Analysis of Rclone Implementation for File Sharing Security on OneDrive Cloud Storage

Lilik Widyawati[1*], **Muhammad Azwar**[2], **Haerudin Alafi**[3], **Iqra Asif**[4]
[1,2,3]Department of Computer Engineering, Bumigora University, Indonesia
[4]Riphah International University, Pakistan
lilikwidya@universitasbumigora.ac.id[1*], muhamadazwar@universitasbumigora.ac.id[2], haerudinalafi9@gmail.com[3], iqraasif706@gmail.com[4]

Article Info:
Received: 26 May 2024, Revised: 28 June 2024, Accepted: 29 June 2024

Abstract-
Background: OneDrive provides a reliable infrastructure for storing and managing user data. However, along with the benefits, the security challenges associated with storing and sharing files in the cloud are also increasing. One of the main aspects of cloud storage security management is the file-sharing process. While OneDrive offers a few security features, such as access control and two-factor authentication, there remains a need to strengthen additional layers of security, especially when sharing files with external parties.
Objective: This research aims to analyze the effectiveness of Rclone in improving file-sharing security on OneDrive, especially File Backup and File Encryption.
Methods: This research uses the Network Development Life Cycle (NDLC) method, which includes six stages. This research focuses on three stages: analysis, design, and simulation prototyping.
Result: The application of Rclone for file sharing security on OneDrive can increase data security in cloud storage, as evidenced by three backup attempts on .doc files with an average time of 2.033 seconds and successful encryption of 4 files with an average time of 37 seconds.
Conclusion: Using Rclone as a tool to manage data security on OneDrive improves data protection and provides flexibility and efficiency in file management, making it an effective solution for file sharing security needs in cloud storage.

Keywords: Rclone, File Sharing, OneDrive, Cloud Storage.

Corresponding Author:
Lilik Widyawati,
Department of Computer Engineering, Bumigora University, Indonesia
Email: lilikwidya@universitasbumigora.ac.id

1. INTRODUCTION

In today's digital era, the need for secure data storage that can be accessed anytime and anywhere has become one of the top priorities for individuals and organizations. One solution that is widely used is cloud storage, which offers large storage capacity, easy access, and efficient collaboration features [1]. It should be understood that when users utilize cloud storage, things that need to be considered are in terms of security in their use, especially those that are public cloud and for users who use the free version of cloud storage from cloud operators [2].

However, with the increasing use of cloud storage, concerns about the security of data stored and shared on the platform also arise. Risks related to data breaches, unauthorized access, and other threats are a serious concern for OneDrive users. Therefore, it is important to implement additional security measures to protect

How to Cite: L. Widyawati, M. Azwar, H. Alafi, and I. Asif, "Analysis of Rclone Implementation for File Sharing Security on OneDrive Cloud Storage". Jurnal Bumigora Information Technology (BITe), vol.6, no.1, Juni 2024

sensitive data stored in the cloud, although OneDrive offers a number of security features, such as access control, and two-factor authentication [3], there is still a need to strengthen additional layers of security, especially when sharing files with external parties, and achieving complete security is almost impossible due to the complex structure of the cloud, but securing data by applying encryption can reduce many risks related to shared data [4]. The eight elements of data security in cloud storage systems are data confidentiality, data integrity, data availability, granular access control, secure data sharing in dynamic groups, complete leak-proof data deletion, and privacy protection [5], so additional security measures need to be taken.

Rclone is a command-line software that is very useful for managing and synchronizing files across various cloud storage services [6]. Rclone supports various features such as encryption, synchronization, and data backup, which makes it a powerful tool for improving security and efficiency in file management in the cloud. With its encryption capabilities, Rclone can ensure that data sent and stored on OneDrive remains protected from unauthorized access, and Rclone can also synchronize data automatically [7].

Some related research, namely [8] securing data on cloud storage media using encryption techniques, this research focuses on critical issues, as well as solutions and future directions for maintaining security and privacy in a cloud computing environment. The next research [9] is the analysis of data security threats in cloud computing. This research focuses on analyzing the risks and challenges in companies' implementation of public cloud services, focusing on observation, documentation studies, and interviews with stakeholders. Further research [10] discusses a cloud storage system that uses stable next cloud media on average, requiring a bandwidth of 1024 kbps (kilobytes per second), which is accessed both on the Kediri City Dispendukcapil network. Furthermore, research [11] discusses utilizing cloud storage efficiently based on API capabilities and analysis of heterogeneous raw data (in extreme quantities). Further research [12] discusses a methodology for evaluating cloud storage providers in the field of data-intensive systems based on the fundamental operations provided by service providers, as well as making performance comparisons of several popular cloud storage services in terms of operation execution time. Further research, namely research [13], which produces OneDrive and Dropbox, has one drawback because it does not have a synchronization folder option available for the Linux operating system, so additional features for synchronization are needed.

Based on the problems that have been described and some of the research above mostly discusses the use of cloud storage without being equipped with additional features, making the authors interested in combining information security perspectives with best practices in cloud storage management, this research is expected to provide valuable insight into the potential use of Rclone, especially file backup and file encryption in improving file sharing security on OneDrive. Through this in-depth analysis, we hope to provide helpful guidance to organizations and individuals looking to strengthen their security strategies in file sharing in a cloud environment.

This research **aims** to analyze the application of Rclone in the context of file-sharing security on OneDrive cloud storage. The main focus is on how Rclone can improve the security of data stored and shared through OneDrive, especially the file backup and file encryption processes, and identify the benefits and challenges that may be faced during its implementation. This analysis is hoped to provide clear guidance for OneDrive users on how to utilize Rclone to maintain data integrity and confidentiality.

2. Research Method

The research method used in this research is the Network Development Life Cycle (NDLC) methodology. NDLC is a cycle of designing or developing a network infrastructure that allows network monitoring to determine network statistics and performance [14]; using NDLC network design can be more adaptive and flexible to keep up with technological developments [15]. The cycle can be seen in Figure 1 below.

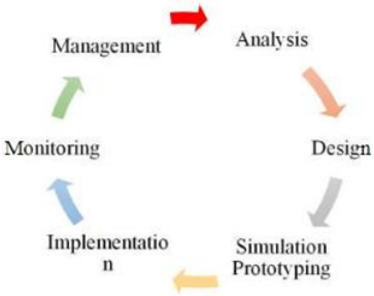

Figure 1. Research method

Figure 1 describes the stages of the NDLC method: analysis, design, simulation prototyping, implementation, monitoring, and management. However, this research only focuses on three stages, namely analysis, design, and simulation prototyping including testing, following the explanation of the 3 stages used:

2.1. Analysis

In this initial stage, the researcher carries out the analysis stage, namely analyzing the needs, analyzing existing problems, and analyzing the design to be built by collecting data by literature study, namely reading journals and scientific articles to obtain information related to cloud storage data security using Rclone to analyze whether the backup and cryptography features in Rclone are fulfilled for cloud storage data security OneDrive.

2.2. Design Stage

In this design stage, researchers create a network design that will be implemented and tested virtually using VirtualBox, where the trial will be operated on 1 (one) computer with a Windows 11 operating system as a host and client to access existing cloud storage data. In VirtualBox, 1 (one) virtual machine uses the Ubuntu desktop 20.04 operating system, which will be the configuration center of Rclone and a cloud server to encrypt data. The design can be seen in Figure 2 below.

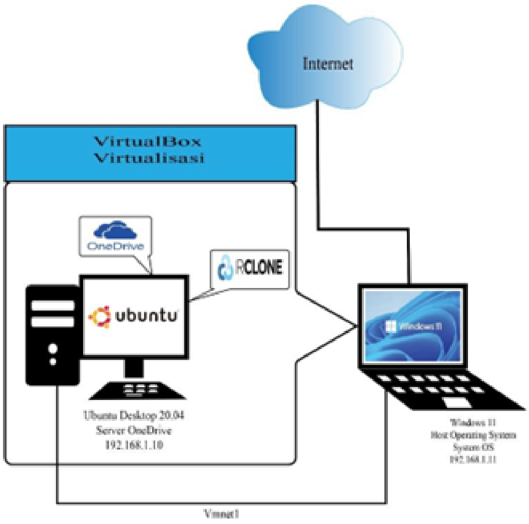

Figure 2. Simulated Network Design

In Figure 2, the network design has two computers: a Windows 11 client that functions to access the OneDrive service through file sharing and an Ubuntu desktop server that is used to install OneDrive and Rclone. The system design of this research can be seen in Figure 3 below, where this design starts from the server side and ends at the client.

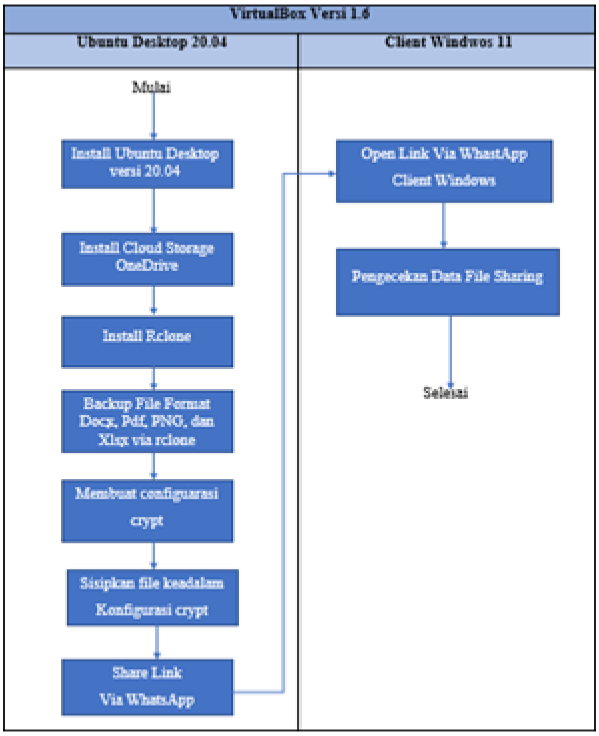
VirtualBox Versi 1.6
Ubuntu Desktop 20.04
Client Windwos 11
Mulai
Install Ubuntu Desktop versi 20.04
Install Cloud Storage OneDrive
Install Rclone
Backup File Format Docx, Pdf, PNG, dan Xlsx via rclone
Membuat configuarasi crypt
Sisipkan file keadalam Konfigurasi crypt
Share Link Via WhatsApp
Open Link Via WhatsApp Client Windows
Pengecekan Data File Sharing
Selesai

Figure 3. Simulated Network Design

In Figure 3, we can see the system design used, when the Ubuntu server is used, the OneDrive cloud storage will be built afterward to run, then the Rclone installation will be carried out from the Ubuntu server side to backup files in the form of files with docx, xlsx, pdf, and PNG formats to the OneDrive cloud storage. Then, to protect or secure files on one drive, the crypt feature on Rclone will be used to be configured on the cloud server side. To ensure the configuration is successfully applied, it will be tested by sharing files that have been uploaded first and sharing links via WhatsApp. So that the final result will be that we can make sure Rclone can be applied to file security on cloud storage OneDrive or vice versa.

2.3. Simulation Prototyping

At this stage, installation, configuration and test scenarios will be carried out on each of the network design devices that have been previously compiled.

2.3.1. Installation and configuration

At this stage, the researcher will divide this stage into several, namely the installation and configuration of the Ubuntu desktop, the installation and configuration of one drive, and finally, the installation and configuration of Rclone on the server. At this stage, the ubuntu 20.04 operating system is installed as a place to place the OneDrive cloud storage server on VirtualBox 1.6. Where will this ubuntu be installed, and then add its IP address configuration? Then, the next stage will install the One Drive cloud storage on the Ubuntu desktop 20.04 operating system and then run the OneDrive application to verify accounts and passwords. The following stage will be installed on the Ubuntu desktop 20.04 server side. This third-party application is used to configure data security or file sharing contained in the OneDrive cloud storage.

2.3.2. System Testing

At this stage, installation, configuration, and test scenarios will be carried out on each of the network design devices that have been made, where this process will install and configure the Ubuntu desktop, install and configure the OneDrive cloud storage, and install the Rclone configuration. Then, in this, Rclone will make two remotes to backup and encrypt OneDrive cloud storage, in this case, the data tested with xlsx, docx, pdf, and png formats did 3x trials of each format both backup and encryption. The results of the scenario analysis will be presented in the table both from the Ubuntu desktop side as a server and Windows 11 as a client.

3. RESULTS AND DISCUSSION

The research results that has been done, namely the use of OneDrive cloud storage by implementing Rclone in maintaining data security, have been successful. This supports the research of Yan et al. [5] on the need for data security in cloud storage. The trial scenario will be carried out, namely the backup and encryption trial scenario through Rclone, each format 3 times the experiment.

3.1. Test Scenario Results

In this testing phase, a test will be carried out, starting by opening the OneDrive browser. After that, the Rclone application will be configured on the Ubuntu desktop 20.04 that is being run. Then, remote access to the OneDrive cloud storage will be configured via Rclone. At this stage, an analysis of the results of the test scenario will be carried out. The file-sharing security carried out in this study is the application of file backup and file encryption, where the results of the application of Rclone will be analyzed from the OneDrive cloud storage server side with the parameters of the speed of data backup time and encryption time, then from the windows 11 client side using encryption parameters only to determine the results of data security. Then, the analysis results will be presented using a table with the parameters of file format, file size, data backup time, encryption time, and encryption fulfilled or not from the Ubuntu server and Windows 11 client side.

3.1.1. Backup Trial

In the following backup trial, experiment 1 was carried out. It contained 4 (four) files that could be backed up from local Ubuntu to OneDrive via Rclone.

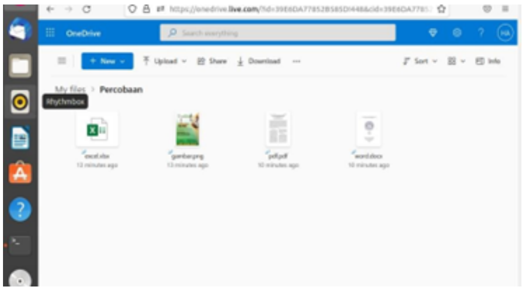

Figure 4. Experiment 1 File Backup Results

In Figure 4, the results of trial 1 backup above show that files with xlsx, png, pdf, and docx formats can be backed up to the OneDrive cloud storage in ubuntu. The next trial backup is experiment 2, which contains 4 files in the experiment2 folder with the backup results shown in the picture below.

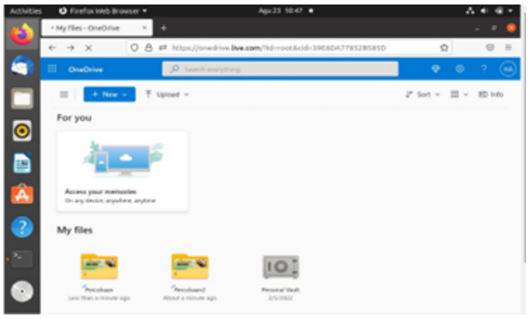

Figure 5. Experiment 2 File Backup Results

In Figure 5, the folder Trial 2 has been successfully backed up, along with 4 files that contain the formats described earlier. The next experiment will backup all file formats to OneDrive via Rclone, and experiment 3 is the last experiment to backup data.

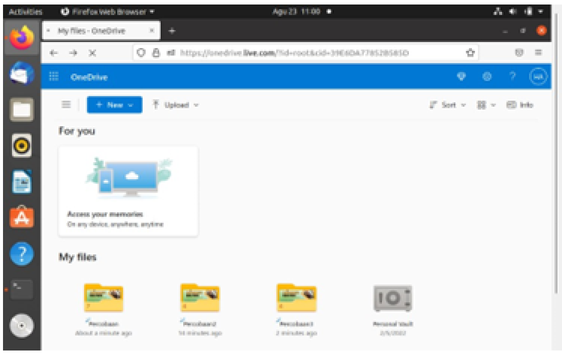

Figure 6. Experiment 1 File Backup Results

In Figure 6 above will be backed up files and folders with the folder name Experiment 3 which includes 4 file formats. Based on the results of the backup, the three experiments in each file format will be analyzed for the backup speed results obtained from each file format which will be presented in the results of the natural analysis in the form of a table.

3.1.2. Encryption Trial

In the encryption trial, 3 trials will be carried out according to the files that have been backed up before. This encryption process is done to secure the file so that the file is not easy to know its meaning.

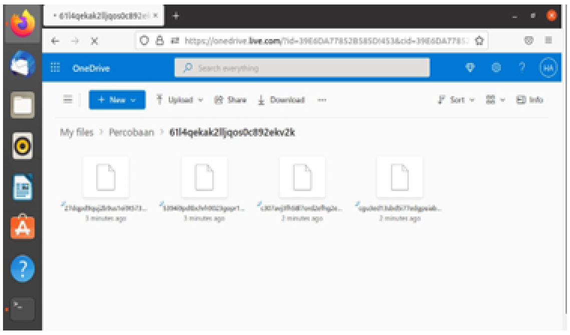

Figure 7. Encryption Result of Experiment 1

In Figure 7, the results of trial 1 encryption can be encrypted in both the folder and its contents. This is where the file format that has been encrypted on OneDrive in Ubuntu will be shared and accessed by the Windows client. Furthermore, in experiment 2 the same thing was done but with a different folder name. The data can be encrypted, as an experiment 1.

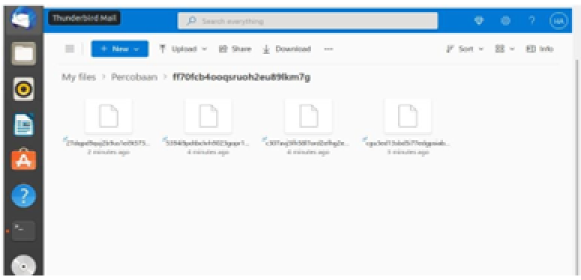

Figure 8. Encryption Result of Experiment 2

In Figure 8 above the encryption results of experiment 2 are different in terms of folder names but the contents are the same. Then, experiment 3 is done encryption through Rclone, which can be done with different encryption results in terms of folder names.

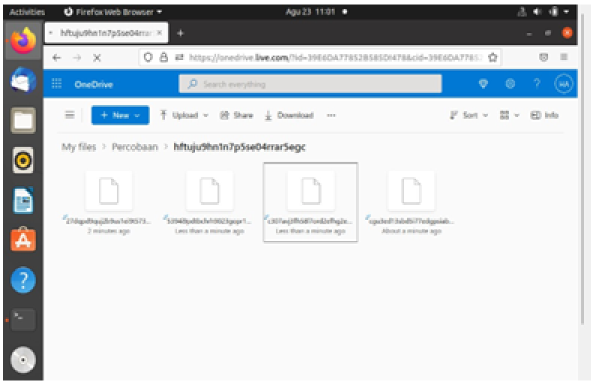

Figure 9. Encryption Result of Experiment 3

So that each encryption experiment is done to determine the fastest encryption time from the Ubuntu side of each experiment.

3.2. Test Scenario Analysis Results

The results of the test scenario analysis will be presented in the following table, where the parameters used are backup time and encryption time. Tests were conducted on 4 types of file formats and different sizes; each document was tested 3 times, as shown in Table 1 below.

Table 1. Backup Analysis Results on Ubuntu Server

Ubuntu Server					
Experiment	**Format file**	**File size**	**Backup time**	**Total**	**Averages**
1	.Docx	132.225 Kb	1.2 s	6.1 s	2.033 s
2			2.6 s		
3			2.3 s		
1	.Pdf	1.14 Mb	3.5 s	14 s	4.666 s
2			5.2 s		
3			5.3 s		
1	.Xlsx	4.321 Kb	3.3 s	11.5 s	3.833 s
2			4 s		
3			4.2 s		
1	.PNG	1.847 Mb	4.5 s	17 s	5.666 s
2			6.1 s		
3			6.4 s		

In table 1. The results of the backup analysis above show that the author combines the three experiments into one table where each file format is combined in one table in the previous experiment table to determine the estimated time used to back up data using Rclone. Where on the Ubuntu server, the .Docx file format, the amount of time used to back up the data from the three experiments was 6.1 seconds with an average of 2,033 seconds. Then, in the. In PDF file format, the time used to back up the data was 14 seconds from the three experiments, with an average of 4,666 seconds. Then the .Xlsx file format with a total backup time of 11.5 s and an average of 3,833 s. Then, the last .Png file format, which can use a total time of 17 seconds with an average of 5,666 seconds for the three experiments on the .png format. So in Rclone, the file backup feature can be done in the OneDrive cloud storage with varying backup times, where files with the .docx format the first experiment was the fastest with a backup time of 1.2 seconds, and the second experiment was the slowest among the 3 experiments. Then, the fastest .Pdf file format in the first experiment with a backup time of 3.5s and 5.3s is the slowest of the three experiments. Then, in the .xlsx file format, the fastest backup time is 3.3s, and the slowest backup time is 4.2s among the three experiments. Then the last with the .png format, the fastest time is 4.5s and the longest is 6.4s. This means that it can be concluded that the larger the file size and file type that is backed up using Rclone to cloud storage OneDrive, the time used will be greater and vice versa, the smaller the file size, even though the different file formats will be the smaller the estimated time spent backing up the data.

Next is the result of encryption analysis on both sides, namely the server side and the client side. The results of the analysis can be seen in Table 2.

Table 2. Encryption Analysis Results on Both Sides

	Ubuntu Server		**Client Windows**	
Experiment	**Format file**	**Encryption time**	**Encryption**	**Encryption**
1	.Docx .Pdf .Xlsx .PNG	1m 21.8 s	Fulfilled	Fulfilled
2	.Docx .Pdf .Xlsx .PNG	12.3 s	Fulfilled	Fulfilled
3	.Docx .Pdf .Xlsx .PNG	16.9 s	Fulfilled	Fulfilled
Total		**111 s**		
Averages		**37 s**		

In Table 2, the results of Encryption Analysis on Both Sides above, researchers conducted 3 encryption experiments with experiments 1, 2, and 3. Experiment 1, with all file formats tested, can be encrypted properly with an encryption time of 1 minute 21.8 seconds, and on the client Windows side, experiment 1 can be encrypted. In experiment 2, the same file format can also be encrypted with an encryption time of 12.3 seconds, and on the client side, the data or file sharing is encrypted properly. In the last experiment, 3, the encryption time used was 16.9 s, and both server and client sides could be encrypted. From these three experiments, the researcher got the amount of time used to encrypt all files with 3x trials, which was 111 s. with an average of 37s. This research is in line with research conducted by [8][9].

4. CONCLUSION

The use of Rclone is proven as a tool for managing data security on OneDrive not only increases data protection but also provides flexibility and efficiency in file management, making it an effective solution for the security needs of file sharing on cloud storage and based on the test scenario of this research, Rclone can backup and encrypt data into OneDrive cloud storage with .docx, .pdf, .xlsx, and .png file formats with varying backup times from each file format which is influenced by file sizes such as . doc file with a size of 132.225 kb takes an average time of 2.033 seconds, a .pdf file with a size of 1.4 Mb takes an average time of 14 seconds and encryption can be fulfilled both from the server and client side and is not affected by the estimated time spent on encryption even though each experiment has a different encryption time due to different file sizes and formats so that the average time required for the 4 file encryption process is 37 seconds.

ACKNOWLEDGEMENT

We thank all those who have helped in this research.

References

[1] P. Prajapati and P. Shah, "A Review on Secure Data Deduplication: Cloud Storage Security Issue," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 7, pp. 3996–4007, Jul. 2022, https://doi.org/10.1016/j.jksuci.2020.10.021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1319157820305140

[2] L. Tantowi and L. Wijayanti, "Peluang dan Tantangan Penyimpanan Cloud Storage pada Dokumen Digital," *Shaut Al-Maktabah : Jurnal Perpustakaan, Arsip dan Dokumentasi*, vol. 15, no. 1, pp. 118–131, Jun. 2023, https://doi.org/10.37108/shaut.v15i1.803. [Online]. Available: https://www.rjfahuinib.org/index.php/shaut/article/view/803

[3] R. P. Mellisa, M. F. Duskarnaen, and A. Idrus, "Peluang Dan Tantangan Penyimpanan Cloud Storage Pada Dokumen Digitalanalisis Perbandingan Kinerja Layanan Cloud Computing Pada Aplikasi Dropbox, Google Drive, dan Onedrive Dengan Metode Boehms Quality Model," *PINTER : Jurnal Pendidikan Teknik Informatika dan Komputer*, vol. 7, no. 1, pp. 72–77, Jun. 2023, https://doi.org/10.21009/pinter.7.1.9. [Online]. Available: https://journal.unj.ac.id/unj/index.php/pinter/article/view/38729

[4] A. Syed, K. Purushotham, and G. Shidaganti, "Cloud Storage Security Risks, Practices and Measures: A Review," in *2020 IEEE International Conference for Innovation in Technology (INOCON)*, Nov. 2020, pp. 1–4, https://doi.org/10.1109/INOCON50539.2020.9298281. [Online]. Available: https://ieeexplore.ieee.org/document/9298281

[5] P. Yang, N. Xiong, and J. Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey," *IEEE Access*, vol. 8, pp. 131 723–131 740, 2020, https://doi.org/10.1109/ACCESS.2020.3009876. [Online]. Available: https://ieeexplore.ieee.org/document/9142202

[6] N. Padhy, "An automation API to optimize the rate of transmission using rclone from local system to cloud storage environment," *Materials Today: Proceedings*, vol. 37, pp. 2462–2466, Jan. 2021, https://doi.org/10.1016/j.matpr.2020.08.288. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214785320361605

[7] R. R. Adityo, "Pengembangan Aplikasi Qiscus Meet SDK Berbasis Framework Jitsi Open Source di Qiscus," *AUTOMATA*, vol. 3, no. 1, pp. 1–6, Jan. 2022, number: 1. [Online]. Available: https://journal.uii.ac.id/AUTOMATA/article/view/21882

[8] Suhada and M. I. P. Nasution, "Keamanan Dan Privasi Data dalam Lingkungan Cloud Computing: Tantangan dan Solusi," *Kohesi: Jurnal Sains dan Teknologi*, vol. 1, no. 10, pp. 71–80, Dec. 2023, number: 10. [Online]. Available: https://ejournal.warunayama.org/index.php/kohesi/article/view/1150

[9] N. Chandra and F. Yanto, "Cloud Computing Analisis Ancaman Keamanan Data Dalam Cloud Computing," *JCOME*, vol. 1, no. 2, pp. 71–75, Nov. 2023, number: 2. [Online]. Available: https://komputer.iam-indonesia.org/index.php/jcome/article/view/12

[10] M. R. Anwarrudin, R. Indriati, and S. Sucipto, "Perancangan dan Implementasi Cloud Storage untuk File Sharing dan File Sinkronisasi," *Prosiding SEMNAS INOTEK (Seminar Nasional Inovasi Teknologi)*, vol. 4, no. 3, pp. 45–50, Aug. 2020, https://doi.org/10.29407/inotek.v4i3.30. [Online]. Available: https://proceeding.unpkediri.ac.id/index.php/inotek/article/view/30

[11] N. Padhy, R. K. Mishra, and S. Mishra, "Archival solution API to upload bulk file and managing the data in cloud storage," *International Journal of Intelligent Defence Support Systems*, vol. 6, no. 1, pp. 35–59, Jan. 2020, https://doi.org/10.1504/IJIDSS.2020.109180. [Online]. Available: https://www.inderscienceonline.com/doi/abs/10.1504/IJIDSS.2020.109180

[12] A. Dimov and S. Kirov, "Data Performance Evaluation of Cloud Storage Providers," in *Information Systems & Grid Technologies: Fifteenth International Conference ISGT2022*, Sofia, Bulgaria, May 2022, pp. 63–73.

[13] S. Gamnis, M. VanderLinden, and A. Mailewa, "Analyzing Data Encryption Efficiencies for Secure Cloud Storages: A Case Study of Pcloud vs OneDrive vs Dropbox," *Advances in*

Technology, pp. 79–98, May 2022, https://doi.org/10.31357/ait.v2i1.5526. [Online]. Available: https://journals.sjp.ac.lk/index.php/ait/article/view/5526

[14] T. Sanjaya and D. Setiyadi, "Network Development Life Cycle (NDLC) Dalam Perancangan Jaringan Komputer Pada Rumah Shalom Mahanaim," *JURNAL MAHASISWA BINA INSANI*, vol. 4, no. 1, pp. 1–10, Aug. 2019. [Online]. Available: https://ejournal-binainsani.ac.id/index.php/JMBI/article/view/1149

[15] Kamdan, Somantri, M. G. Sundayana, and I. L. Kharisma, "Rancang Bangun Layanan Private cloud Berbasis Infrastructure as a Service Menggunakan OpenStack dengan Metode Network Development Life Cycle(NDLC)," *KLIK: Kajian Ilmiah Informatika dan Komputer*, vol. 4, no. 1, pp. 252–262, Aug. 2023, https://doi.org/10.30865/klik.v4i1.1001. [Online]. Available: https://djournals.com/klik/article/view/1001