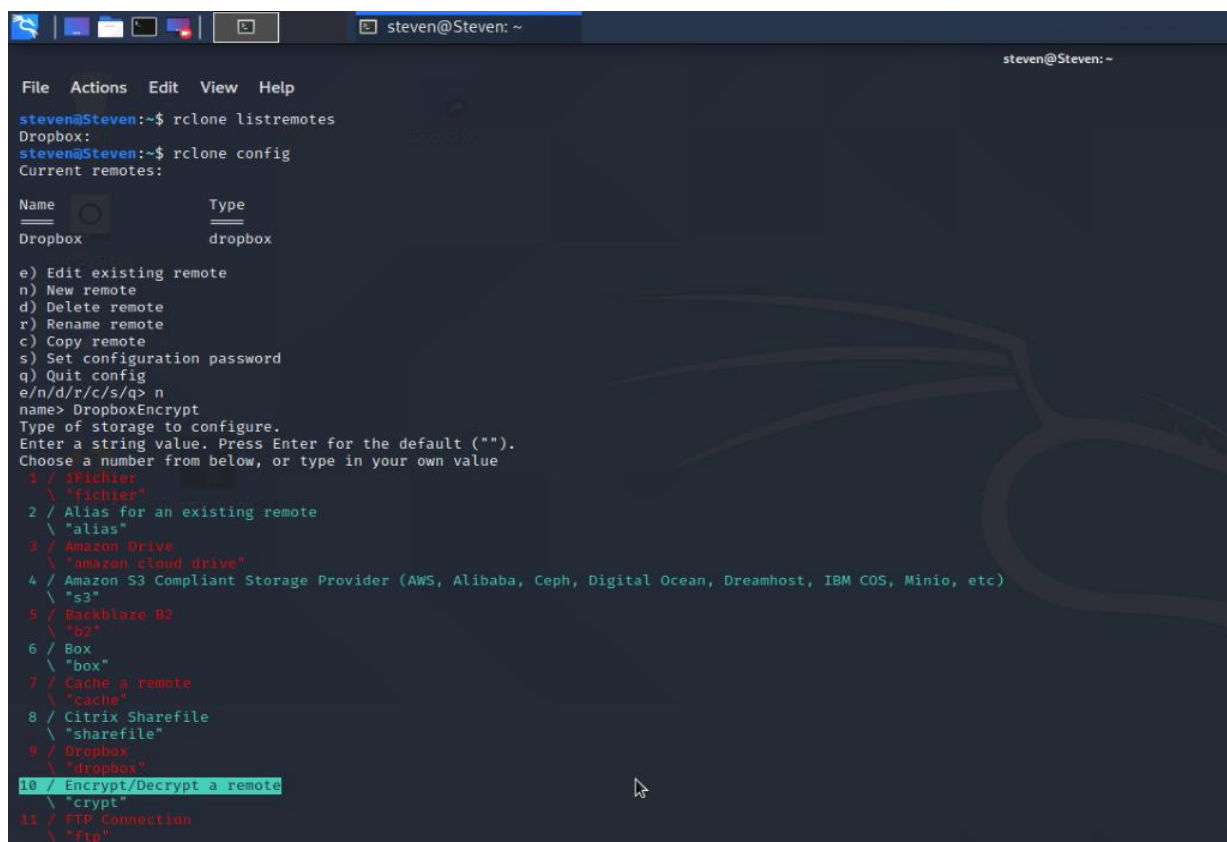


Figure 3. DropBox Setup_Stage-03

Encryption Setup

The next section will setup the encryption setting for Dropbox. When following these steps please follow the steps carefully and follow Figures 4 -6 for more information. A mistake made in the next few steps could result in loss of data and require to start over. Type "rclone listremotes" and should be able to see the Dropbox and the Dropbox setup is successful. To create the encryption setup, first, start with typing "rclone config". Then select "n" for the new remote (Figure 4). A list of numbers with different options will appear. To make the encryption setup select "10" and then the system prompt to enter a name and it should contain ":" and name it "Dropbox:Test". Then a list of 3 options will appear for how to encrypt file names and click "enter" in this example however if choose to change these settings then select the number that requires. The next two options will appear to either encrypt directory names or leave them intact. For the setup choose, not to encrypt directory names in order to keep organization easier when syncing large amounts of files, select "2" (Figure 4). Now generate 2 sets of passwords. Then enter "g" to generate a random password. Then set the key size to 64 bits to keep it secure. Even though having a larger bit password will be more secure but keep in mind that the password will be longer and more complex and might not be practical for most uses. Therefore, this study chose 64 bits to keep simple but still secure. Next, click "y" when asked to keep a password and press "y" to generate another password (Figure 5). For the second password press "g" for generating a random password and select 64 bits. Then enter "y" for yes to keep the password. After finishing this will get a list showing the setting for out Dropbox:Encrypt and the output should be similar to the one seen in Figure 6. Click "y" for yes this is OK to complete this entire setup and have the encryption bucket ready for the encryption sync.



```

steven@Steven: ~
File Actions Edit View Help
steven@Steven:~$ rclone listremotes
Dropbox:
steven@Steven:~$ rclone config
Current remotes:

Name           Type
-----
Dropbox        dropbox

e) Edit existing remote
n) New remote
d) Delete remote
r) Rename remote
c) Copy remote
s) Set configuration password
q) Quit config
e/n/d/r/c/s/q> n
name> DropboxEncrypt
Type of storage to configure.
Enter a string value. Press Enter for the default ("").
Choose a number from below, or type in your own value
 1 / 1Fichier
   \ "fichier"
 2 / Alias for an existing remote
   \ "alias"
 3 / Amazon Drive
   \ "amazon cloud drive"
 4 / Amazon S3 Compliant Storage Provider (AWS, Alibaba, Ceph, Digital Ocean, Dreamhost, IBM COS, Minio, etc)
   \ "s3"
 5 / Backblaze B2
   \ "b2"
 6 / Box
   \ "box"
 7 / Cache a remote
   \ "cache"
 8 / Citrix Sharefile
   \ "sharefile"
 9 / Dropbox
   \ "dropbox"
10 / Encrypt/Decrypt a remote
   \ "crypt"
11 / FTP Connection
   \ "ftp"

```

Figure 4. Encryption setting for Dropbox_Stage-01


```

File Actions Edit View Help
\ < "http"
32 < premiumize.me
   < "premiumizeme"
Storage> 10
** See help for crypt backend at: https://rclone.org/crypt/ **

Remote to encrypt/decrypt.
Normally should contain a ':' and a path, eg "myremote:path/to/dir",
"myremote:bucket" or maybe "myremote:" (not recommended).
Enter a string value. Press Enter for the default ("").
remote> Dropbox:Test
How to encrypt the filenames.
Enter a string value. Press Enter for the default ("standard").
Choose a number from below, or type in your own value
 1 < Don't encrypt the file names. Adds a ".bin" extension only.
   < "off"
 2 < Encrypt the filenames see the docs for the details.
   < "standard"
 3 < Very simple filename obfuscation.
   < "obfuscate"
filename_encryption>
Option to either encrypt directory names or leave them intact.
Enter a boolean value (true or false). Press Enter for the default ("true").
Choose a number from below, or type in your own value
 1 < Encrypt directory names.
   < "true"
 2 < Don't encrypt directory names, leave them intact.
   < "false"
directory_name_encryption> 2
Password or pass phrase for encryption.
y) Yes type in my own password
g) Generate random password
n) No leave this optional password blank
y/g/n> g
Password strength in bits.
64 is just about memorable
128 is secure
1024 is the maximum
Bits> 64
Your password is: *****IV9o
Use this password? Please note that an obscured version of this
password (and not the password itself) will be stored under your
configuration file, so keep this generated password in a safe place.
y) Yes
n) No
y/n> y
Password or pass phrase for salt. Optional but recommended.
Should be different to the previous password.
y) Yes type in my own password
g) Generate random password
n) No leave this optional password blank
y/g/n> g

```

Figure 5. Encryption setting for Dropbox_Stage-02

```

File Actions Edit View Help
y/n> y
Password or pass phrase for salt. Optional but recommended.
Should be different to the previous password.
y) Yes type in my own password
g) Generate random password
n) No leave this optional password blank
y/g/n> g
Password strength in bits.
64 is just about memorable
128 is secure
1024 is the maximum
Bits> 64
Your password is: *****bgM
Use this password? Please note that an obscured version of this
password (and not the password itself) will be stored under your
configuration file, so keep this generated password in a safe place.
y) Yes
n) No
y/n> y
Remote config

[DropboxEncrypt]
remote = Dropbox:Test
directory_name_encryption = false
password = *** ENCRYPTED ***
password2 = *** ENCRYPTED ***

y) Yes this is OK
e) Edit this remote
d) Delete this remote
y/e/d> y
Current remotes:

Name                Type
-----                -
Dropbox              dropbox
DropboxEncrypt       crypt

e) Edit existing remote
n) New remote
d) Delete remote
r) Rename remote
c) Copy remote
s) Set configuration password
q) Quit config
e/n/d/r/c/s/q> q

```

Figure 6. Encryption setting for Dropbox_Stage-03

After the setup is complete, it will be able to execute the encryption process. For the implementation place the test file in the root directory under 'Test' file. To execute the execution and have it sync to the cloud storage it is required to follow the command, 'rclone sync ~/Test/ DropBoxEncrypt:'. Use the commandline interface, rclone to sync the 'Test' file for encrypting into the Dropbox in this specific case. This is the long process of the setup for rclone and is considered to be the largest negative aspect of this program because of the long configuration process. However, once all setup the execution of the program is a simple one-line code into the terminal making the process once all setup extremely easy to use.

P7zip

"p7zip" is a file archiver that handles the 7z format which features very high compression ratios. This p7zip has a command-line interface similar to rclone, which is mostly used on the Linux OS but some versions are available for Windows. Installation is faster as the software is smaller in size. The encryption it uses is the secure slated SHA256 with EME format. As this is the default encryption and the one this study uses with p7zip. With the newest hardware (CPU and GPU) improvements, it is become possible to decrypt SHA256 algorithm back. So, it is no longer recommended to use it for password protection or other similar use cases [31]. SHA256 is well known for its security and is even used in Bitcoin hashing. To install p7zip simply type into the terminal 'sudo apt-get install p7zip-full'. Right-click on a file and click on create an archive and make sure it is a .7z and make sure to click on more options and create a password to encrypt the compressed file as seen in Figure 7.

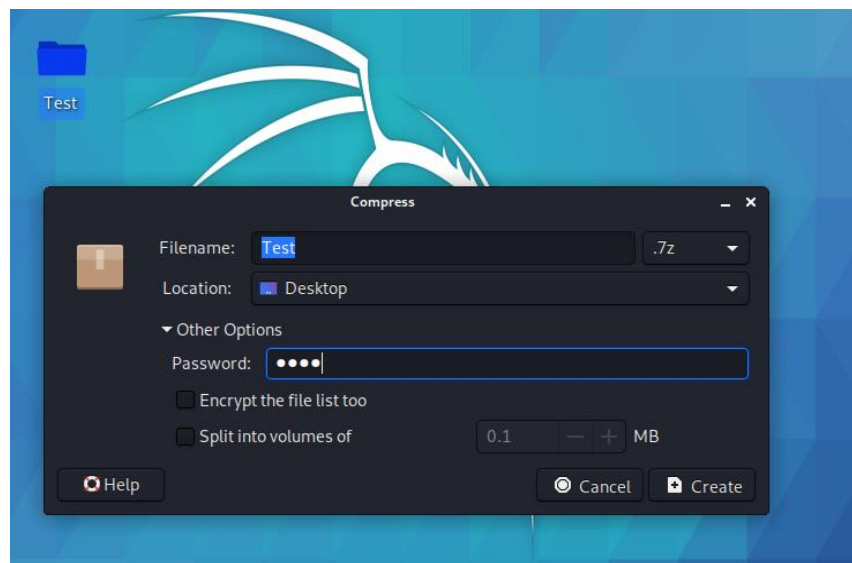


Figure 7. P7zip Setup

Methodology

In the implementation of the test environment, it is required to use the Linux operating system. This study uses Kali Linux as a Virtual Machine to implement all experiments. To make sure data is consistent it is created a file the size of 100Mb can be used when encrypting and decrypting throughout all the test cases. To solve the main problem, it is essential to look at the two most popular cloud storage services and this research also plan to look at one less common cloud storage service "Pcloud". To conclude the outcome of the experimental results this research has created and used the following formula to determine the best outcome of each scenario.

$$T = E + C + N + t$$

- T = Total ranking points
- E = Encryption
- C = CPU usage
- N = Network usage
- t = Time to complete each operation entirely (Format HH:MM:SS)

To determine the points for each factor it is created a number ranking. For Time any results above a 2:20:00 = 0 points. Next any time between 2:00:00 – 2:20:00 = 1 point. Finally, any time under 2:00:00 = 2 points. For CPU usage this research assigned values such that if the percentage is below 33% = 2 points, between 33%-66% = 1 point, and anything above 66% = 0 points. Network usage is determined by adding the total sent data and received data to assign the points. The total sent and received below 100 = 1 point and anything above 100 = 0 points. For encryption, it is assigned AES 256 bit key a 2-point value because it is the stronger of the given two encryptions. In addition for SHA 256 a total of 1 since its encryption will still stop most low-level attacks.

Results

This section discusses initially, after executing all the experiments as indicated in the figures from 8 to 23 in sections 4.1 through 4.3 the authors obtained the following results for total execution time (t), CPU usage (C), Network usage (N), and Encryption Strength (E) as shown in Table 1. Thereafter, based on the actual experimental data, Table 2 shows the calculated rankings for each cloud technology with “rclone” and “7zip”, according to the pre-defined formula “T = E + C + N + t”. Next, section 4.1 shows the Dropbox experimental results for both CPU and Network usages with “rclone” and “p7zip”. Thereafter, section 4.2 demonstrates Pcloud experimental results for both CPU and Network usages with “rclone” and “p7zip”. Finally, section 4.3 presents OneDrive experimental results for both CPU and Network usages with “rclone” and “p7zip” .

Table 1. Actual Experimental Data

	Time (t) (HH:MM:SS)	CPU usage (C) (max percentage use)	Network usage (N) (megabits/s) (max sent) / (max received)	Encryption Strength (E)
Dropbox-rclone	2:22.56	34.5	22.2sent / 38.7received	AES with 256 bit key
Dropbox-p7zip	2:11.16	55.2	18.9sent / 775.7received	SHA256
Pcloud-rclone	2:26.27	13.8	22.6sent / 35.6received	AES with 256 bit key
Pcloud-p7zip	1:52.62	62.0	19.1sent / 789.1 received	SHA256
OneDrive-rclone	2:06.60	52.8	24.0sent / 36.6 received	AES with 256 bit key
OneDrive-p7zip	1:53.09	74.5	23.1sent / 35.7 received	SHA256

Table 2. Calculated Ranking with formula $T = E + C + N + t$

	Time (t)	CPU usage (C)	Network usage (N)	Encryption Strength (E)	Total Points (T)
Dropbox-rc1one	0	1	1	2	4
Dropbox-p7zip	1	1	0	1	3
Pcloud-rc1one	0	2	1	2	5
Pcloud-p7zip	2	1	0	1	4
OneDrive-rc1one	1	1	1	2	5
OneDrive-p7zip	1	0	1	1	4

Dropbox Results

This section shows the Dropbox experimental results for both CPU and Network usages with “rc1one” and “p7zip”. The following Figure 8 shows the maximum CPU usage of Dropbox with rc1one is 34.5 as a percentage while 100Mb data file is used when encrypting and decrypting throughout the test case, in the real experimental environment.

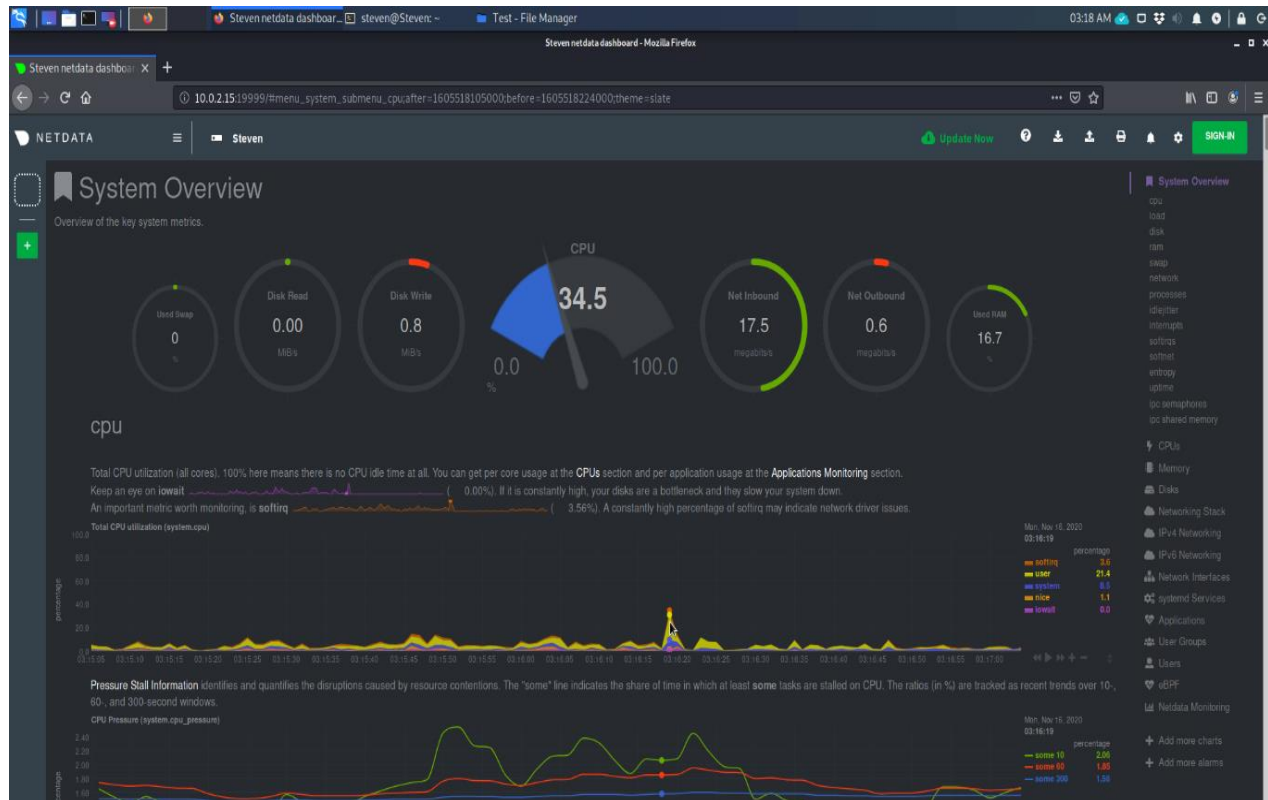


Figure 8. Dropbox rc1one CPU usage

In the real experimental environment, Figure 9 shows the maximum network usage of Dropbox with rc1one when sending data as 22.2 (megabits/s) while 100Mb data file is used when encrypting and decrypting throughout the test case.



Figure 9. Dropbox rclone network usage when sending data

In the real experimental environment, Figure 10 shows the maximum network usage of Dropbox with rclone when receiving data as 38.7 (megabits/s) while 100Mb data file is used when encrypting and decrypting throughout the test case.



Figure 10. Dropbox rclone network usage when receiving data

The following Figure 11 shows the maximum CPU usage of Dropbox with p7zip is 55.2 as a percentage while 100Mb data file is used when encrypting and decrypting throughout the test case, in the real experimental environment.

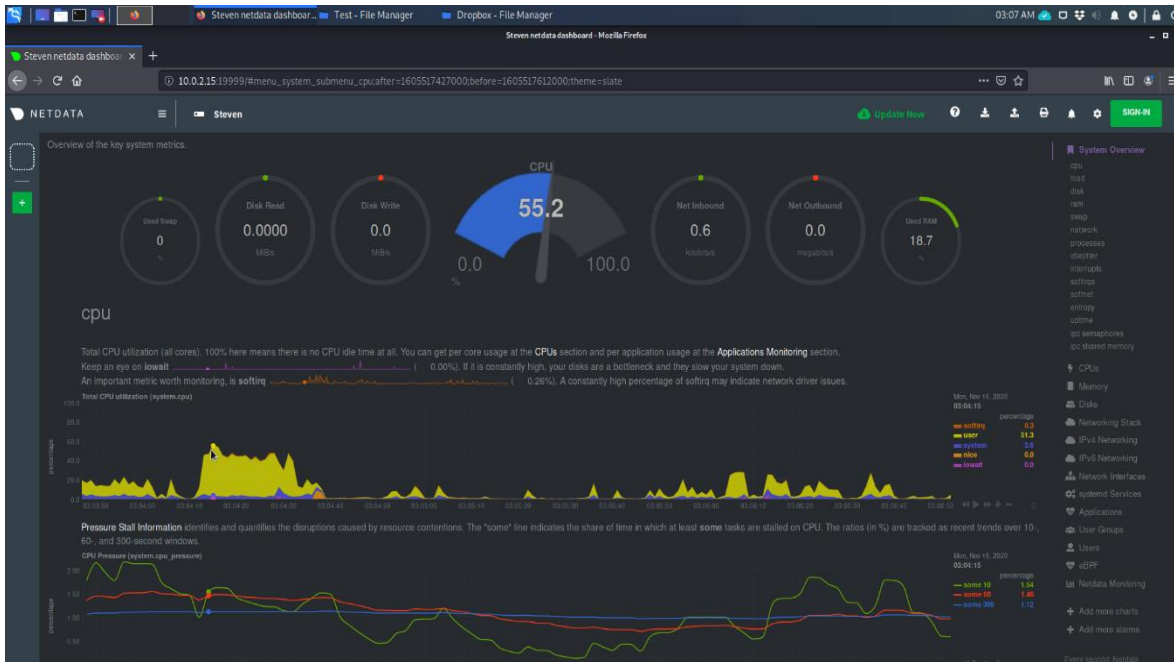


Figure 11. Dropbox p7zip CPU usage

In the real experimental environment, Figure 12 shows the maximum network usage of Dropbox with p7zip when sending data as 18.9 (megabits/s) as shown in red color and when receiving data as 775.7 (megabits/s) as shown in green color while 100Mb data file is used when encrypting and decrypting throughout the test case.

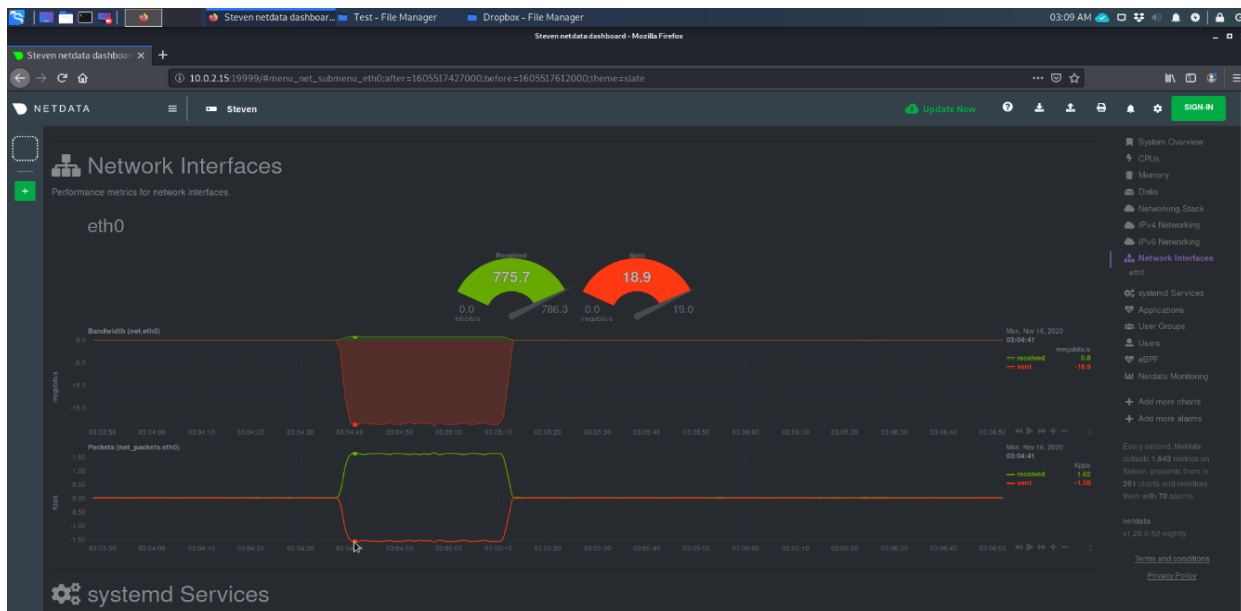


Figure 12. Dropbox p7zip network usage when sending and receiving data

Pcloud Results

This section demonstrates Pcloud experimental results for both CPU and Network usages with “rclone” and “p7zip”. The following Figure 13 shows the maximum CPU usage of Pcloud with rclone is 13.8 as a percentage while 100Mb data file is used when encrypting and decrypting throughout the test case, in the real experimental environment.

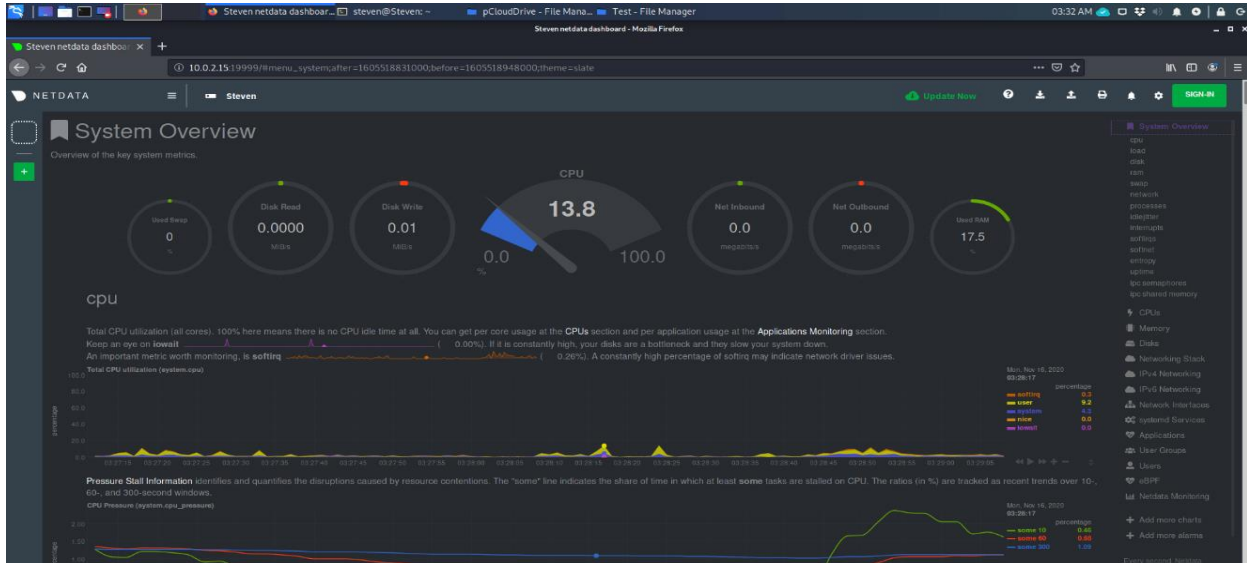


Figure 13. Pcloud rclone CPU usage

In the real experimental environment, Figure 14 shows the maximum network usage of Pcloud with rclone when sending data as 22.6 (megabits/s) while 100Mb data file is used when encrypting and decrypting throughout the test case.



Figure 14. Pcloud rclone network usage when sending data

In the real experimental environment, Figure 15 shows the maximum network usage of Dropbox with rclone when receiving data as 35.6 (megabits/s) while 100Mb data file is used when encrypting and decrypting throughout the test case.



Figure 15. Pcloud rclone network usage when receiving data

The following Figure 16 shows the maximum CPU usage of Pcloud with p7zip is 62.0 as a percentage while 100Mb data file is used when encrypting and decrypting throughout the test case, in the real experimental environment.

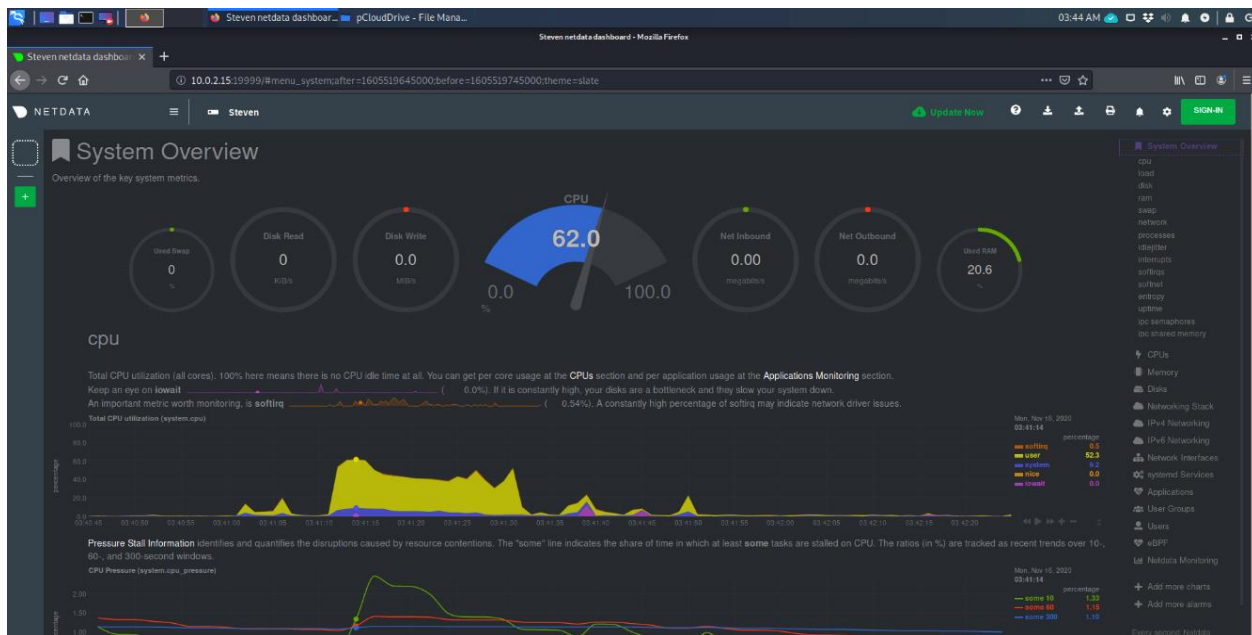


Figure 16. Pcloud p7zip CPU usage

In the real experimental environment, Figure 17 shows the maximum network usage of Pcloud with p7zip when sending data as 19.1 (megabits/s) as shown in red color and when receiving data as 789.1 (megabits/s) as shown in green color while 100Mb data file is used when encrypting and decrypting throughout the test case.

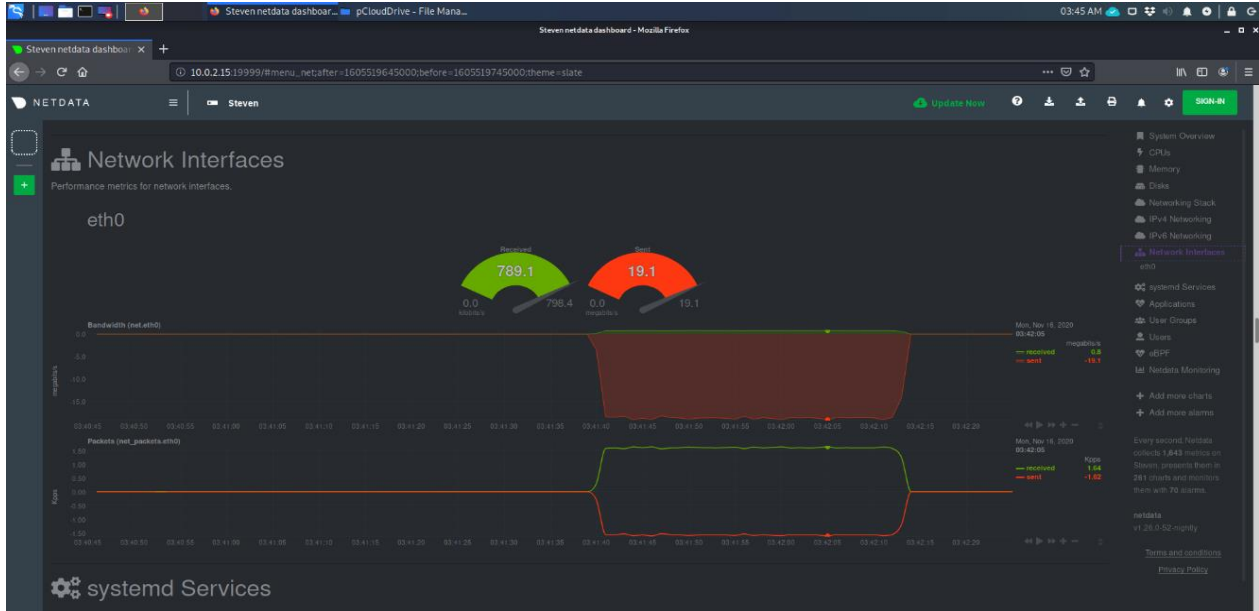


Figure 17. Pcloud p7zip network usage when sending and receiving data

OneDrive Results

This section demonstrates OneDrive experimental results for both CPU and Network usages with “rclone” and “p7zip”. The following Figure 18 shows the maximum CPU usage of OneDrive with rclone is 52.8 as a percentage while 100Mb data file is used when encrypting and decrypting throughout the test case, in the real experimental environment.

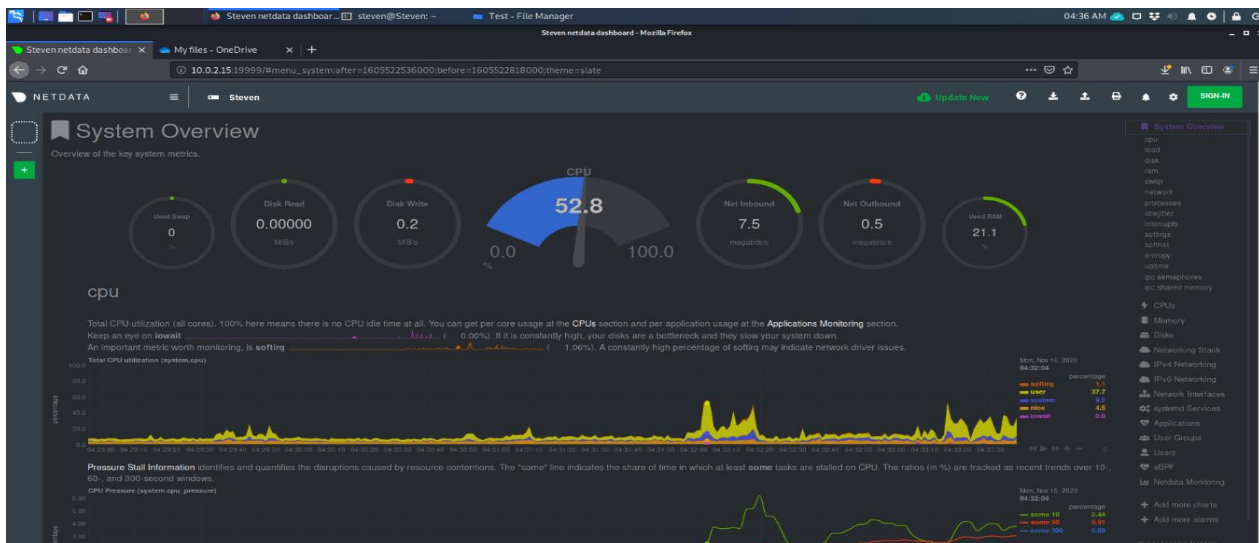


Figure 18. OneDrive rclone CPU usage

In the real experimental environment, Figure 19 shows the maximum network usage of OneDrive with rclone when sending data as 24.0 (megabits/s) while 100Mb data file is used when encrypting and decrypting throughout the test case.

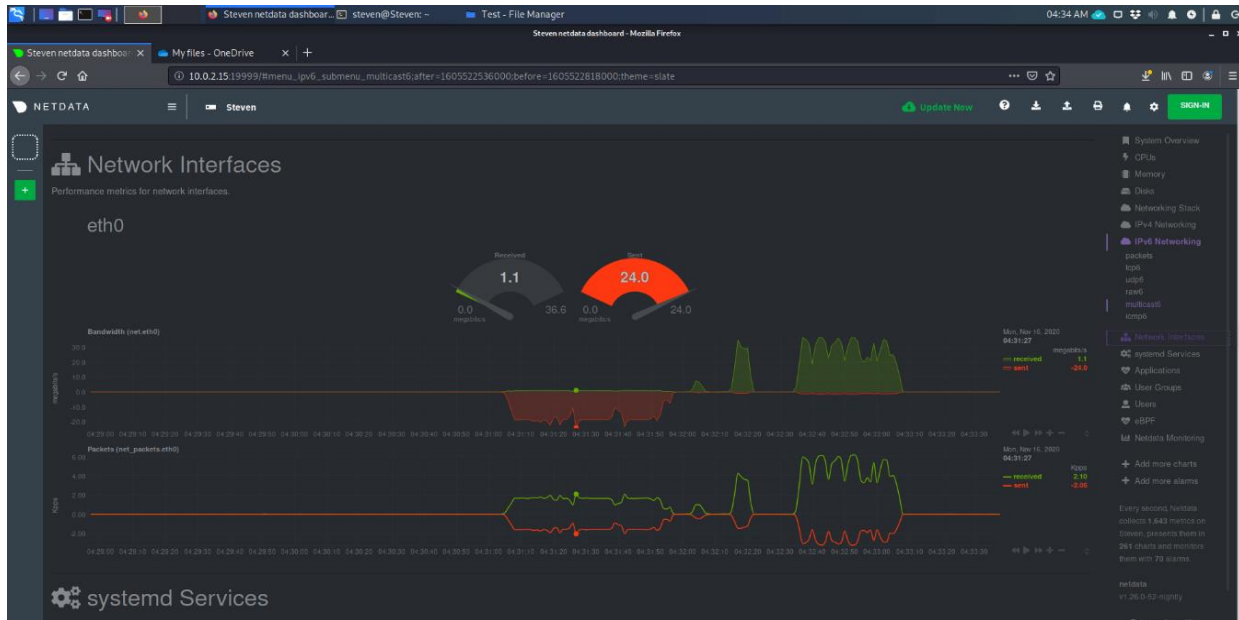


Figure 19. OneDrive rclone network usage when sending data

In the real experimental environment, Figure 20 shows the maximum network usage of OneDrive with rclone when receiving data as 36.6 (megabits/s) while 100Mb data file is used when encrypting and decrypting throughout the test case.

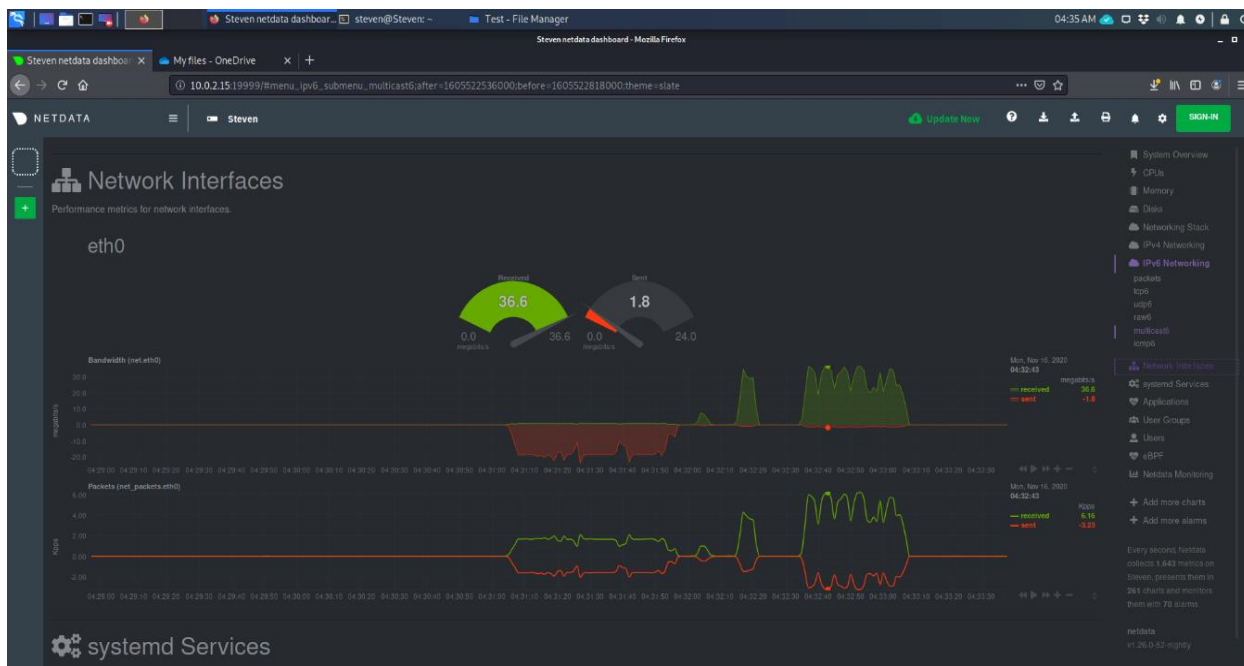


Figure 20. OneDrive rclone network usage when receiving data

The following Figure 21 shows the maximum CPU usage of OneDrive with p7zip is 74.5 as a percentage while 100Mb data file is used when encrypting and decrypting throughout the test case, in the real experimental environment.

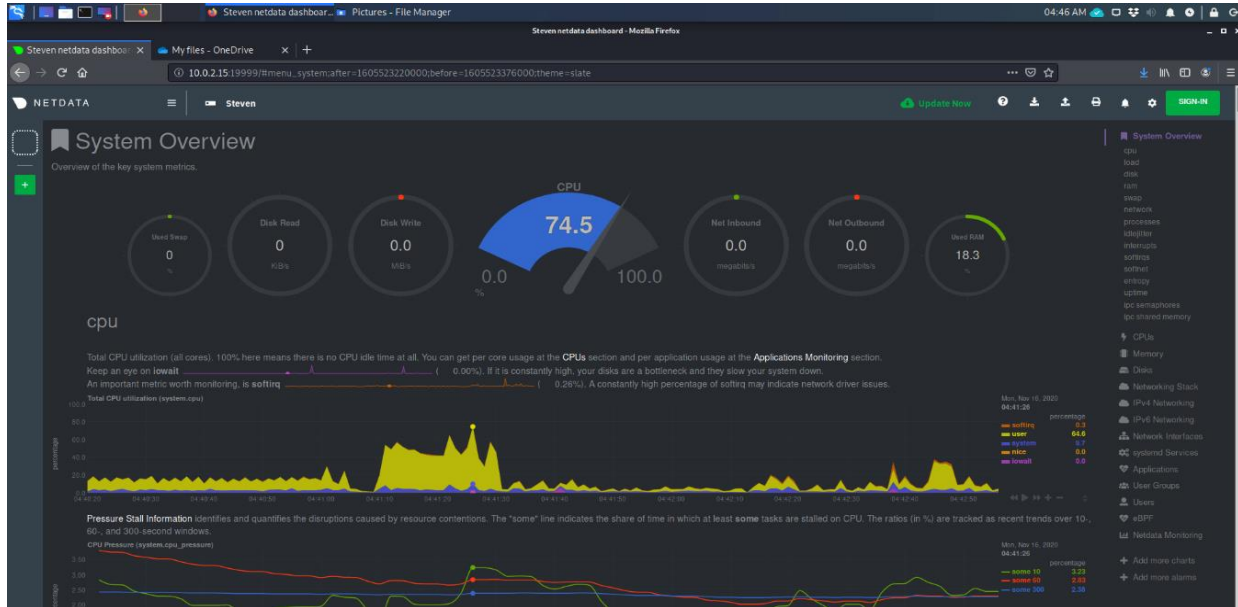


Figure 21. OneDrive p7zip CPU usage

In the real experimental environment, Figure 22 shows the maximum network usage of OneDrive with p7zip when sending data as 23.1 (megabits/s) while 100Mb data file is used when encrypting and decrypting throughout the test case.

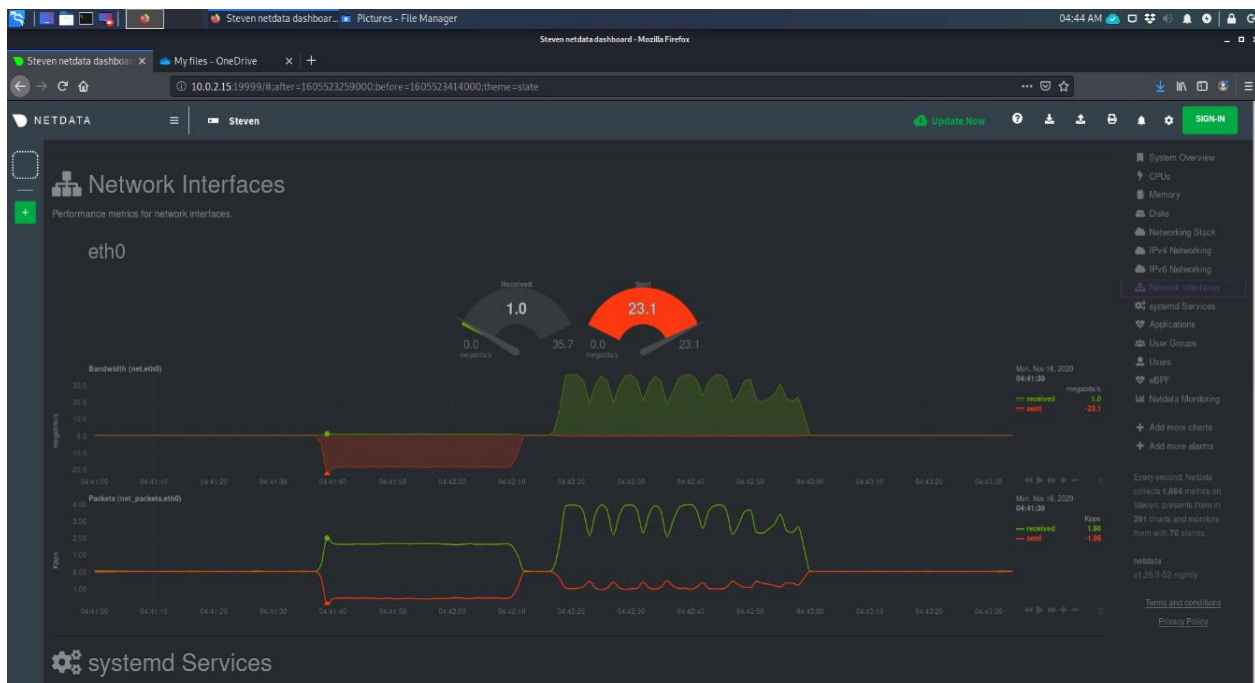


Figure 22. OneDrive p7zip network usage when sending data

In the real experimental environment, Figure 23 shows the maximum network usage of OneDrive with p7zip when receiving data as 35.7 (megabits/s) while 100Mb data file is used when encrypting and decrypting throughout the test case.

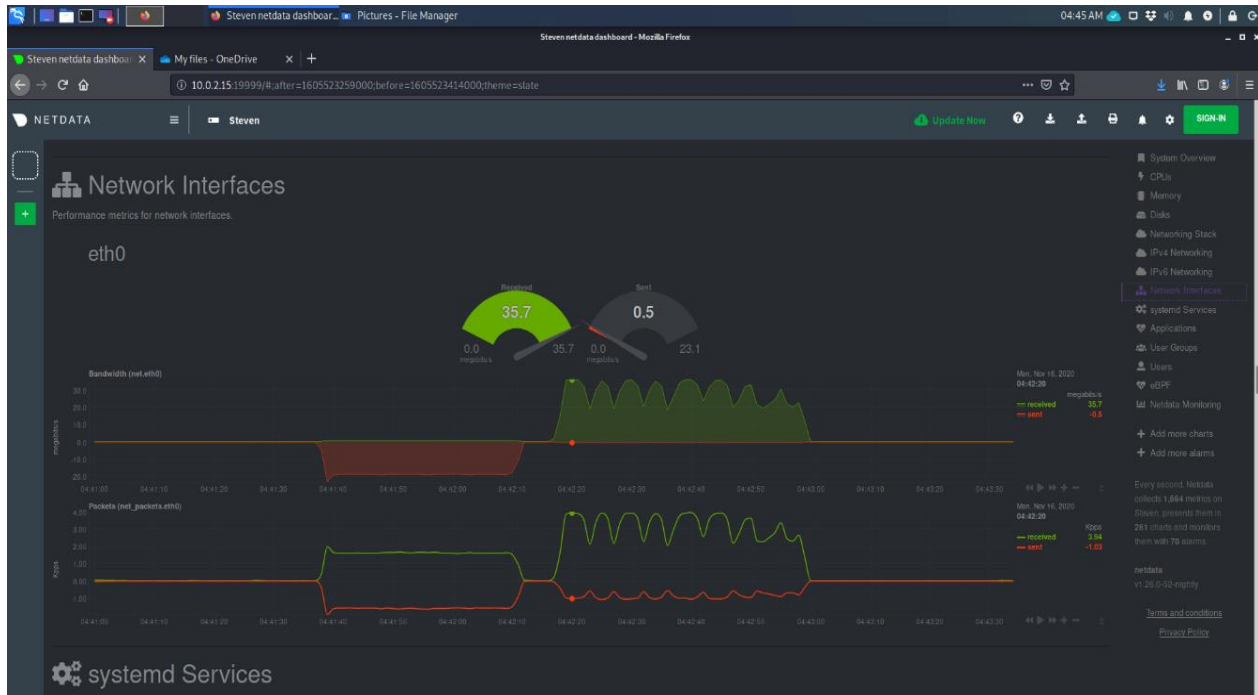


Figure 23. OneDrive p7zip network usage when receiving data

Conclusion

After executing all the experiments, according to the aforementioned Table 1 and Table 2 it can be clearly seen that Pcloud rclone and OneDrive rclone both tie in with total points while Dropbox rclone total point is less by 1 point compared to other two services. In addition, the story is the same with p7zip for all their cloud services. Based on the results, in this study, we found that Pcloud was more convenient to work with because there is a Pcloud sync folder that could quickly view from. OneDrive and Dropbox had the one disadvantage of not having a sync folder option available for Linux operating systems. For this factor authors are giving the tie to Pcloud rclone setup. In addition, it is also found that this setup was the most secure and less demanding scenario that allows for users to safely encrypt their data onto the cloud without having to worry about anyone viewing their sensitive information. In this experimentation we also found that p7zip was extremely easy to work with however the demand on network and the limitations of its encryption limited it results compared with OneDrive and Dropbox. To use any of these scenarios will be more than good enough for any average user who uses a cloud storage service, however if the need was to come when the information needed to stay secure from viewing eyes that one scenario is best for this task. Final conclusion has come with the clear recommendation that if someone is a cloud storage user and wish to keep his/her information secure online that user use Pcloud with rclone to keep the information safe and secure from any unwanted eyes.

Conflict of Interest

The authors declare no conflict of interest.

References

- [1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Lecture Notes in Computer Science*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 457-473.
- [2] "A new hybrid cryptography technique in wireless sensor network," *VOLUME-8 ISSUE-10, AUGUST 2019, REGULAR ISSUE*, vol. 8, no. 10, pp. 121-131, 2019.
- [3] A. Mailewa Dissanayaka, R. R. Shetty, S. Kothari, S. Mengel, L. Gittner, and R. Vadapalli, "A review of MongoDB and singularity container security in regards to HIPAA regulations," in *Companion Proceedings of the 10th International Conference on Utility and Cloud Computing*, 2017.
- [4] R. R. Shetty, A. M. Dissanayaka, S. Mengel, L. Gittner, R. Vadapalli, and H. Khan, "Secure NoSQL based medical data processing and retrieval: The exposome project," in *Companion Proceedings of the 10th International Conference on Utility and Cloud Computing*, 2017.
- [5] D. Agrawal and C. C. Aggarwal, "On the design and quantification of privacy preserving data mining algorithms," in *Proceedings of the twentieth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems - PODS ' 01*, 2001.
- [6] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in *Proceedings of the 2004 ACM SIGMOD international conference on Management of data - SIGMOD ' 04*, 2004.
- [7] W. Itani, A. Kayssi, and A. Chehab, "Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures," in *2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*, 2009.
- [8] A. M. Dissanayaka, S. Mengel, L. Gittner, H. Khan, "Dynamic & portable vulnerability assessment testbed with Linux containers to ensure the security of MongoDB in Singularity LXC's." In *Companion Conference of the Supercomputing-2018 (SC18)*. 2018.
- [9] A. M. Dissanayaka, S. Mengel, L. Gittner, and H. Khan, "Security assurance of MongoDB in singularity LXC's: an elastic and convenient testbed using Linux containers to explore vulnerabilities," *Cluster Comput.*, 2020.
- [10] P. Brebner and A. Liu, "Performance and cost assessment of cloud services," in *Service-Oriented Computing*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 39-50.
- [11] A. Mailewa, and J. Herath. "Operating systems learning environment with VMware." *The Midwest Instruction and Computing Symposium (MICS)*, Verona, WI. 2014.
- [12] R. Rahimi et al., "An industrial robotics application with cloud computing and high-speed networking," in *2017 First IEEE International Conference on Robotic Computing (IRC)*, 2017.
- [13] A. Mailewa, J. Herath, and S. Herath, "A survey of effective and efficient software testing." *The Midwest Instruction and Computing Symposium (MICS)*, Grand Forks, ND. 2015.
- [14] A. N. Khan, M. L. Mat Kiah, M. Ali, S. Shamshirband, and A. ur R. Khan, "A cloud-manager-based re-encryption scheme for mobile users in cloud environment: A hybrid approach," *J. Grid Comput.*, vol. 13, no. 4, pp. 651-675, 2015.
- [15] T. Dargahi, A. Dehghantanha, and M. Conti, "Investigating storage as a service cloud platform: pCloud as a case study," *arXiv [cs.CR]*, 2017.
- [16] F. Daryabar, A. Dehghantanha, B. Eterovic-Soric, and K.-K. R. Choo, "Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices," *Aust. J. Forensic Sci.*, vol. 48, no. 6, pp. 615-642, 2016.
- [17] L. Caviglione, M. Podolski, W. Mazurczyk, and M. Ianigro, "Covert channels in personal cloud storage services: The case of dropbox," *IEEE Trans. Industr. Inform.*, vol. 13, no. 4, pp. 1921-1931, 2017.
- [18] A. M. Dissanayaka, S. Mengel, L. Gittner, and H. Khan, "Vulnerability prioritization, root cause analysis, and mitigation of secure data analytic framework implemented with MongoDB on singularity Linux containers," in *Proceedings of the 2020 the 4th International Conference on Compute and Data Analysis*, 2020.
- [19] S. Islam, M. Ouedraogo, C. Kalloniatis, H. Mouratidis, and S. Gritzalis, "Assurance of security and privacy requirements for cloud deployment models," *IEEE trans. cloud comput.*, vol. 6, no. 2, pp. 387-400, 2018.
- [20] Z. Zhang, Q. Pei, J. Ma, and L. Yang, "Implementing trustworthy dissemination of digital contents by using a third party attestation proxy-enabling remote attestation model," in *2008 International Conference on MultiMedia and Information Technology*, 2008.
- [21] A. Mailewa, S. Mengel, L. Gittner, and H. Khan, "Mechanisms and techniques to enhance the security of big data analytic framework with mongodb and Linux containers," *SSRN Electron. J.*, 2021.

- [22] B.-H. Lee, E. K. Dewi, and M. F. Wajdi, "Data security in cloud computing using AES under HEROKU cloud," in 2018 27th Wireless and Optical Communication Conference (WOCC), 2018.
- [23] N. H. Ahmad, A. S. S. A. Hamid, N. S. S. Shahidan, and K. A. Z. Ariffin, "Cloud forensic analysis on pCloud: From volatile memory perspectives," in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Cham: Springer International Publishing, 2020, pp. 3-15.
- [24] I. Agus, F. Destiawati, and H. Dhika, "Perbandingan cloud computing Microsoft onedrive, dropbox, dan Google drive," *Fakt. exacta*, vol. 12, no. 1, p. 20, 2019.
- [25] J. Yun, J. Hur, Y. Shin, and D. Koo, "CLDSafe: An efficient file backup system in cloud storage against ransomware," *IEICE Trans. Inf. Syst.*, vol. E100.D, no. 9, pp. 2228-2231, 2017.
- [26] N. Padhy, "An automation API to optimize the rate of transmission using rclone from local system to cloud storage environment," *Mater. Today*, vol. 37, pp. 2462-2466, 2021.
- [27] S. Thapa, and A. Mailewa. "The Role of Intrusion Detection/Prevention Systems in Modern Computer Networks: A Review." *The Midwest Instruction and Computing Symposium (MICS)*, vol. 53, pp. 1-14. 2020.
- [28] N. Padhy, R. Kumar Mishra, S. C. Satapathy, and K. S. Raju, "An automation API for authentication and security for file uploads in the cloud storage environment," *Intell. Decis. Technol.*, vol. 14, no. 3, pp. 393-407, 2020.
- [29] N. S. S. Srinivas and M. Akramuddin, "FPGA based hardware implementation of AES Rijndael algorithm for Encryption and Decryption," in 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016.
- [30] M. Akintaro, T. Pare, and A. Mailewa. "Darknet and black market activities against the cybersecurity: a survey." *The Midwest Instruction and Computing Symposium (MICS)*, North Dakota State University, Fargo, ND. 2019.
- [31] M. Padhi and R. Chaudhari, "An optimized pipelined architecture of SHA-256 hash function," in 2017 7th International Symposium on Embedded Computing and System Design (ISED), 2017.