

## **Analisis Integritas Data Dalam Mekanisme Berbagi *File* Google Drive: Studi Kasus Pengujian *End-To-End***

**Aan Alamsyah<sup>1</sup>, Kholik Prasajo<sup>2\*</sup>, Nurul Aulia Rais<sup>3</sup>, Dhea Januarti<sup>4</sup>, Salsabila Aurelia<sup>5</sup>, Fauzan Abdullah<sup>6</sup>**

<sup>1,2,3,4,5,6</sup>Universitas Negeri Makassar

(\*)Corresponding Author E-mail: [kholik.prasajo@unm.ac.id](mailto:kholik.prasajo@unm.ac.id)

### **ARTICLE HISTORY**

*Received* :

*Revised* :

*Accepted* :



### **ABSTRACT**

Ensuring data integrity is a critical aspect of cloud storage systems, especially in *file-sharing* mechanisms between users. This study aims to analyze how well Google Drive preserves data integrity during *file* transfers by employing an end-to-end testing approach. The method used is experimental, involving a systematic procedure: creating test *files* in various formats, calculating initial *hash* values, uploading them to Google Drive, downloading from different accounts or devices, and re-calculating the *hash* values after transfer. The results show that *hash* values remain identical before and after the *file-sharing* process across all tested *files*, ranging from small text documents to large ISO *files*. These findings indicate that Google Drive reliably maintains data integrity during cross-user and cross-device sharing, with no undetected modifications to *file* contents. This study contributes to a technical understanding of data reliability within modern cloud storage services.

**Keywords:** Data integrity, Google Drive, End-to-end testing, Hash, File sharing, Cloud storage

## **1. PENDAHULUAN**

Transformasi digital yang masif dalam dua dekade terakhir telah membawa perubahan fundamental dalam cara individu dan organisasi menyimpan, mengelola, dan mendistribusikan data. Salah satu perubahan paling signifikan adalah peralihan dari sistem penyimpanan lokal menuju penggunaan layanan penyimpanan berbasis awan (*cloud storage*) seperti Google Drive, Dropbox, OneDrive, dan berbagai platform lainnya. Layanan-layanan ini semakin menjadi tulang punggung dalam aktivitas penyimpanan dan kolaborasi data digital karena menawarkan kemudahan akses, skalabilitas tinggi, serta efisiensi operasional [1], [2]. Dalam konteks ini, tidak mengherankan jika individu hingga organisasi skala besar kini sangat bergantung pada cloud, terutama dalam aktivitas berbagi *file* secara daring yang cepat dan lintas perangkat.

Namun, peningkatan adopsi layanan cloud ini juga membawa tantangan baru, khususnya dalam hal keamanan dan integritas data, terutama saat *file* berpindah dari satu pihak ke pihak lain [3]. Dalam dunia digital, integritas data menjadi aspek krusial karena menjamin bahwa data tidak mengalami perubahan—baik akibat gangguan sistem, kesalahan teknis, maupun serangan siber selama proses penyimpanan maupun transfer *file* [4], [5]. Kegagalan dalam menjaga integritas data dapat menyebabkan konsekuensi serius, termasuk kehilangan informasi penting, manipulasi data, hingga kerugian reputasi.

Sejumlah penelitian terdahulu menekankan pentingnya penerapan mekanisme verifikasi data, seperti penggunaan algoritma *hash*, untuk memvalidasi keutuhan *file*. Fungsi *hash* memungkinkan pengguna untuk membandingkan nilai *hash file* sebelum dan sesudah proses transfer, sehingga dapat mendeteksi apakah terjadi perubahan, sekecil apa pun, pada data yang bersangkutan [1], [6]. Dalam konteks keamanan cloud, pendekatan ini menjadi fondasi utama

untuk menjamin bahwa *file* tetap otentik dan tidak termodifikasi secara tidak sah selama dibagikan antar pengguna.

Beberapa studi, baik di tingkat nasional maupun internasional, juga telah menekankan pentingnya pengujian *end-to-end* sebagai metode untuk mengukur efektivitas *platform cloud* dalam menjaga integritas *file*. Pengujian ini dilakukan dengan cara mengamati apakah nilai *hash file* tetap identik sebelum dan sesudah proses *upload-download* atau berbagi *file* berlangsung, yang secara tidak langsung menjadi indikator keandalan sistem dalam mendeteksi manipulasi data tersembunyi [7].

Google Drive, sebagai salah satu *platform cloud storage* paling populer dan banyak digunakan secara global, memainkan peran strategis dalam mendukung aktivitas berbasis data baik dalam dunia akademik, sektor bisnis, hingga pemerintahan digital [3]. Tidak hanya dikenal karena antarmukanya yang ramah pengguna, Google Drive juga dilengkapi dengan arsitektur keamanan yang kuat, dirancang untuk melindungi *file* dari akses tidak sah maupun perubahan yang tidak terdeteksi [4]. Sejumlah penelitian menunjukkan bahwa layanan ini telah mengadopsi protokol keamanan canggih, yang mencakup enkripsi, autentikasi ganda, serta sistem log yang cermat dalam setiap aktivitas berbagi *file* [1], [8].

Berdasarkan latar belakang tersebut, penelitian ini akan berfokus pada pengujian integritas data melalui pendekatan *end-to-end* dalam proses berbagi *file* menggunakan Google Drive. Studi ini dirancang dengan melakukan eksperimen berupa:

- 1) Pembuatan *file* uji dengan berbagai format dan ukuran
- 2) Penghitungan nilai *hash* sebelum dan sesudah proses berbagi *file*
- 3) Analisis komparatif terhadap hasil *hash* untuk mengidentifikasi kemungkinan perubahan data.

Dengan pendekatan tersebut, diharapkan penelitian ini mampu memberikan kontribusi konkret terhadap pemahaman mengenai keandalan sistem Google Drive dalam menjaga keutuhan data, serta menjadi pijakan awal untuk evaluasi dan pengembangan sistem keamanan cloud storage di masa depan [1], [7].

## 2. Metodologi

Penelitian ini menggunakan metode pengujian eksperimen (*experimental testing method*) dengan pendekatan *end-to-end* yang dilakukan terhadap sistem penyimpanan google drive. Jadi dalam penelitian ini, akan dilakukan pengujian langsung dengan bereksperimen secara nyata dimana beberapa jenis data yang dipilih, akan diuji secara keseluruhan dalam pengujian *end-to-end testing* pada google drive.

Untuk mendapatkan hasil yang lebih representatif, pengujian dilakukan terhadap 8 hingga 10 jenis *file* yang berbeda format, diantaranya *txt*, *omv*, *docx*, *jpg*, *xls*, *png*, *pdf*, *exe*, *mp4*, dan *iso*. Pemilihan berbagai jenis *file* ini bertujuan untuk menguji apakah integritas data tetap terjaga secara konsisten pada berbagai format *file* yang umum digunakan.

Pengujian ini dibagi menjadi 2 bagian yaitu pengujian *hash file* dan pengujian enkripsi dan dekripsi. Dari dua pengujian tersebut, terdapat beberapa tahapan yang harus dilakukan untuk menguji *file* secara keseluruhan.

### 2.1 Pengujian Hash File

Pengujian *hash file* ini bertujuan untuk memastikan keutuhan dan integritas dari *file* yang diuji, yaitu apakah *file* yang diunggah ke Google Drive masih sama setelah diunduh kembali, dalam hal ini *file* tidak berubah sedikit pun.



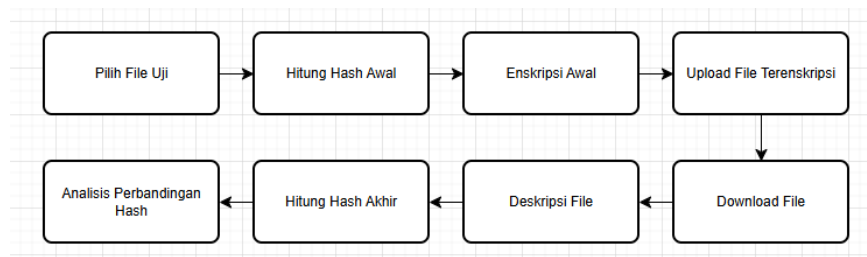
Gambar 1. Alur Pengujian Hash File

Pengujian ini dilakukan dengan menggunakan aplikasi *Hash Checker*, yaitu perangkat lunak yang digunakan untuk menghasilkan nilai *hash* dari sebuah *file* menggunakan algoritma tertentu. Alur dari pengujian *hash file* yaitu:

- Pembuatan *file* uji dengan berbagai format.
- Penghitungan *hash* awal sebelum diunggah.
- Upload* ke Google drive.
- Download file* dari akun lain atau perangkat lain.
- Penghitungan *hash* setelah transfer.
- Analisis perbandingan *hash* (apakah berubah atau tetap sama).

## 2.2 Pengujian Enkripsi dan Dekripsi

Pengujian ini bertujuan untuk meningkatkan keamanan data selama proses berbagi, dan menguji apakah *file* terenkripsi dapat dikembalikan ke bentuk aslinya tanpa kehilangan informasi.



Gambar 2. Alur Pengujian Enkripsi dan Dekripsi

Alur dari pengujian enkripsi dan dekripsi yaitu:

- Pilih *file* uji
- Hitung *hash* awal
- Enkripsi *file*
- Upload file* terenkripsi ke Google Drive
- Download file* dari akun atau perangkat lain
- Dekripsi *file*
- Hitung *hash* hasil dekripsi
- Analisis perbandingan *hash* (apakah berubah atau tetap sama).

### 3. HASIL DAN PEMBAHASAN

Tabel 1. Hasil Pengujian Hash Awal

| No | Nam File                           | Hash Awal                                                        | Link Google Drive                                                                                                                                                                                                                                                                                                     |
|----|------------------------------------|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Teks1.txt                          | 45a93c99dc1af9764fc5442e8861dc0019a2d564d3cd0d39c8b731409f2702c7 | <a href="https://drive.google.com/file/d/1d3qhlSKR1bD1EfZVO7R1LB_jKNfW0I6-/view?usp=sharing">https://drive.google.com/file/d/1d3qhlSKR1bD1EfZVO7R1LB_jKNfW0I6-/view?usp=sharing</a>                                                                                                                                   |
| 2  | statistik.omv                      | 3b5d666abe4e185ff9e72410d287e723a8d43d1a0f1d0d6a426cd5890d69832c | <a href="https://drive.google.com/file/d/1FIUFb8FjpA6cRO4LQ6mKaVu6Cy2c0kr/view?usp=sharing">https://drive.google.com/file/d/1FIUFb8FjpA6cRO4LQ6mKaVu6Cy2c0kr/view?usp=sharing</a>                                                                                                                                     |
| 3  | File gambar.png                    | 08351570b3bd6f17b6e84937c92afa70d2e4fa5c5884d64fa57eab7bb654af45 | <a href="https://drive.google.com/file/d/1A-Kr-3KGipMltkoUAFxQzcJA7wPVlgrD/view?usp=drive_link">https://drive.google.com/file/d/1A-Kr-3KGipMltkoUAFxQzcJA7wPVlgrD/view?usp=drive_link</a>                                                                                                                             |
| 4  | DaVinci Resolve_19.1.3_Windows.exe | f2a175463ee2c73f5156cd8b4abc768bb2f528aedc6b81d6f6af769af23f4d47 | <a href="https://drive.google.com/file/d/11XTPlawKcnKFwMXTab1DQ2IN9Er9PEw1/view?usp=sharing">https://drive.google.com/file/d/11XTPlawKcnKFwMXTab1DQ2IN9Er9PEw1/view?usp=sharing</a>                                                                                                                                   |
| 5  | Video PI.mp4                       | 5f5bc0a77a7d01374991c7f3106a62d75c092313b84c395cc35c0de65fc2434  | <a href="https://drive.google.com/file/d/1Obrbg2A4_mQ1KSeRRupfmsKKJ3s3vNoE/view?usp=sharing">https://drive.google.com/file/d/1Obrbg2A4_mQ1KSeRRupfmsKKJ3s3vNoE/view?usp=sharing</a>                                                                                                                                   |
| 6  | debian-12.9.0-amd64-DVD-1.iso      | d336415ab09c0959d4ef32384637d8b15fcaee12a04154d69bbca8b4442d2aa3 | <a href="https://drive.google.com/file/d/1gSPjG8edhCF-4AE6sc8PYpjsi1N1L0iG/view?usp=sharing">https://drive.google.com/file/d/1gSPjG8edhCF-4AE6sc8PYpjsi1N1L0iG/view?usp=sharing</a>                                                                                                                                   |
| 7  | Kelompok1.pdf                      | 72f69e61dd0a86fef000f4b04316eac513974864b19b8a407aff72135e905f51 | <a href="https://drive.google.com/file/d/1v0Y2bNDj_wZzZddQRlW8chg9hFSkYlsz/view?usp=sharing">https://drive.google.com/file/d/1v0Y2bNDj_wZzZddQRlW8chg9hFSkYlsz/view?usp=sharing</a>                                                                                                                                   |
| 8  | Tugas sistem terdistribusi.docx    | 0611096074de09a6525bde621e8cf8f7d14747844ff8a05a10cf6aa050df7e7f | <a href="https://docs.google.com/document/d/1i5KnvW9bKqaUK4MU3MoK3_6PcGHycLk/edit?usp=sharing&amp;oid=112725336299182628588&amp;rtopof=true&amp;sd=true">https://docs.google.com/document/d/1i5KnvW9bKqaUK4MU3MoK3_6PcGHycLk/edit?usp=sharing&amp;oid=112725336299182628588&amp;rtopof=true&amp;sd=true</a>           |
| 9  | exel.xls                           | 9a2babc758d709fd2a4f2b91833b204734a5ba898ecd7088cd0951dbf2d4676f | <a href="https://docs.google.com/spreadsheets/d/1dcu3PS6EvZh5OfWScIcV8AUzqLc12J7q/edit?usp=sharing&amp;oid=112725336299182628588&amp;rtopof=true&amp;sd=true">https://docs.google.com/spreadsheets/d/1dcu3PS6EvZh5OfWScIcV8AUzqLc12J7q/edit?usp=sharing&amp;oid=112725336299182628588&amp;rtopof=true&amp;sd=true</a> |
| 10 | gambar 2.jpg                       | 7bbd98a7593d99e1b8a74e1836e4cc7335c251af1a1ac2af7d1e88fce18a227d | <a href="https://drive.google.com/file/d/1booYPvfAFy_ZPf6IXHCTLriNZ3kXOWlp/view?usp=sharing">https://drive.google.com/file/d/1booYPvfAFy_ZPf6IXHCTLriNZ3kXOWlp/view?usp=sharing</a>                                                                                                                                   |

Berdasarkan tabel di atas, dapat disimpulkan bahwa hasil dari pengujian *end-to-end* terhadap proses unggah dan unduh *file* di Google Drive menunjukkan bahwa semua *file*, baik berukuran kecil maupun besar, mempertahankan nilai *hash* yang identik sebelum dan sesudah proses transfer. *File* seperti dokumen teks, gambar, video, hingga *file* instalasi berukuran besar seperti DaVinci Resolve\_19.1.3\_Windows.exe tidak mengalami perubahan data yang terdeteksi. Bahkan pada skenario yang melibatkan proses enkripsi dengan 7zip sebelum unggah dan dekripsi setelah unduh, nilai *hash* tetap konsisten dengan *file* asli sebelum enkripsi dilakukan.

Dari Tabel 2, menunjukkan bahwa pada simbol ✓ hasil *hash* nya itu sama. Konsistensi nilai *hash* menunjukkan bahwa tidak terjadi modifikasi atau korupsi data selama proses unggah dan unduh di Google Drive. Hal ini menandakan bahwa sistem penyimpanan dan transmisi data yang digunakan oleh Google Drive memiliki keandalan yang tinggi, terutama dalam menjamin integritas data digital. Selain itu, penggunaan enkripsi tidak mengganggu integritas *file*, menunjukkan kompatibilitas antara protokol keamanan pengguna dengan sistem Google Drive. Hasil ini mengindikasikan bahwa layanan cloud ini mampu mendukung praktik keamanan data modern tanpa menimbulkan gangguan terhadap isi *file*.

Tabel 2. Hasil Pengujian Hash Akhir

| No | Nama File                          | Hash Akhir                                                       | Uji Coba |    |    |    |    |
|----|------------------------------------|------------------------------------------------------------------|----------|----|----|----|----|
|    |                                    |                                                                  | S1       | S2 | S3 | S4 | S5 |
| 1  | Teks1.txt                          | 45a93c99dc1af9764fc5442e8861dc0019a2d564d3cd0d39c8b731409f2702c7 | ✓        | ✓  | ✓  | ✓  | ✓  |
| 2  | statistik.omv                      | 3b5d666abe4e185ff9e72410d287e723a8d43d1a0f1d0d6a426cd5890d69832c | ✓        | ✓  | ✓  | ✓  | ✓  |
| 3  | File gambar.png                    | 08351570b3bd6f17b6e84937c92afa70d2e4fa5c5884d64fa57eab7bb654af45 | ✓        | ✓  | ✓  | ✓  | ✓  |
| 4  | DaVinci Resolve_19.1.3_Windows.exe | f2a175463ee2c73f5156cd8b4abc768bb2f528aedc6b81d6f6af769af23f4d47 | ✓        | ✓  | ✓  | ✓  | ✓  |

| No | Nama File                      | Hash Akhir                                                       | Uji Coba |    |    |    |    |
|----|--------------------------------|------------------------------------------------------------------|----------|----|----|----|----|
|    |                                |                                                                  | S1       | S2 | S3 | S4 | S5 |
| 5  | Video Pl.mp4                   | 5f5bc0a77a7d01374991cff73106a62d75c092313b84c395cc35c0de65fc2434 | ✓        | ✓  | ✓  | ✓  | ✓  |
| 6  | debian-12.9.0-amd64-DVD-1.iso  | d336415ab09c0959d4ef32384637d8b15fcaee12a04154d69bbca8b4442d2aa3 | ✓        | ✓  | ✓  | ✓  | ✓  |
| 7  | Kelompok1.pdf                  | 72f69e61dd0a86fef000f4b04316eac513974864b19b8a407aff72135e905f51 | ✓        | ✓  | ✓  | ✓  | ✓  |
| 8  | Tugassistem terdistribusi.docx | 0611096074de09a6525bde621e8cf87d14747844ff8a05a10cf6aa050df7e7f  | ✓        | ✓  | ✓  | ✓  | ✓  |
| 9  | exel.xls                       | 9a2babc758d709fd2a4f2b91833b204734a5ba898ecd7088cd0951dbf2d4676f | ✓        | ✓  | ✓  | ✓  | ✓  |
| 10 | gambar 2.jpg                   | 7bbd98a7593d99e1b8a74e1836e4cc7335c251af1a1ac2af7d1e88fce18a227d | ✓        | ✓  | ✓  | ✓  | ✓  |

Hasil uji coba yang dilakukan melalui metode pengujian *end-to-end* menunjukkan bahwa Google Drive secara konsisten mampu menjaga integritas data selama proses berbagi *file* antar akun dan perangkat. Hal ini terlihat dari konsistensi nilai *hash file* yang diuji sebelum dan sesudah proses unggah dan unduh, tanpa menunjukkan adanya perbedaan atau penyimpangan sedikit pun [9]. Nilai *hash* yang identik pada seluruh jenis *file*, baik yang berukuran kecil seperti .txt dan .jpg, maupun yang berukuran besar seperti .mp4, .iso, dan .exe, menunjukkan bahwa Google Drive menerapkan mekanisme penyimpanan dan transmisi *file* yang mampu mencegah terjadinya korupsi data ataupun manipulasi tidak sah.

Uji coba ini memperlihatkan bahwa *hash file*, sebagai representasi digital dari isi *file*, menjadi indikator utama dalam menguji integritas data. Seperti ditegaskan oleh [4], fungsi *hash* kriptografis seperti SHA-256 atau SHA-512 mampu mendeteksi bahkan perubahan sekecil satu bit pada data digital, sehingga sangat ideal digunakan untuk memverifikasi keutuhan *file* pada sistem penyimpanan awan [10]. Dalam konteks ini, penggunaan *hash checker* dalam penelitian ini memberikan landasan teknis yang kuat untuk menyatakan bahwa *file* tetap utuh setelah melalui proses transfer via Google Drive. Hal ini sangat penting, terutama ketika pengguna melakukan kolaborasi *file* di lingkungan kerja, pendidikan, atau sektor bisnis yang menuntut akurasi data tinggi.

Selain itu, hasil pengujian terhadap *file* yang dienkripsi menggunakan 7zip dan didekripsi kembali setelah diunduh menunjukkan bahwa proses enkripsi dan dekripsi tidak memengaruhi nilai *hash file* asli. Ini menandakan bahwa praktik pengamanan tambahan melalui enkripsi tidak bertentangan dengan integritas *file* selama prosedur berbagi dilakukan dengan tepat. Integritas *file* pada layanan cloud tetap dapat dipertahankan jika pengguna menerapkan enkripsi berbasis algoritma yang tidak mengubah struktur dasar *file* saat proses dekripsi dilakukan dengan benar [11].

Google Drive sendiri sebagai layanan penyimpanan berbasis awan telah mengadopsi berbagai fitur pengamanan, seperti enkripsi data saat diam (at rest) dan saat transit (in transit), serta sistem autentikasi ganda (2FA) untuk melindungi akses pengguna. Disebutkan bahwa tingkat kepercayaan pengguna terhadap keamanan Google Drive cukup tinggi, terutama karena sistem ini mampu mengurangi risiko perubahan *file* secara tidak terdeteksi saat *file* berpindah antar pengguna [3]. Penelitian ini semakin memperkuat pernyataan tersebut, karena hasil uji coba membuktikan bahwa *file* tetap memiliki *hash* yang konsisten bahkan ketika diakses dari perangkat dan akun yang berbeda.

Dengan mempertimbangkan hasil eksperimen terhadap sepuluh jenis *file* yang bervariasi format dan ukurannya, dapat disimpulkan bahwa Google Drive tidak hanya menyediakan layanan berbagi *file* yang efisien, tetapi juga menjamin keandalan dan keutuhan *file* tersebut. Konsistensi ini menunjukkan adanya mekanisme verifikasi dan manajemen data yang matang di balik infrastruktur cloud Google, sehingga setiap *file* yang diunggah tidak dimodifikasi secara

implisit oleh sistem. Temuan ini memiliki dampak praktis yang besar, terutama dalam lingkungan profesional di mana *file* seperti dokumen hukum, laporan keuangan, atau data hasil penelitian harus tetap tidak berubah meskipun dibagikan secara daring.

Keandalan ini juga dapat dijadikan acuan dalam pengembangan sistem keamanan data berbasis cloud di institusi pendidikan dan pemerintahan. Salah satu tantangan utama dalam layanan cloud adalah risiko data leakage dan modifikasi data akibat kegagalan sistem atau serangan pihak ketiga [1]. Namun, hasil penelitian ini membuktikan bahwa, setidaknya dalam konteks integritas data saat berbagi *file*, Google Drive menunjukkan performa yang sangat baik dan stabil.

Di sisi lain, penelitian ini juga menunjukkan pentingnya keterlibatan pengguna dalam menjaga integritas *file*, yaitu dengan melakukan verifikasi *hash* sebelum dan sesudah proses unggah-unduh [12]. Kesadaran ini penting untuk meningkatkan data hygiene, yaitu kebiasaan menjaga dan mengelola *file* digital dengan prosedur yang aman. Dengan demikian, integritas data bukan hanya tanggung jawab penyedia layanan cloud, tetapi juga para penggunanya. Dalam jangka panjang, adopsi metode seperti ini diharapkan dapat menjadi bagian dari kebijakan standar keamanan digital pada organisasi yang mengelola dokumen penting.

Dari keseluruhan hasil, tidak ditemukan adanya perubahan nilai *hash* dari seluruh *file* yang diuji, bahkan setelah melalui lima skenario uji coba yang melibatkan kombinasi akun, perangkat, serta skenario enkripsi [13], [14]. Hal ini menandakan bahwa Google Drive sangat layak digunakan sebagai platform berbagi *file* yang mengutamakan keutuhan dan keamanan *file*. Namun, perlu digarisbawahi bahwa integritas *file* yang terjamin tidak serta merta mencakup aspek privasi atau kerahasiaan isi *file*, sehingga enkripsi tambahan tetap disarankan jika *file* bersifat sangat sensitif.

#### 4. KESIMPULAN DAN SARAN

Penelitian ini membuktikan bahwa Google Drive mampu menjaga integritas data selama proses berbagi *file* antar perangkat dan antar akun pengguna, sebagaimana ditunjukkan oleh konsistensi nilai *hash* pada *file* sebelum dan sesudah proses transfer. Hasil ini berlaku untuk berbagai format dan ukuran *file*, termasuk dalam skenario dengan penerapan enkripsi dan dekripsi. Hal ini menunjukkan bahwa layanan penyimpanan awan ini dapat diandalkan dari sisi keutuhan data, menjadikannya relevan tidak hanya bagi pengguna individu, tetapi juga organisasi yang membutuhkan jaminan keamanan dan integritas *file* digital. Studi ini memperkuat pemahaman teknis bahwa sistem *cloud* modern, jika dirancang dengan baik, mampu menjawab tantangan integritas data dalam ekosistem berbagi *file* lintas jaringan dan perangkat.

Google Drive sebagai layanan *cloud storage* terbukti mampu menjaga integritas data selama proses unggah dan unduh dalam skenario berbagi *file*. Penggunaan metode *hash* dan enkripsi menegaskan bahwa data tetap utuh selama proses transfer [15]. Penelitian ini mendukung penggunaan Google Drive dalam skenario yang membutuhkan keandalan transfer data, termasuk untuk *file* berukuran besar.

#### REFERENSI

- [1] M. Sravani And M. Krishna Murthy, "Reduction Of Data Leakage In Distributed Cloud Storage Systems Using Distributed Cloud Guard (Dcg)," *Indian Journal Of Computer Science And Engineering*, Vol. 14, No. 3, Pp. 444–450, Jun. 2023, Doi: 10.21817/Indjcse/2023/V14i3/231403014.
- [2] M. A. Á. M. F. I. F. K. B. S. O. A. M. H. Thar Baker, "A Secure Fog-Based Platform For Scada-Based Iot Critical Infrastructure," 2019.

- [3] L. Hasimu, L. Wiry Mardan, P. Studi Teknologi Informasi, And I. Teknologi Dan Bisnis Muhammadiyah Wakatobi, “Kesadaran Pengguna Terhadap Keamanan Penyimpanan Data Dalam Google Drive Studi Kasus Pada Dinas Komunikasi Kabupaten Wakatobi.”
- [4] M. Z. Hasan, N. Sarwar, I. Alam, M. Z. Hussain, A. A. Siddiqui, And A. Irshad, “Data Recovery And Backup Management: A Cloud Computing Impact,” In *Proceedings - 2023 Ieee International Conference On Emerging Trends In Engineering, Sciences And Technology, Ices And T 2023*, Institute Of Electrical And Electronics Engineers Inc., 2023. Doi: 10.1109/Icest56843.2023.10138852.
- [5] G. Mirjalily And Z. Luo, “Optimal Network Function Virtualization And Service Function Chaining: A Survey,” *Chinese Journal Of Electronics*, Vol. 27, No. 4, Pp. 704–717, Jul. 2018, Doi: 10.1049/Cje.2018.05.008.
- [6] R. Karim, “End-To-End Qos Computation For Vertical Service Composition In The Cloud.”
- [7] M. Ratna Manikam, “Perancangan Sistem Cloud Storage Data Siswa Pada Smp Islam Al Hikma Berbasis Website.”
- [8] M. Uddin, A. Khalique, And A. K. Juman, “Next-Generation Blockchain-Enabled Virtualized Cloud Security Solutions: Review And Open Challenges,” Nov. 17, 2020. Doi: 10.36227/Techrxiv.13233887.V1.
- [9] R. Taqiyyah And A. R. Adriansyah, “Jurnal Informatika Terpadu Visualisasi Implementasi Autentifikasi Digital Signature Menggunakan Fungsi *Hash* Pada *File* Digital,” *Jurnal Informatika Terpadu*, Vol. 6, No. 1, Pp. 7–13, 2020, [Online]. Available: <https://Journal.Nurulfikri.Ac.Id/Index.Php/Jit>
- [10] M. Anum Fadhilah *Et Al.*, “Algoritme *Hashing* Sha-512 Pada Sistem Halaman Sign Up Java.”
- [11] M. Ratna Manikam, “Perancangan Sistem Cloud Storage Data Siswa Pada Smp Islam Al Hikma Berbasis Website,” 2024.
- [12] J. Warta, M. Khaerudin, And A. Hidayat, “Ikram: Jurnal Ilmu Komputer Al Muslim Sistem Keamanan Transaksi Penjualan Baja Dengan Menerapkan Algoritma *Hashing* Pada Pt. Bakrie Metal Industries,” Vol. 1, 2025.
- [13] S. Anam And H. Hayadi, “Analisis Peran Algoritma Dalam Pengaturan Dan Perhitungan Big Data Yang Kompleks Analyze The Role Of Algorithms In Complex Big Data Organizations And Calculations.”
- [14] A. Kusyanti, I. P. Agrabita Wiguna, And F. Andri Bakhtiar, “Implementasi Algoritme Spongnet Sebagai Algoritme *Hashing* Untuk Integritas Pada Modul Komunikasi Lora,” *Jurnal Teknologi Informasi Dan Ilmu Komputer*, Vol. 10, No. 6, Pp. 1311–1318, Dec. 2023, Doi: 10.25126/Jtiik.2023107119.
- [15] T. Zeng *Et Al.*, “Deep *Hashing* And Attention Mechanism-Based Image Retrieval Of Osteosarcoma Scans For Diagnosis Of Bone Cancer,” *J Bone Oncol*, Vol. 49, Dec. 2024, Doi: 10.1016/J.Jbo.2024.100645.