

Implementasi Server Cloud Storage Menggunakan SFTPGo, Docker, dan Cloudflare Tunnel

Zen Aufa Bahalwan, Dimas Febriawan

Fakultas Teknologi Industri dan Informatika, Universitas Muhammadiyah Prof. DR. HAMKA

Email: hello@zenaufa.id, dimas.febriawan@uhamka.ac.id

Article Info

Received: March 19, 2025

Accepted: September 10, 2025

Published: September 31, 2025

ABSTRAK

Implementasi server cloud storage berbasis SFTPGo memungkinkan pengguna untuk mengakses dan mengelola penyimpanan file melalui WebGUI dan klien SFTP. Penelitian ini bertujuan untuk mengembangkan sistem penyimpanan berbasis cloud yang aman dan dapat diakses dengan mudah menggunakan teknologi Docker dan Cloudflare Tunnel. Sistem ini diimplementasikan pada server berbasis Linux dan diuji dengan berbagai skenario untuk memastikan kehandalan akses WebGUI serta konektivitas melalui protokol SFTP. Hasil implementasi menunjukkan bahwa kombinasi SFTPGo, Docker, dan Cloudflare Tunnel dapat menyediakan lingkungan penyimpanan yang fleksibel dan aman. Dengan mekanisme ini, pengguna dapat mengunggah dan mengunduh file dengan kredensial yang telah ditentukan, serta memastikan bahwa akses melalui SFTP hanya dapat dilakukan melalui Cloudflare Tunnel, meningkatkan keamanan sistem.

Kata kunci : *Cloudflare Tunnel, Cloud Storage, Docker, SFTP, SFTPGo, WebGUI*

ABSTRACT

The implementation of a cloud storage server based on SFTPGo allows users to access and manage file storage via WebGUI and SFTP clients. This study aims to develop a secure and easily accessible cloud storage system using Docker and Cloudflare Tunnel technology. The system is implemented on a Linux-based server and tested in various scenarios to ensure the reliability of WebGUI access and connectivity via the SFTP protocol. The implementation results show that the combination of SFTPGo, Docker, and Cloudflare Tunnel provides a flexible and secure storage environment. With this mechanism, users can upload and download files using predefined credentials, while ensuring that SFTP access is only possible through Cloudflare Tunnel, enhancing system security.

Keywords : *Cloudflare Tunnel, Cloud Storage, Docker, SFTP, SFTPGo, WebGUI*

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat saat ini telah memicu transformasi signifikan dalam cara individu dan organisasi memperlakukan data. *Cloud storage* menjadi salah satu solusi utama yang populer karena kemampuannya untuk menyediakan sistem penyimpanan data yang aman, efisien, dan mudah diakses. Layanan penyimpanan berbasis *cloud* memungkinkan pengguna untuk mengakses data dari berbagai perangkat dan lokasi, menghilangkan ketergantungan pada penyimpanan fisik tradisional. Hal ini sekaligus memungkinkan pengelolaan data yang lebih baik dan kolaborasi antar pengguna yang lebih efektif, yang dibuktikan dalam berbagai penelitian (Pawitra et al., 2020; Purwantoro E.S.G.S, 2022).

Namun, di balik kenyamanan dan efisiensi yang ditawarkan oleh cloud storage, terdapat tantangan serius terkait keamanan dan privasi data. Aspek keamanan menjadi perhatian utama karena berkaitan dengan transfer data, terutama melalui jaringan publik. *SFTP (Secure File Transfer Protocol)* muncul sebagai salah satu metode yang diandalkan untuk mentransfer file secara aman. Keunggulan *SFTP* terletak pada kemampuannya untuk mengenkripsi data selama proses pengiriman, sehingga meminimalkan risiko penyadapan dan akses tidak sah (Rachmawanto & Sari, 2022; Robbi et al., 2019). Implementasi perangkat lunak *open-source* seperti *SFTPGo* memungkinkan pengguna untuk menggunakan *WebGUI* maupun klien

SFTP, sehingga meningkatkan kemudahan akses tanpa mengorbankan aspek keamanan.

Untuk lebih memperkuat keamanan sistem *cloud storage*, integrasi dengan teknologi modern seperti *Docker* dan *Cloudflare Tunnel* juga sangat dianjurkan. *Docker* memungkinkan aplikasi untuk berjalan dalam kontainer yang terisolasi, yang dapat mengurangi kerentanan terhadap serangan dari *Cloudflare Tunnel*, di sisi lain, memberikan lapisan tambahan dengan menyembunyikan alamat *server* asli dari pengguna, serta mengamankan akses dengan menerapkan enkripsi.. Dalam konteks ini, penggunaan metode yang tepat dalam pengelolaan dan penyimpanan data sangat penting untuk keberlangsungan operasi yang aman dan efisien.

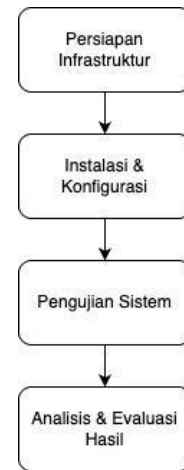
Penerapan *server cloud storage* yang menyatukan berbagai teknologi ini diharapkan tidak hanya menawarkan fleksibilitas dan kemudahan penggunaan, tetapi juga memperhatikan aspek keamanan yang krusial. Dengan sistem yang dirancang untuk dapat diakses melalui *WebGUI* dan klien *SFTP*, pengguna dapat merasakan keuntungan dari penyimpanan berbasis *cloud* yang memiliki lapisan keamanan yang lebih mantap (Malvi & Painem, 2020) Peningkatan dalam metode pengamanan file seperti kriptografi dan steganografi juga memberikan kontribusi penting dalam memastikan bahwa data sensitif tetap terlindungi selama proses penyimpanan dan pengiriman (Malvi & Painem, 2020; Rachmawanto & Sari, 2022).

Meskipun berbagai studi telah membahas elemen-elemen teknologi ini secara terpisah, penelitian yang secara eksplisit mengintegrasikan *SFTPGO*, *Docker*, dan *Cloudflare Tunnel* dalam satu solusi *cloud storage* yang aman, ringan, dan mudah diimplementasikan masih sangat terbatas. Inilah kesenjangan yang hendak dijawab dalam penelitian ini.

Penelitian ini bertujuan untuk mengembangkan dan mengevaluasi implementasi server cloud storage berbasis Linux yang menggabungkan *SFTPGO*, *Docker*, dan *Cloudflare Tunnel*. Tujuan utama adalah menciptakan sistem penyimpanan file yang dapat diakses dengan aman melalui *WebGUI* dan klien *SFTP*, serta terlindungi dari akses langsung melalui internet. Kontribusi utama dari studi ini adalah demonstrasi sistem cloud storage yang terintegrasi dan efisien untuk skala kecil hingga menengah, dengan fokus pada keamanan dan kemudahan penggunaan, yang diharapkan dapat memperluas praktik-praktik terbaik dalam pengembangan infrastruktur *cloud* yang aman dan terjangkau.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan eksperimental dalam mengimplementasikan server cloud storage berbasis *SFTPGO*, *Docker*, dan *Cloudflare Tunnel*. Metode penelitian ini terdiri dari beberapa tahapan utama, yaitu **persiapan infrastruktur, instalasi dan konfigurasi layanan, serta pengujian sistem.**



Gambar 1. Alur Metodologi Penelitian

2.1. Persiapan Infrastruktur

Pada tahap ini, dilakukan persiapan perangkat keras dan perangkat lunak yang digunakan dalam implementasi cloud storage, antara lain:

- 1) **Perangkat Keras:** Server berbasis Linux dengan spesifikasi yang mendukung kontainerisasi dan layanan jaringan.
- 2) **Perangkat Lunak:**
 - a) **SFTPGO:** SFTPGO merupakan sebuah solusi server SFTP yang memiliki beragam fitur untuk mendukung penyimpanan dan pengelolaan data secara aman di cloud. Dengan kemampuan untuk mengakomodasi berbagai protokol seperti SFTP, SCP, dan WebDAV, SFTPGO menciptakan lingkungan penyimpanan yang fleksibel serta aman bagi penggunaanya. Layanan penyimpanan berbasis cloud harus memiliki kontrol akses yang ketat untuk menjamin keamanan dan integritas data (Sudetlin et al., 2018), Fitur manajemen pengguna pada SFTPGO juga memungkinkan pengelolaan hak akses yang mendetail, memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses data sensitif.
 - b) **Docker:** Docker berfungsi sebagai platform kontainerisasi yang signifikan dalam mengelola penyebaran aplikasi. Dengan menggunakan Docker, pengembang dapat menjalankan SFTPGO di dalam kontainer yang terisolasi, yang mengurangi risiko konflik dengan perangkat lunak lain serta memberi kemudahan dalam pengelolaan aplikasi. Penggunaan Docker dalam penyebaran aplikasi memberikan efisiensi yang tinggi serta memudahkan integrasi dengan berbagai layanan cloud.. Selain itu, teknologi kontainer seperti Docker

memfasilitasi pembelajaran dan pengembangan aplikasi cloud dengan menunjukkan kemudahan penerapan dan efektivitas dalam pelajaran berbasis cloud (Erlangga et al., 2022).

- c) **Cloudflare Tunnel:** Cloudflare Tunnel memungkinkan pengamanan akses ke server SFTPGo dari internet dengan memberikan lapisan keamanan tambahan untuk mencegah serangan siber. Cloudflare secara efektif melindungi server dari serangan DDoS dan serangan berbasis web lainnya, memastikan ketersediaan dan integritas layanan. Penelitian menunjukkan pentingnya pendekatan keamanan dalam adopsi teknologi cloud, yang mencakup pengamanan data dan privasi pengguna. Perlindungan yang ditawarkan oleh layanan seperti Cloudflare sangat penting untuk meningkatkan kepercayaan pengguna dalam adopsi solusi cloud computing (Setiawan & Gui, 2023). Selain itu, penerapan teknologi cloud harus mempertimbangkan keamanan sebagai salah satu faktor utama dalam menyusun layanan publik yang efektif (Suhendar, 2022).

2.2. Instalasi dan Konfigurasi Layanan

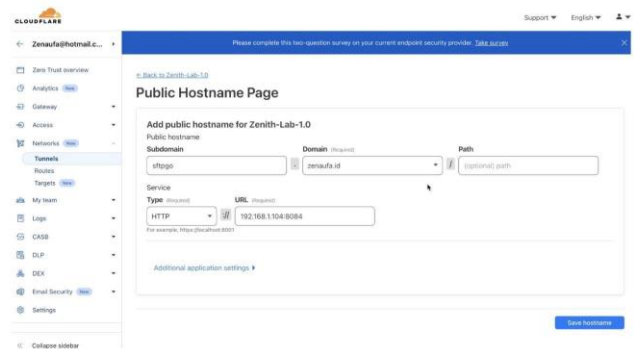
Tahap ini mencakup proses instalasi dan konfigurasi perangkat lunak yang diperlukan agar sistem dapat beroperasi dengan optimal. Langkah-langkah yang dilakukan meliputi:

- 1) **Instalasi Docker:** Menggunakan perintah berikut untuk menginstal Docker pada server berbasis Linux:
`sudo apt update && sudo apt install docker.io -y`
- 2) **Deploy SFTPGo di dalam Docker:** Menjalankan SFTPGo menggunakan perintah berikut

```
lab.zenaufa.id/webterminal/ttyd/
root@zenithlab1:~# docker pull drakkan/sftpggo
Using default tag: latest
latest: Pulling from drakkan/sftpggo
2d429b9e73a6: Pull complete
831f55fca1a0: Pull complete
c80e73d1b617: Pull complete
c7da3857337b: Pull complete
837ed6973272: Pull complete
2a0c819c6a4a: Pull complete
ed37644b8c5d: Pull complete
7c384828c817: Pull complete
3fa5cc75d61a: Pull complete
448244219a04: Pull complete
d1953a9cc744: Pull complete
9731f3b1174c: Pull complete
446fa70eef54: Pull complete
Digest: sha256:42ef940421b43f9651a8dacf882ac6467cee32a74f8d213617daf3c0ebf74344
Status: Downloaded newer image for drakkan/sftpggo:latest
docker.io/drakkan/sftpggo:latest
root@zenithlab1:~#
```

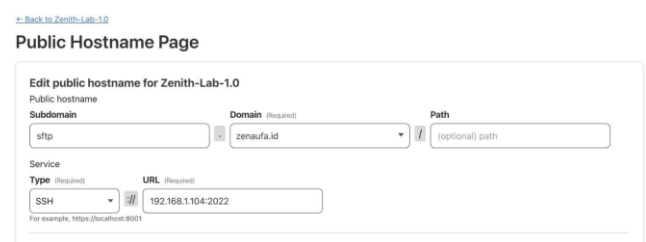
Gambar 2. Tampilan terminal yang berhasil melakukan Deployment SFTPGo di dalam Docker.

- **Konfigurasi Cloudflare Tunnel untuk WebGUI :** Membuat dan menghubungkan Cloudflare Tunnel untuk membuka akses WebGUI ke internet dengan konfigurasi sebagai berikut :



Gambar 3. Konfigurasi Cloudflare Tunnel untuk WebGUI SFTPGo

- **Konfigurasi Cloudflare Tunnel untuk akses FTP :** Membuat dan menghubungkan Cloudflare Tunnel untuk mengamankan akses FTP melalui internet dengan konfigurasi sebagai berikut :



Gambar 4. Konfigurasi Cloudflare Tunnel untuk akses FTP ke server SFTPGo

- 3) **Pengaturan WebGUI:** Mengkonfigurasi akses ke SFTPGo melalui WebGUI menggunakan port 8084 agar pengguna dapat mengelola penyimpanan melalui antarmuka berbasis web.
- 4) **Pembuatan dan Manajemen Pengguna:** Menambahkan pengguna dengan kredensial tertentu agar dapat mengakses cloud storage melalui WebGUI maupun klien SFTP seperti FileZilla.

2.3. Pengujian Sistem

Untuk memastikan keandalan sistem, dilakukan serangkaian pengujian dengan skenario sebagai berikut:

- 1) **Pengujian Akses WebGUI:** Pada tahap ini, uji akses dilakukan untuk memastikan bahwa WebGUI SFTPGo dapat diakses melalui tautan yang telah dikonfigurasi. Pengujian ini penting untuk mengkonfirmasi bahwa antarmuka pengguna dapat dijangkau dengan baik dan memberikan pengalaman yang intuitif bagi pengguna. Dalam konteks cloud computing, kemampuan aksesibilitas merupakan salah satu indikator utama dalam menilai kinerja sistem (Huang & Liu, 2013). Selain itu, pemantauan keamanan melalui HTTPS juga harus diimplementasikan untuk melindungi data dari potensi serangan (Lim, 2020).
- 2) **Pengujian Koneksi SFTP:** Pengujian ini melibatkan penggunaan klien SFTP seperti FileZilla untuk memastikan konektivitas dan

keamanan dalam transfer data antara klien dan server. Pengujian ini penting untuk menilai apakah transfer data berlangsung dengan lancar dan aman, serta untuk mengidentifikasi potensi masalah keamanan yang mungkin muncul selama proses transfer data (H. Wang & Poplett, 2019). Memastikan transfer menggunakan protokol SFTP, yang mengenkripsi koneksi, adalah langkah krusial dalam melindungi data yang ditransfer dari sumber yang tidak sah (Poshtkahi & Ghaznavi-Ghouschi, 2012)

- 3) **Pengujian Cloudflare Tunnel:** Evaluasi dilakukan terhadap efektivitas Cloudflare Tunnel dalam melindungi akses ke server dari ancaman eksternal. Pengujian ini bertujuan untuk mengidentifikasi apakah konfigurasi dan pengaturan Cloudflare Tunnel benar-benar memberikan lapisan keamanan tambahan yang diharapkan. Konfigurasi yang baik dapat membantu mengamankan server dari serangan DDoS (Gupta & Saini, 2017). Penelitian sebelumnya menunjukkan bahwa integrasi solusi keamanan seperti Cloudflare dapat meningkatkan kepercayaan pengguna dalam layanan cloud (Yang et al., 2011).
- 4) **Pengujian Upload dan Download File:** Setelah pengaturan dan koneksi dipastikan berfungsi, tahap ini mengukur performa dan kestabilan sistem dalam menangani proses unggah dan unduh file dengan berbagai ukuran. Pengujian ini penting untuk memastikan bahwa sistem dapat menangani beban kerja yang bervariasi tanpa mengalami penurunan performa (X. Wang & Wang, 2015). Selain itu, eksperimen yang dilakukan akan memberikan wawasan tentang batasan bandwidth dan latensi yang mungkin mempengaruhi pengalaman pengguna selama transfer data (Zhu et al., 2016).

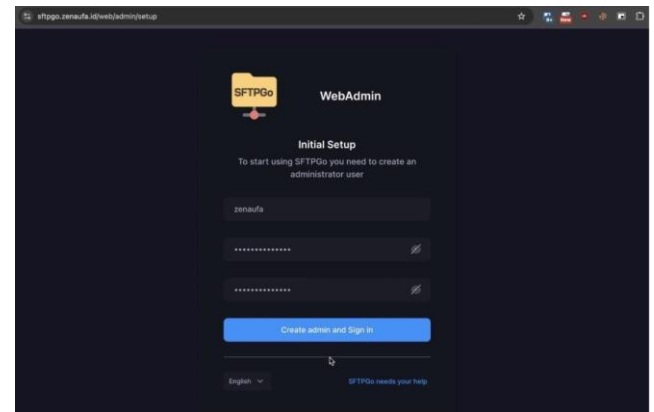
Dengan metode pengujian yang sistematis dan komprehensif ini, diharapkan implementasi cloud storage yang dikembangkan dapat beroperasi secara optimal, aman, dan dapat diakses dengan mudah oleh pengguna. Hal ini juga mencerminkan komitmen untuk menyediakan solusi cloud yang tidak hanya handal tetapi juga menghadapi tantangan keamanan dan performa dengan baik.

3. HASIL DAN PEMBAHASAN

3.1. Implementasi Server Cloud Storage Menggunakan SFTPGo

Hasil dari penelitian ini menunjukkan bahwa server cloud storage berbasis **SFTPGo**, **Docker**, dan **Cloudflare Tunnel** berhasil diimplementasikan dan dapat diakses melalui **WebGUI** dan klien **SFTP**. Server diinstal pada sistem operasi berbasis **Linux**, dengan **SFTPGo** yang berjalan dalam lingkungan **Docker**. Konfigurasi dilakukan untuk memastikan bahwa layanan dapat diakses dengan kredensial yang telah ditentukan.

Berikut adalah tampilan awal dari **WebGUI SFTPGo** yang berhasil diakses melalui **browser** setelah proses instalasi dan konfigurasi selesai dilakukan.



Gambar 5. Tampilan **WebGUI SFTPGo** yang berhasil diakses melalui browser.

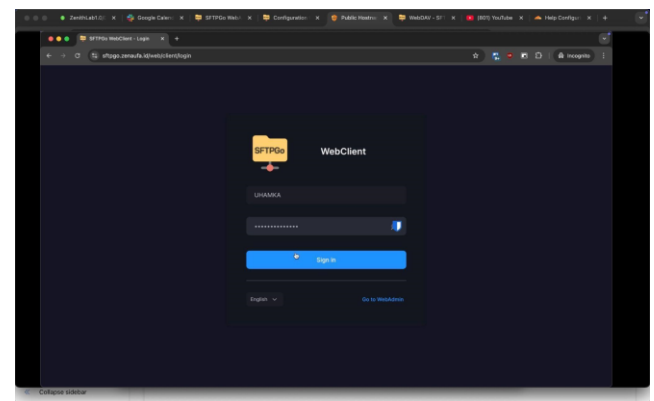
Proses konfigurasi **SFTPGo** di dalam kontainer **Docker** menghasilkan **output** berikut pada **terminal**, yang menandakan bahwa layanan berjalan dengan baik.



Gambar 6. Hasil konfigurasi **SFTPGo** dalam **Docker**.

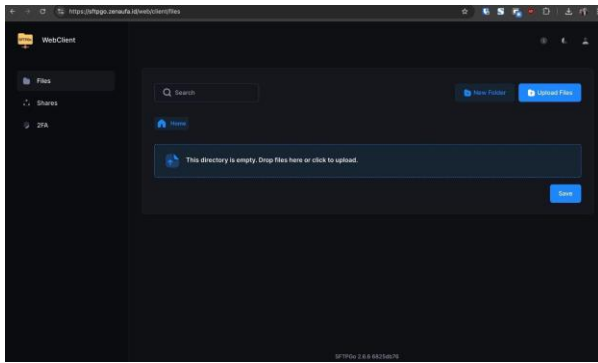
3.2. Akses WebGUI dan Manajemen Pengguna

Setelah implementasi berhasil, **WebGUI** dapat diakses melalui alamat <https://SFTPGo.zenaufa.id/>. Pengguna dapat masuk ke sistem menggunakan kredensial yang telah ditentukan. **WebGUI** ini menyediakan fitur untuk **mengunggah dan mengunduh file**, serta melakukan manajemen akun pengguna.



Gambar 7. Login **WebGUI SFTPGo**.

Setelah berhasil masuk ke sistem, pengguna akan diarahkan ke dashboard utama **WebGUI SFTPGo** seperti tampak pada gambar berikut.



Gambar 8. Tampilan dashboard *WebGUI SFTPGo* setelah login berhasil.

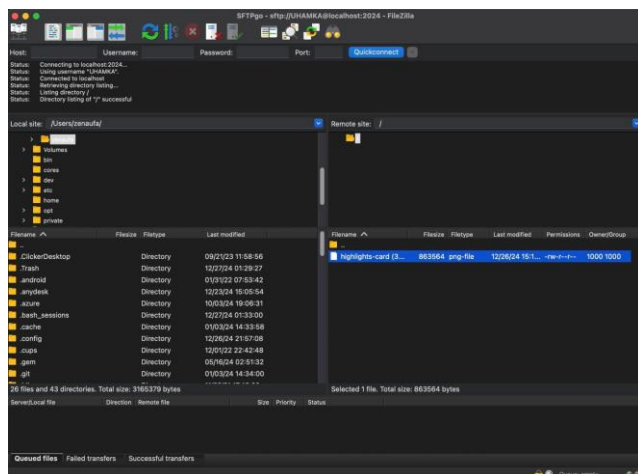
3.3. Akses *SFTP* melalui *Cloudflare Tunnel*

Untuk memastikan keamanan akses ke server, koneksi *SFTP* hanya dapat dilakukan melalui *Cloudflare Tunnel*. Dengan konfigurasi ini, akses langsung ke server melalui internet dibatasi, sehingga hanya pengguna yang memiliki kredensial yang dapat terhubung melalui *FileZilla* atau klien *SFTP* lainnya. Pengujian dilakukan dengan menjalankan perintah berikut pada klien:

```
MacBook-Pro-2:~ zenaufa$ cloudflared access ssh --hostname sftp.zenaufa.id --url localhost:2024
2024-12-26T18:43:16Z INF Start Websocket listener host=localhost:2024
```

Gambar 9. Tangkapan layar *terminal* yang menunjukkan perintah *Cloudflare Tunnel* berjalan sukses sehingga server *SFTP* dapat diakses melalui alamat *localhost:2024*.

Hasil pengujian menunjukkan bahwa koneksi **berhasil tersambung** dan pengguna dapat mengelola file melalui klien *SFTP*.



Gambar 10. Tangkapan layar *FileZilla* yang berhasil terkoneksi ke server *SFTP* melalui *Cloudflare Tunnel*.

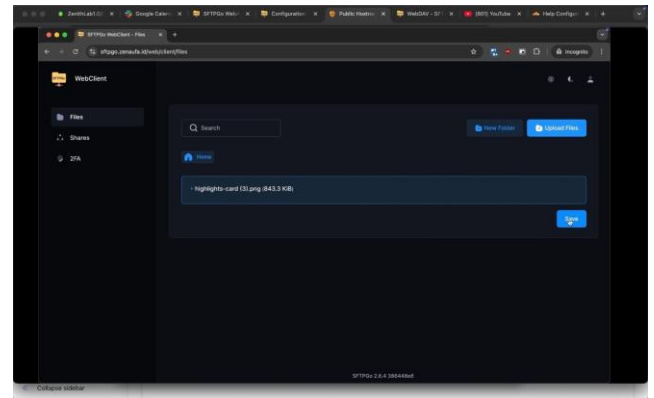
3.4. Pengujian Unggah dan Unduh File

Pengujian dilakukan untuk memastikan bahwa pengguna dapat melakukan **unggah dan unduh file** melalui *WebGUI* dan klien *SFTP*. Hasil pengujian menunjukkan bahwa:

- 1) **File berhasil diunggah ke server melalui *WebGUI* tanpa kendala.**

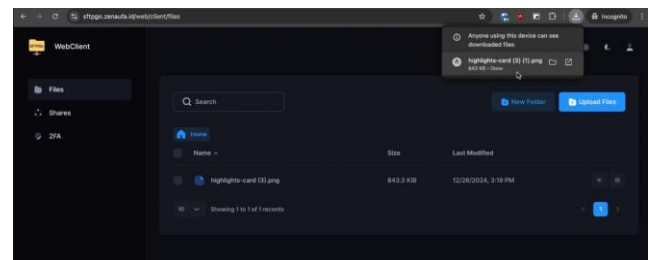
- 2) **File dapat diunduh kembali menggunakan *WebGUI* maupun klien *SFTP*.**
- 3) **Kecepatan transfer file stabil, menyesuaikan dengan kecepatan koneksi jaringan.**

Pengguna dapat melakukan unggah *file* ke *server* melalui antarmuka *WebGUI*, seperti diperlihatkan dalam gambar berikut.



Gambar 11. Tangkapan layar proses unggah file melalui *WebGUI*.

File yang telah diunggah sebelumnya juga dapat diunduh kembali melalui *WebGUI* dengan tampilan seperti pada gambar berikut.



Gambar 12. Tangkapan layar proses unduh file dari *WebGUI*.

3.5. Evaluasi Keamanan dan Kinerja Sistem

Hasil pengujian pada penelitian ini menunjukkan bahwa integrasi *SFTPGo*, *Docker*, dan *Cloudflare Tunnel* mampu menyediakan sistem penyimpanan yang aman, efisien, dan stabil. Temuan ini sejalan dengan penelitian oleh (Malvi & Painem, 2020), yang menekankan pentingnya penggunaan kriptografi dan sistem terenkapsulasi untuk meningkatkan keamanan data digital. Selain itu, hasil kinerja sistem dalam lingkungan *Docker* juga konsisten dengan studi (Erlangga et al., 2022) yang menunjukkan efisiensi dan stabilitas *container* dalam pembelajaran berbasis *cloud*.

Jika dibandingkan dengan penelitian oleh (Sudetlin et al., 2018) yang memanfaatkan private cloud storage berbasis *IaaS*, penelitian ini menunjukkan peningkatan dalam hal kemudahan implementasi dan fleksibilitas akses (Sudetlin et al., 2018) lebih menekankan pada arsitektur berbasis infrastruktur virtual, sementara penelitian ini menunjukkan integrasi *WebGUI* dan *SFTP* berbasis *container*, serta pengamanan akses dengan tunneling terenkripsi dari *Cloudflare Tunnel*. Pendekatan ini memberikan lapisan keamanan tambahan yang lebih

kuat terhadap serangan eksternal, serta menyederhanakan proses *deployment*.

Dengan demikian, implementasi yang dilakukan dalam penelitian ini tidak hanya menguatkan temuan-temuan sebelumnya, tetapi juga memberikan kontribusi praktis dengan menggabungkan berbagai pendekatan teknologi menjadi satu solusi yang terintegrasi dan aman.

4. KESIMPULAN

Hasil implementasi menunjukkan bahwa kombinasi *SFTPGO*, *Docker*, dan *Cloudflare Tunnel* dapat menyediakan cloud storage yang aman, fleksibel, dan mudah diakses. Pengguna dapat mengunggah dan mengunduh file melalui *WebGUI* atau klien *SFTP* dengan kredensial yang telah ditentukan. Penggunaan *Cloudflare Tunnel* memastikan bahwa akses ke server tetap aman dari ancaman eksternal.

DAFTAR PUSTAKA

- Erlangga, E., Wahyudin, W., & Wihardi, Y. (2022). Pengembangan Framework Smart Mobile Cloud Learning System Untuk Pendidikan Pembelajaran Cerdas Menuju Smart Learning Environment. *INFORMATION SYSTEM FOR EDUCATORS AND PROFESSIONALS: Journal of Information System*, 6(2), 117. <https://doi.org/10.51211/isbi.v6i2.1773>
- Gupta, S., & Saini, A. K. (2017). Modeling Trust Based Risk Management in Cloud Adoption using Fuzzy Inference System. *International Journal of Technology Diffusion*, 8(1), 52–60. <https://doi.org/10.4018/IJTD.2017010104>
- Huang, L. N., & Liu, F. H. (2013). Data Storage Technology and its Development Based on Cloud Computing. *Advanced Materials Research*, 756–759, 1275–1279. <https://doi.org/10.4028/www.scientific.net/AMR.756-759.1275>
- Lim, M. (2020). C2CFTP: Direct and Indirect File Transfer Protocols Between Clients in Client-Server Architecture. *IEEE Access*, 8, 102833–102845. <https://doi.org/10.1109/ACCESS.2020.2998725>
- Malvi, A., & Painem, P. (2020). Pengamanan File Gambar pada Media Video dengan Kriptografi Algoritma RSA dan Steganografi Algoritma End of File (EOF). *Informatik: Jurnal Ilmu Komputer*, 16(2), 67. <https://doi.org/10.52958/iftk.v16i2.1860>
- Pawitra, I. G. N. Y., Hartati, R. S., & Divayana, Y. (2020). Rancang Bangun Aplikasi File Transfer Menggunakan Library ZeroMQ. *Majalah Ilmiah Teknologi Elektro*, 19(1), 55. <https://doi.org/10.24843/MITE.2020.v19i01.P08>
- Poshtkahi, A., & Ghaznavi-Ghouschi, M. B. (2012). The xDotGrid native, cross-platform, high-performance xDFS file transfer framework. *Computers & Electrical Engineering*, 38(6), 1409–1432. <https://doi.org/10.1016/j.compeleceng.2012.04.007>
- Purwanto E.S.G.S, S. (2022). Perbandingan Kinerja Clustered File System pada Cloud Storage menggunakan GlusterFS dan Ceph. *INOVTEK Polbeng - Seri Informatika*, 7(2), 319. <https://doi.org/10.35314/isi.v7i2.2753>
- Rachmawanto, E. H., & Sari, C. A. (2022). Gabungan Advanced Encryption Standard Dan Vigenere Cipher Untuk Pengamanan Dokumen Digital. *Jurnal Informatika Polinema*, 8(4), 1–8. <https://doi.org/10.33795/jip.v8i4.996>
- Robbi, F. A. A., Prasetyo, A. B., & Widiyanto, E. D. (2019). Perbandingan Kinerja Block Storage Ceph dan ZFS di Lingkungan Virtual. *Jurnal Teknologi Dan Sistem Komputer*, 7(1), 7–11. <https://doi.org/10.14710/jtsiskom.7.1.2019.7-11>
- Setiawan, S., & Gui, A. (2023). Faktor-Faktor Penentu Yang Mempengaruhi Adopsi Cloud Computing Di Indonesia. *Infotech: Journal of Technology Information*, 9(1), 1–8. <https://doi.org/10.37365/jti.v9i1.144>
- Sudetlin, S., Natasha, N. D., & Darusalam, U. (2018). Pemanfaatan Private Cloud Storage Berbasis Infrastructure As A Service (IAAS). *JOINTECS (Journal of Information Technology and Computer Science)*, 3(1). <https://doi.org/10.31328/jointecs.v3i1.497>
- Suhendar, E. (2022). Tinjauan Sistematis: Implementasi Cloud Computing Terhadap Keamanan Layanan Publik. *Smart Comp: Jurnalnya Orang Pintar Komputer*, 11(4). <https://doi.org/10.30591/smartcomp.v11i4.4245>
- Wang, H., & Poplett, L. (2019). Developing a Practical Electronic Records Transfer Workflow for Wisconsin Public Records. *Archival Issues*, 40(1). <https://doi.org/10.31274/archivalissues.11086>
- Wang, X., & Wang, H. (2015). *Research on Digital Library Based on Cloud Computing*. <https://doi.org/10.2991/iiicec-15.2015.326>
- Yang, X., Shen, Q., Yang, Y., & Qing, S. (2011). *A Way of Key Management in Cloud Storage Based on Trusted Computing* (pp. 135–145). https://doi.org/10.1007/978-3-642-24403-2_11
- Zhu, H., Wu, L., Huang, K., & Zhou, Z. (2016). Research on Methods for Discovering and Selecting Cloud Infrastructure Services Based on Feature Modeling. *Mathematical Problems in Engineering*, 2016, 1–19. <https://doi.org/10.1155/2016/8194832>