Analisis Komparatif Efektivitas Client-Side Encryption Cryptomator dan Rclone Crypt pada Google Drive

I Komang Wahyu Ambara Putra [1], Bagus Gede Krishna Yudistira [2]
[1,2] Ilmu Komputer / Fakultas Teknik dan Kejuruan
[1,2] Universitas Pendidikan Ganesha
Jalan Udayana No.11 Singaraja, Buleleng, Bali 81116
wahyu.ambara@student.undiksha.ac.id [1], krishna.yudistira@undiksha.ac.id [2]

Abstrak. Penggunaan *cloud storage* seperti *Google Drive* yang semakin masif dihadapkan pada tantangan keamanan data. *Client-Side Encryption* (CSE) menjadi solusi penting untuk melindungi privasi pengguna, namun studi komparatif mengenai efektivitas perangkat lunak CSE masih terbatas. Penelitian ini melakukan analisis komparatif dengan pendekatan eksperimental untuk mengevaluasi efektivitas enkripsi *client-side Cryptomator* dan *Rclone Crypt.* Analisis mencakup parameter kinerja seperti kecepatan enkripsi dan unggah data, perubahan ukuran file, visibilitas metadata, aksesibilitas, portabilitas, dan kecepatan unduh data. Hasil pengujian menunjukkan *Rclone Crypt* secara konsisten dan signifikan secara statistik lebih unggul dalam hal kecepatan proses dan *overhead* ukuran file kurang dari setengah yang dihasilkan *Cryptomator.* Sebaliknya, *Cryptomato*r menawarkan kemudahan penggunaan dan portabilitas yang lebih superior bagi pengguna umum, serta mampu menyamarkan struktur folder secara total untuk privasi yang lebih baik. Kesimpulan utama dari penelitian ini adalah adanya *trade-off* fundamental antara performa dan kemudahan penggunaan. *Rclone Crypt* direkomendasikan untuk pengguna teknis yang memprioritaskan kecepatan dan efisiensi, sedangkan Cryptomator menjadi solusi yang lebih tepat bagi pengguna non-teknis yang mengutamakan kesederhanaan dan privasi struktural. Penelitian ini memberikan panduan praktis bagi pengguna untuk memilih solusi CSE yang sesuai dengan kebutuhan teknis dan preferensi pengguna.

Kata Kunci: CSE, *Cloud_Storage, Cryptomator, Rclone_Crypt*

1 Pendahuluan

Transformasi digital global telah mendorong perubahan signifikan dalam cara individu dan institusi mengelola, menyimpan, serta mengakses data. Salah satu teknologi utama yang menjadi tulang punggung transformasi ini adalah *cloud storage*, yang dapat didefinisikan sebagai teknologi yang memungkinkan penyimpanan, pengolahan, dan akses data secara online [1]. Salah satu layanan *cloud storage* yaitu *Google Drive* yang memungkinkan pengguna menyimpan data secara online dengan fleksibilitas tinggi, akses lintas perangkat, serta kemampuan berbagi dan berkolaborasi secara *real-time.* Kemudahan ini menjadikan cloud storage sebagai pilihan utama dalam ekosistem manajemen informasi modern.

Di Indonesia, pemanfaatan *Google Drive* semakin meluas, khususnya dalam dunia pendidikan. *Google Drive* telah digunakan sebagai bagian dari sistem repositori digital yang mendukung efisiensi dan efektivitas pengelolaan dokumen akademik dan administratif di lingkungan kampus [2]. Dalam konteks pembelajaran, penggunaan *Google Drive* juga terlihat dalam integrasinya dengan platform seperti *Google Classroom*, yang membantu proses pembelajaran jarak jauh [3]. Namun di balik manfaat tersebut, muncul tantangan besar yang tidak bisa diabaikan, yaitu isu keamanan data digital yang tersimpan di layanan *cloud storage.*

Berbagai studi telah menyoroti bahwa isu keamanan seperti keandalan dan privasi menjadi salah satu kelemahan utama dan penyebab keraguan dalam mengadopsi layanan berbasis *cloud storage* secara penuh [4]. Keamanan data menjadi perhatian utama dalam pemanfaatan layanan ini, khususnya terkait risiko akses tidak sah, kebocoran informasi, hingga potensi pengawasan oleh pihak ketiga. Berbagai ancaman keamanan, mulai dari pelanggaran privasi, kebocoran informasi, hingga penyalahgunaan data untuk tujuan seperti penyebaran informasi palsu [5], menggarisbawahi pentingnya kontrol pengguna atas data mereka.

Dari perspektif hukum, urgensi perlindungan data pribadi juga telah menjadi sorotan penting, terlebih karena data pribadi merupakan aset yang sangat penting sementara cara memperolehnya semakin mudah di era digital saat ini [6]. Oleh karena itu, pendekatan *client-side encryption* (CSE) menjadi sangat relevan, di mana proses enkripsi dan dekripsi dilakukan langsung di sisi pengguna, sehingga hanya pengguna yang memiliki akses terhadap data mereka. Pemilihan teknik CSE yang tepat dapat memberikan dampak signifikan terhadap keamanan, efisiensi, dan usabilitas sebuah sistem, yang menjadikannya sebuah tantangan praktis dalam komputasi awan [7]. Untuk menerapkan CSE, berbagai perangkat lunak telah dikembangkan dengan pendekatan yang berbeda.

ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)

Di antara solusi yang tersedia, *Cryptomator* menonjol sebagai perangkat lunak *open-source* yang populer karena antarmuka grafisnya yang intuitif. Cryptomator menyediakan mekanisme enkripsi transparan yang kompatibel dengan berbagai layanan cloud storage, memungkinkan pengguna dari berbagai latar belakang teknis untuk mengamankan file mereka dengan mudah sebelum diunggah ke *cloud storage*. Di sisi lain, terdapat *Rclone Crypt*, sebuah fitur dari alat sinkronisasi baris perintah *Rclone*, yang juga menerapkan CSE. *Rclone Crypt* dikenal di kalangan pengguna teknis karena fleksibilitas, kinerja tinggi, dan kemampuannya untuk diotomatisasi, menawarkan pendekatan yang lebih kuat dan terkontrol bagi mereka yang familiar dengan *command-line.*

Meskipun konsep *client-side encryption* telah dikenal luas, kajian yang membandingkan efektivitas berbagai alat CSE secara praktis dalam layanan seperti *Google Drive* masih terbatas, terutama di Indonesia. Hal ini sejalan dengan pandangan bahwa *cloud computing* masih merupakan bidang penelitian yang terus berkembang dalam berbagai dimensi [8]. Kebutuhan untuk mengatasi celah keamanan ini mendorong adanya sebuah terobosan pengembangan teknologi [9], salah satunya melalui analisis komparatif terhadap efektivitas *Cryptomator* dan *Rclone Crypt* dalam meningkatkan keamanan dan efisiensi penggunaan *Google Drive.*

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis dan membandingkan efektivitas dua perangkat lunak *client-side encryption, yakni Cryptomator* dan *Rclone Crypt*, dalam konteks penggunaan *Google Drive*. Evaluasi dilakukan melalui pendekatan eksperimental berdasarkan parameter performa dan keamanan, guna memberikan panduan praktis bagi pengguna dalam memilih solusi enkripsi yang sesuai dengan kebutuhan dan preferensi masing-masing.

2 Metodologi Penelitian

2.1 Pendekatan Penelitian

Penelitian ini menggunakan pendekatan eksperimental untuk menganalisis dan membandingkan secara langsung efektivitas *client-side encryption Cryptomator* dan *Rclone Crypt* dalam penggunaan *Google Drive*. Selain eksperimen, penelitian ini didukung oleh studi literatur, di mana studi literatur merupakan sebuah metode yang sistematis, eksplisit dan reprodusibel untuk melakukan identifikasi, evaluasi dan sintesis terhadap karya-karya hasil penelitian [10]. Pendekatan ini sejalan dengan praktik penelitian pada umumnya, di mana pengumpulan data untuk studi literatur dilaksanakan dengan cara meneliti berbagai jurnal, media *online*, atau dokumen lain yang relevan dengan topik penelitian [11].

2.2 Desain dan Lingkungan Eksperimen

Perangkat lunak utama yang diuji adalah *Cryptomator* versi 1.16.0 dan Rclone versi 1.69.2. *Cryptomator* mengimplementasikan enkripsi berlapis menggunakan algoritma AES-256 dengan mode *Galois/Counter Mode* (GCM) untuk mengenkripsi isi file dan AES-SIV untuk nama file, yang memberikan perlindungan kuat terhadap modifikasi data dan serangan *chosen-plaintext*. Metode pengelolaan kuncinya berbasis kata sandi pengguna yaitu kata sandi diolah menggunakan fungsi derivasi kunci untuk menghasilkan kunci utama yang kemudian mengenkripsi masterkey untuk setiap vault. Keamanan model ini sangat bergantung pada kekuatan kata sandi yang dipilih oleh pengguna. Di sisi lain, Rclone Crypt juga menggunakan enkripsi AES-256 (dengan mode GCM) yang diautentikasi. Metode pengelolaan kuncinya berbeda, di mana kunci enkripsi untuk data dan nama file dihasilkan dari kombinasi kata sandi dan salt yang kemudian disimpan secara terenkripsi di dalam file konfigurasi rclone.conf. Potensi kerentanan utama pada *Rclone Crypt* terletak pada pengamanan file rclone.conf itu sendiri, karena siapa pun yang mendapatkan akses ke file ini dan berhasil mendekripsinya dapat mengakses seluruh data. Perbedaan fundamental ini menyoroti bahwa Cryptomator mengelola kunci secara terdesentralisasi per vault, sementara Rclone mengelolanya secara terpusat.

Proses pengujian juga dilakukan pada *Google Drive* dengan antarmuka web standar pada browser Google Chrome versi 137.0.7151.69. Seluruh pengujian dilakukan menggunakan koneksi internet dengan kecepatan yang terukur melalui *Speedtest by Ookla*. Kecepatan unduh rata-rata adalah 12 Mbps dan kecepatan unggah rata-rata adalah 4 Mbps. Konsistensi jaringan dijaga dengan tidak menjalankan aplikasi lain yang membutuhkan bandwidth

ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)

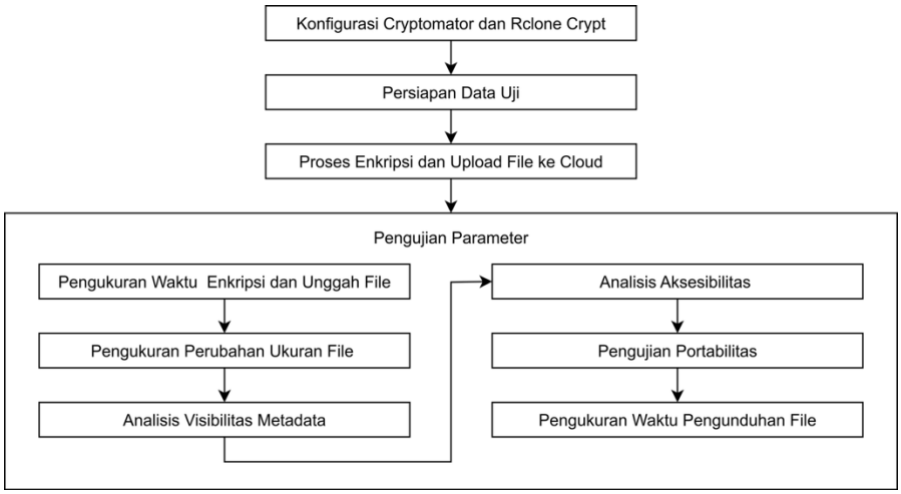
selama proses pengujian. Objek penelitian terdiri dari tiga jenis file yang umum digunakan yaitu dokumen (PDF), gambar (JPG), dan arsip (ZIP). Untuk menjaga integritas dan etika penelitian, seluruh file uji yang digunakan merupakan data dummy (tidak sensitif) yang disiapkan khusus untuk keperluan eksperimen dan tidak mengandung informasi pribadi atau rahasia. Masing-masing jenis file diuji dalam dua variasi ukuran sesuai Tabel 1.

Tabel 1. Data Pengujian

Nomor	File	Ukuran
1	PDF 1	1.071 KB
2	PDF 2	17.733 KB
3	JPG 1	1.972 KB
4	JPG 2	10.863 KB
5	ZIP 1	5.178 KB
6	ZIP 2	50.032 KB

2.3 Prosedur Pengujian

Langkah-langkah yang dilakukan dalam penelitian ini dapat dilihat pada Gambar 1.



Gambar. 1. Prosedur Pengujian

1. Konfigurasi *Cryptomator* dan *Rclone Crypt*
   Pada tahap ini dilakukan konfigurasi aplikasi *Cryptomator* dan *Rclone Crypt* agar siap digunakan dalam proses pengujian.
2. Persiapan Data Uji
   Tiga jenis file digunakan sebagai data uji, yaitu PDF, JPG, dan ZIP, masing-masing dengan dua variasi ukuran sesuai pada Tabel 1.
3. Proses Enkripsi dan Unggah File ke *Cloud*
   Untuk *Cryptomator,* proses enkripsi dilakukan dengan membuat *vault* khusus, kemudian file yang telah dienkripsi diunggah ke *Google Drive*. Sementara itu, pada *Rclone Crypt,* file dienkripsi dan diunggah langsung ke *Google Drive* menggunakan perintah rclone copy.
4. Pengujian Parameter
   Terdapat enam parameter yang digunakan dalam pengujian, dengan penjelasan sebagai berikut:
   a. Pengukuran Waktu Enkripsi dan Unggah File
      Untuk memastikan validitas dan reliabilitas data, waktu enkripsi dan unggah setiap file diukur sebanyak tiga kali menggunakan stopwatch digital. Nilai yang dicatat merupakan rata-rata dari ketiga pengukuran tersebut, disertai dengan standar deviasi.
   b. Pengukuran Perubahan Ukuran File
      Perubahan ukuran file diamati dengan membandingkan ukuran file sebelum dan sesudah proses unggah ke *Google Drive.*

ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)

c. Analisis Visibilitas Metadata
Pemeriksaan dilakukan terhadap metadata file yang diunggah ke *Google Drive*, seperti nama asli, ukuran asli, dan tanggal modifikasi, untuk mengetahui apakah informasi tersebut masih dapat diakses.

d. Analisis Aksesibilitas
Analisis ini bertujuan untuk mengetahui apakah file yang telah dienkripsi dapat diakses langsung melalui antarmuka web *Google Drive* tanpa proses dekripsi.

e. Pengujian Portabilitas
Portabilitas diuji dengan mengevaluasi kemudahan akses data terenkripsi dari perangkat lain. Pengujian dilakukan menggunakan dua unit laptop untuk mensimulasikan penggunaan pada perangkat yang umum dimiliki oleh pengguna. Laptop A (perangkat utama) menggunakan prosesor Intel Celeron, RAM 4 GB, dan SSD 256 GB. Laptop B (perangkat sekunder) menggunakan prosesor Intel Core i3-13400, RAM 8 GB, dan SSD 512 GB. Kedua laptop berjalan pada sistem operasi Windows 11.

Kriteria untuk mengevaluasi portabilitas (disajikan pada Tabel 5) dirumuskan dengan mengoperasionalkan konsep kualitas perangkat lunak berdasarkan standar internasional ISO/IEC 25010:2023 [12]. Standar ini mendefinisikan portabilitas sebagai tingkat efektivitas dan efisiensi suatu sistem atau komponen saat ditransfer dari satu lingkungan ke lingkungan lain. Untuk mengukur ini secara praktis, penelitian ini berfokus pada dua sub-karakteristik yang relevan yaitu instalabilitas (kemudahan instalasi dan konfigurasi) dan adaptabilitas (kemampuan beradaptasi dengan lingkungan baru).

f. Pengukuran Waktu Pengunduhan File
Waktu yang dibutuhkan untuk mengunduh file terenkripsi diukur sebanyak tiga kali. Nilai rata-rata dari ketiga pengukuran tersebut digunakan untuk meningkatkan akurasi hasil pengujian.

2.4 Teknik Analisis Data

Analisis data dalam penelitian ini menggunakan pendekatan kuantitatif dan kualitatif. Data numerik dari pengujian kinerja dianalisis secara deskriptif untuk menghasilkan nilai rata-rata dan standar deviasi, serta dianalisis secara inferensial menggunakan Uji-t Sampel Independen untuk menguji signifikansi statistik. Sementara itu, parameter non-numerik seperti visibilitas metadata dan portabilitas dianalisis secara kualitatif berdasarkan observasi.

Dalam merancang sebuah solusi keamanan, penting untuk tidak hanya memastikan aspek privasi data, tetapi juga merancang skema yang efisien, karena efisiensi sebuah sistem bergantung pada bagaimana sumber daya dialokasikan kepada pengguna [13]. Atas dasar itu, kesimpulan akhir ditarik dengan mensintesis seluruh hasil, baik kuantitatif maupun kualitatif, untuk memberikan rekomendasi yang berimbang mengenai keunggulan masing-masing perangkat lunak sesuai profil pengguna.

3 Hasil dan Pembahasan

3.1 Pengukuran Waktu Enkripsi dan Unggah File

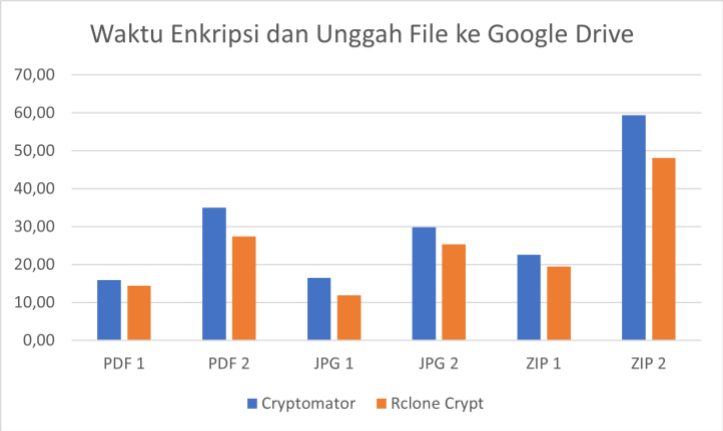
Bagian ini menyajikan dan membahas hasil pengukuran waktu yang dibutuhkan oleh *Cryptomator* dan *Rclone Crypt* untuk melakukan proses enkripsi file dan mengunggahnya secara penuh ke *Google Drive*. Parameter ini krusial untuk menilai efisiensi dan kinerja dari kedua perangkat lunak. Data kuantitatif hasil pengukuran ini disajikan dalam bentuk tabel dan diagram batang untuk mempermudah perbandingan. Pengukuran dilakukan sebanyak tiga kali untuk setiap file, kemudian dihitung nilai rata-rata dan standar deviasinya untuk memastikan validitas dan reliabilitas data. Tabel 2 menyajikan data numerik hasil pengukuran, sementara Gambar 2 memvisualisasikan perbandingan nilai rata-rata dari kedua perangkat lunak.

Tabel 2. Waktu Enkripsi dan Unggah File ke Google Drive

Nomor	File	Cryptomator (Detik)		Rclone Crypt (Detik)		Uji T	
		Rata-rata	Standar Deviasi	Rata-rata	Standar Deviasi	Statistik t	Nilai p
1	PDF 1	15,88	0,59	14,15	0,53	3,78	0,0194
2	PDF 2	34,96	0,84	29,72	0,72	8,24	0,0011
3	JPG 1	16,20	0,68	11,87	0,73	7,49	0,0016

ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)

Nomor	File	Cryptomator (Detik)		Rclone Crypt (Detik)		Uji T	
		Rata-rata	Standar Deviasi	Rata-rata	Standar Deviasi	Statistik t	Nilai p
4	JPG 2	30,12	0,67	25,04	0,63	9,55	0,0006
5	ZIP 1	22,60	0,67	19,54	0,51	7,42	0,0017
6	ZIP 2	59,34	0,56	49,80	0,56	20,96	0,00003



Gambar. 2. Waktu Enkripsi dan Unggah File ke Google Drive

Berdasarkan data pada Tabel 2, dapat disimpulkan bahwa Rclone Crypt secara konsisten menunjukkan kinerja yang lebih cepat dibandingkan Cryptomator pada semua skenario pengujian. Analisis statistik menggunakan Uji-t Sampel Independen mengonfirmasi bahwa perbedaan kinerja ini signifikan secara statistik (p<,05) untuk seluruh file yang diuji. Keunggulan Rclone Crypt menjadi semakin jelas pada file berukuran besar. Sebagai contoh, untuk file ZIP 2, perbedaan waktu antara Cryptomator dan Rclone Crypt terbukti sangat signifikan yaitu t(4)=20,96,p<,00003. Selain itu, nilai standar deviasi yang rendah pada semua pengujian mengindikasikan bahwa data yang dihasilkan memiliki tingkat reliabilitas yang tinggi.

3.2 Pengukuran Perubahan Ukuran File

Parameter ini menguji efisiensi penggunaan ruang penyimpanan dari kedua perangkat lunak dengan mengukur penambahan ukuran file setelah proses enkripsi. Hasil perbandingan ukuran file sebelum dan sesudah proses enkripsi, beserta perhitungan overhead dalam format persentase, disajikan secara rinci pada Tabel 3.

Tabel 3. Perubahan Ukuran File

Nomor	File	Ukuran Asli (KB)	Cryptomator (KB)	Overhead Cryptomator	Rclone Crypt (KB)	Overhead Rclone Crypt
1	PDF 1	1,071	1,072	0,093%	1,072	0,093%
2	PDF 2	17,733	17,749	0,090%	17,738	0,028%
3	JPG 1	1,972	1,974	0,101%	1,972	0,000%
4	JPG 2	10,863	10,872	0,083%	10,866	0,028%
5	ZIP 1	5,178	5,183	0,097%	5,18	0,039%
6	ZIP 2	50,032	50,075	0,086%	50,045	0,026%
	Rata-rata		0,092%		0,036%	

Dari data tersebut, dapat diketahui bahwa kedua perangkat lunak menghasilkan overhead yang secara umum sangat kecil, menunjukkan efisiensi yang baik. *Rclone Crypt* secara konsisten menghasilkan *overhead* yang lebih rendah dibandingkan *Cryptomator* pada hampir semua file uji. Rata-rata overhead yang dihasilkan oleh *Rclone Crypt* adalah 0,036%, kurang dari setengah rata-rata *overhead Cryptomator* yang sebesar 0,092%. Perlu dicatat pula pada kasus file JPG 1, *Rclone Crypt* mampu mengenkripsi file dengan overhead 0,000%, artinya hampir tidak ada penambahan ukuran sama sekali.

Perbedaan efisiensi *overhead* ini berasal dari perbedaan fundamental dalam arsitektur enkripsi kedua perangkat lunak. *Cryptomator* bekerja dengan menciptakan sebuah *vault.* Selain mengenkripsi konten file,

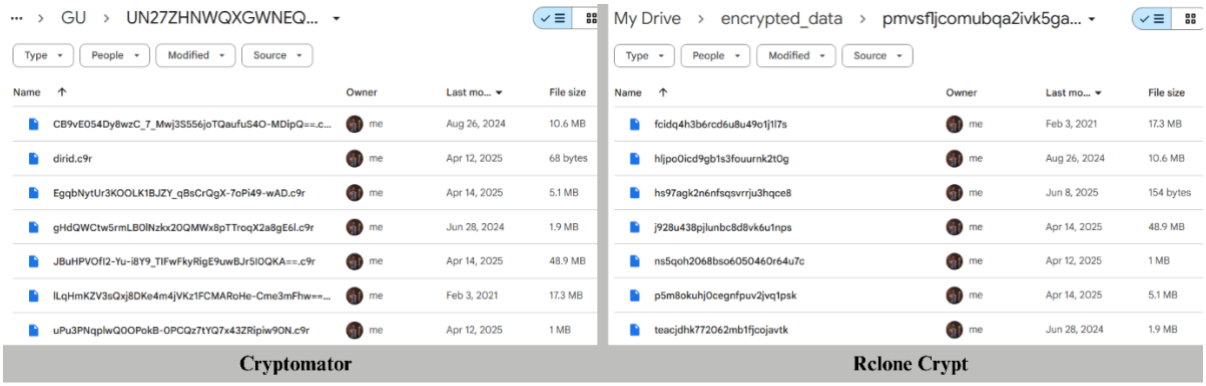
ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)

Cryptomator juga mengenkripsi nama file dan struktur folder, yang kemudian disimpan dalam struktur folder yang kompleks. Arsitektur ini memerlukan file metadata tambahan untuk setiap file dan folder serta sebuah file kunci utama untuk mengelola keseluruhan vault. Meskipun memberikan keuntungan dalam menyamarkan struktur folder secara total (seperti yang dibahas pada bagian 3.3), pendekatan ini secara inheren menghasilkan *overhead* yang sedikit lebih tinggi karena adanya metadata tambahan untuk setiap komponen di dalam *vault.*

Di sisi lain, *Rclone Crypt* berfungsi sebagai lapisan enkripsi yang bekerja langsung di atas remote lain (dalam kasus ini Google Drive). Rclone mengenkripsi konten dan nama file secara individual tanpa mengubah struktur folder asli. Model ini tidak memerlukan struktur vault yang kompleks atau file metadata per folder seperti *Cryptomator*. *Overhead* yang dihasilkan *Rclone Crypt* sebagian besar hanya berasal dari padding yang diperlukan oleh algoritma enkripsi dan sejumlah kecil metadata per file. Hal ini membuat *Rclone Crypt* secara signifikan lebih efisien dari segi penggunaan ruang penyimpanan. Bagi pengguna *Google Drive* dengan kuota terbatas, kemampuan *Rclone Crypt* untuk memaksimalkan ruang penyimpanan sangatlah berharga. Dalam skala yang lebih besar, seperti untuk *backup* data perusahaan yang mencapai terabyte, efisiensi ini dapat berujung pada penghematan biaya *cloud storage* yang signifikan dalam jangka panjang.

3.3 Analisis Visibilitas Metadata

Parameter ini menguji aspek keamanan fundamental dari *client-side encryption*, yaitu kemampuannya untuk menyamarkan metadata pada file yang diunggah di *Google Drive*. Dalam konteks forensik digital, metadata itu sendiri merupakan informasi yang menyimpan data terkait dari sebuah file yang dapat digunakan untuk proses identifikasi [14]. Oleh karena itu, analisis dilakukan dengan mengobservasi secara langsung tampilan file dan folder yang telah dienkripsi pada antarmuka *web Google Drive*. Gambar 3 menyajikan bukti visual perbandingan antara struktur file yang dihasilkan oleh *Cryptomator* dan *Rclone Crypt*, sementara Tabel 4 merangkum perbandingan atribut metadata secara rinci.



Gambar. 3. Perbandingan Metadata File Terenkripsi pada Antarmuka Google Drive

Tabel 4. Perbandingan Atribut Metadata

Atribut Metadata	Kondisi Asli	Setelah Enkripsi (Cryptomator)	Setelah Enkripsi (Rclone Crypt)
Nama file	Terlihat	Tersamarkan sepenuhnya, berubah menjadi nama acak.	Tersamarkan sepenuhnya, berubah menjadi nama acak.
Struktur folder	Terlihat	Tersamarkan sepenuhnya. Semua file berada dalam struktur folder d dengan subfolder acak.	Tersamarkan. Struktur folder asli tetap dipertahankan.
Ukuran file	Terlihat	Ukuran asli tidak terlihat, hanya ukuran file terenkripsi.	Ukuran asli tidak terlihat, hanya ukuran file terenkripsi.
Tipe file	Terlihat	Tidak dapat diidentifikasi, seringkali menjadi .bin.	Tidak dapat diidentifikasi, seringkali menjadi .bin.
Tanggal modifikasi	Terlihat	Terlihat	Terlihat
Pemilik file	Terlihat	Terlihat	Terlihat
Tanggal file dibuat	Terlihat	Terlihat	Terlihat
Pratinjau file	Terlihat	Tidak terlihat	Tidak terlihat

ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)

Dari hasil tersebut, ditemukan bahwa kedua perangkat lunak berhasil menyembunyikan atribut metadata yang paling krusial, yaitu nama file dan tipe file, serta membuat isi file tidak dapat diakses pada fitur pratinjau. Namun, terdapat perbedaan signifikan dalam penanganan struktur folder, di mana *Cryptomator* menyamarkannya secara total, sedangkan *Rclone Crypt* mempertahankannya. Atribut lain seperti tanggal modifikasi file juga tercatat masih dapat terlihat. Temuan pada parameter ini menegaskan bahwa baik *Cryptomator* maupun *Rclone Crypt* efektif dalam melindungi pilar utama kerahasiaan data berupa isi dan nama file. Dengan menyamarkan kedua aspek ini, pengguna dapat mencegah penyedia layanan cloud storage atau pihak ketiga yang tidak sah untuk mengetahui data apa yang disimpan.

Perbedaan fundamental terletak pada pendekatan terhadap privasi struktural. Kemampuan *Cryptomator* untuk mengaburkan struktur folder secara total menawarkan lapisan privasi yang lebih superior. Hal ini mencegah analisis terhadap bagaimana pengguna mengorganisir data, yang bisa saja membocorkan informasi. Sebaliknya, *Rclone Crypt* memprioritaskan kemudahan navigasi dan pengelolaan dengan mempertahankan struktur folder asli. Pendekatan ini lebih praktis untuk keperluan restorasi data, namun mengorbankan sebagian kecil aspek privasi struktural.

Satu catatan penting adalah visibilitas tanggal modifikasi file pada kedua alat. Dalam skenario forensik digital, jejak aktivitas ini justru bisa menjadi bukti yang berharga, yang menunjukkan bahwa enkripsi sisi klien berfokus melindungi isi data, bukan menyembunyikan fakta adanya aktivitas pada data tersebut.. Hal ini berpotensi memungkinkan pihak lain untuk menganalisis pola aktivitas pengguna. Temuan ini menunjukkan bahwa meskipun *client-side encryption* sangat kuat, tidak semua jejak digital dapat dihilangkan sepenuhnya, dan pengguna perlu menyadari hal tersebut.

3.4 Analisis Aksesibilitas

Analisis ini bertujuan untuk memverifikasi apakah file yang sudah dienkripsi dapat diakses atau dibuka secara langsung dari antarmuka *web Google Drive* tanpa proses dekripsi terlebih dahulu. Hasilnya konsisten untuk kedua perangkat lunak, tidak ada satu pun file terenkripsi yang dapat dibuka atau dipratinjau yang dimana *Google Drive* menampilkan pesan galat "Pratinjau tidak tersedia". Ketika ingin mengunduh file juga tidak berhasil mengunduh file asli melainkan berupa file yang terenkripsi. Hal ini membuktikan bahwa enkripsi telah mengubah struktur data file secara fundamental.

Kegagalan *Google Drive* untuk membuka file terenkripsi adalah hasil yang diharapkan dan merupakan validasi keberhasilan enkripsi sisi klien. Ini membuktikan bahwa kunci enkripsi benar-benar hanya berada di tangan pengguna, dan penyedia layanan atau pihak ketiga tidak memiliki kemampuan untuk melihat dan mendekripsi isi data.

3.5 Pengujian Portabilitas

Parameter portabilitas bertujuan untuk mengevaluasi kemudahan dan kepraktisan pengguna dalam mengakses data terenkripsi dari perangkat yang berbeda. Aspek ini mengukur seberapa fleksibel setiap perangkat lunak dapat diintegrasikan ke dalam alur kerja pengguna yang dinamis. Hasil pengujian dari proses penyiapan dan akses data pada perangkat sekunder dirangkum pada Tabel 5.

ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)

Tabel 5. Perbandingan Aspek Portabilitas Lintas Perangkat

Kriteria	Cryptomator	Rclone Crypt
Perangkat lunak yang diperlukan	Cryptomator dan Google Drive	File rclone.exe dan Google Drive
Proses konfigurasi perangkat lunak	Menyalin folder Cryptomator, yang bisa diunduh melalui Google Drive ataupun menyalin dari perangkat utama. Lalu menggunakna fitur add existing vault dan memasukan password vault	Menyalin file rclone.conf dari perangkat utama, tidak bisa melalui Google Drive karena secara default tidak ditambahkan. Mengkonfigurasi Rclone Crypt agar mengakses file tersebut.
Proses konfigurasi ke Google Drive	Mudah, konfigurasi seperti biasa laptop dihubungkan pada Google Drive	Cukup teknis karena perlu konfigurasi khusus dari Rclone Crypt ke Google Drive
Kredensial yang diperlukan	Perlu memasukan password ketika add existing vault pada Cryptomator	Hanya perlu menkonfigurasi Rclone Crypt agar mengakses file rclone.exe tanpa perlu memasukan password kembali oleh user
Ketergantungan	Bergantung tinggi. Proses sinkronisasi sepenuhnya bergantung pada Google Drive yang harus terinstal dan berjalan.	Independen, dapat melakukan sinkronisasi langsung ke Google Drive tanpa memerlukan instalasi sinkronisasi.
Pengalaman akses file	Sangat Mulus. Vault yang terbuka muncul sebagai drive baru di File Explorer, file dapat diakses seperti folder biasa.	Fleksibel, dapat diakses dengan perintah rclone mount atau dengan perintah rclone copy untuk mengunduh file.
Tingkat kesulitan	Rendah. Proses sepenuhnya berbasis antarmuka grafis yang intuitif dan mudah dipahami pengguna umum.	Tinggi. Memerlukan pengetahuan teknis karena proses berbasis baris perintah dan memerlukan pemahaman file konfigurasi.

Dari data tersebut, dapat disimpulkan bahwa *Cryptomator* menawarkan proses portabilitas yang lebih mudah bagi pengguna umum. Hal ini terlihat dari tingkat kesulitan yang rendah dan proses yang sepenuhnya mengandalkan antarmuka grafis yang intuitif. Sebaliknya, *Rclone Crypt* menunjukkan tingkat kesulitan yang tinggi dan menuntut pemahaman teknis, namun memberikan keuntungan berupa independensi dari perangkat lunak klien sinkronisasi. Hasil pengujian portabilitas menyoroti adanya *trade-off* fundamental antara kemudahan penggunaan dan fleksibilitas teknis. *Cryptomator* secara jelas memprioritaskan pengalaman pengguna yang sederhana dan terintegrasi. Dengan proses penyiapan yang mudah dipahami dan pengalaman akses file yang mulus layaknya folder biasa, *Cryptomator* sangat cocok untuk pengguna non-teknis yang sering berpindah perangkat dan menginginkan proses tanpa konfigurasi yang rumit.

Di sisi lain, *Rclone Crypt* menawarkan model portabilitas yang berbeda, yang lebih berorientasi pada pengguna teknis. Meskipun proses konfigurasinya lebih sulit, kemampuannya untuk beroperasi secara independen dari klien sinkronisasi *Google Drive* merupakan sebuah keuntungan besar dalam hal efisiensi dan minimalisme sistem. Fleksibilitas akses melalui berbagai perintah juga memberikan kontrol yang lebih besar kepada pengguna. Model ini sangat ideal untuk administrator sistem, developer yang membutuhkan solusi portabel yang kuat dan dapat diotomatisasi di berbagai lingkungan, termasuk server.

3.6 Pengukuran Waktu Pengunduhan File

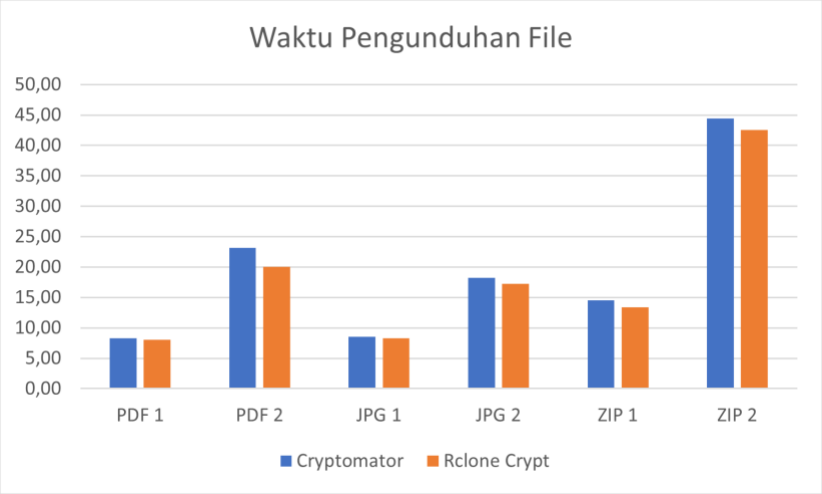
Bagian ini menyajikan hasil analisis perbandingan waktu yang dibutuhkan untuk mengunduh file terenkripsi dari *Google Drive.* Parameter ini penting untuk menilai efisiensi dan kecepatan akses kembali terhadap data yang telah disimpan di *Google Drive.* Proses pengukuran dilakukan dengan mencatat waktu dari awal perintah unduh dieksekusi hingga file selesai tersimpan di penyimpanan lokal. Untuk menjaga validitas dan reliabilitas, pengujian diulang sebanyak tiga kali untuk setiap file, dan hasilnya disajikan dalam bentuk nilai rata-rata serta standar deviasi pada Tabel 6. Visualisasi perbandingan rata-rata juga disajikan pada Gambar 4.

Tabel 6. Waktu Pengunduhan File

Nomor	File	Cryptomator (Detik)		Rclone Crypt (Detik)		Uji T	
		Rata-rata	Standar Deviasi	Rata-rata	Standar Deviasi	Statistik t	Nilai p
1	PDF 1	8,30	0,04	8,08	0,07	4,97	0,0076
2	PDF 2	23,15	0,37	20,01	0,33	11,05	0,0003
3	JPG 1	8,54	0,44	8,27	0,08	1,04	0,3557

ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)

Nomor	File	Cryptomator (Detik)		Rclone Crypt (Detik)		Uji T	
		Rata-rata	Standar Deviasi	Rata-rata	Standar Deviasi	Statistik t	Nilai p
4	JPG 2	18,22	0,32	17,22	0,41	3,34	0,0286
5	ZIP 1	14,51	0,17	13,40	0,44	4,09	0,0149
6	ZIP 2	44,40	0,45	42,53	0,46	5,05	0,0072



Gambar. 4. Waktu Pengunduhan File

Data hasil pengujian secara konsisten menunjukkan bahwa *Rclone Crypt* memiliki waktu pengunduhan yang lebih cepat dibandingkan *Cryptomator*. Untuk memvalidasi temuan ini secara statistik, dilakukan Uji T Sampel Independen. Hasilnya membuktikan bahwa keunggulan *Rclone Crypt* adalah signifikan secara statistik ($p<.05$) untuk lima dari enam jenis file yang diuji. Sebagai contoh, untuk file PDF 2, perbedaan waktu unduh antara *Cryptomator* dan *Rclone Crypt* terbukti sangat signifikan, $t(4)=11,05, p<,0003$. Temuan ini secara kuantitatif mengonfirmasi bahwa efisiensi *Rclone Crypt* berdampak langsung pada kecepatan pemulihan data.

3.7 Sintesis Komparatif

Analisis terhadap berbagai parameter teknis secara konsisten mengungkap adanya *trade-off* fundamental antara performa dan kemudahan penggunaan pada perangkat lunak *client-side encryption*. Temuan ini penting karena menyoroti dilema utama dalam pemanfaatan teknologi cloud. Sebuah penelitian menyebutkan bahwa bagi para profesional keamanan, *cloud* menghadirkan dilema besar mengenai bagaimana cara memanfaatkan manfaatnya sambil tetap mempertahankan kendali atas keamanan aset organisasi [15]. Meskipun penyedia layanan seperti Google telah menegaskan bahwa data yang disimpan di *server* Google dan data yang dikirimkan ke server tersebut dienkripsi [16], kebutuhan akan kontrol di sisi pengguna tetap tinggi.

Tidak ada satu alat yang unggul secara absolut, sehingga pilihan antara *Rclone Crypt* dan *Cryptomator* sangat bergantung pada profil dan prioritas pengguna. Temuan ini sejalan dengan penelitian lain yang menyatakan bahwa perbedaan paling signifikan antara berbagai solusi enkripsi seringkali bukan terletak pada kekuatan enkripsinya, melainkan pada bagaimana setiap aplikasi secara efektif mengimplementasikan fitur-fitur efisiensi lainnya [17]. Di satu sisi, *Rclone Crypt* tampil sebagai solusi yang superior dari segi kinerja mentah. Keunggulannya dalam kecepatan proses, baik enkripsi, unggah, maupun unduh, sejalan dengan temuan bahwa algoritma simetris seperti AES secara inheren memiliki performa yang jauh lebih cepat [18]. Penelitian lain juga mengonfirmasi bahwa metode simetris standar menawarkan kecepatan komputasi yang lebih baik, menjadikannya pilihan yang diinginkan untuk distribusi data yang cepat [19]. Hal ini menjadikan *Rclone Crypt* pilihan ideal untuk pengguna teknis, administrator sistem, atau dalam skenario yang melibatkan volume data besar.

Di sisi lain, *Cryptomator* secara jelas memprioritaskan pengalaman pengguna. Keunggulannya terletak pada kemudahan proses konfigurasi dan portabilitas lintas perangkat yang intuitif berkat antarmuka grafisnya. Hal ini membuatnya sangat cocok untuk pengguna umum yang tidak memiliki latar belakang teknis namun tetap ingin menerapkan lapisan keamanan yang kuat pada data mereka. Pendekatan dalam menarik kesimpulan berdasarkan prioritas pengguna ini sejalan dengan penelitian komparatif lainnya, di mana sebuah perangkat lunak bisa menjadi

ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)

pilihan terbaik jika aspek kecepatan menjadi prioritas utama, sementara perangkat lunak lain lebih unggul jika aspek kemampuan atau kemudahan yang diutamakan [20].

Pada akhirnya, tujuan utama dari analisis ini adalah untuk memberikan panduan yang jelas bagi pengguna. Hasil perbandingan ini dapat membantu pengguna untuk menyadari risiko yang mungkin terjadi sehingga dapat mengambil tindakan untuk mencegah dan mengatasinya dengan memilih perangkat lunak yang paling sesuai dengan kebutuhan keamanan dan alur kerja mereka [21]. Dengan demikian, baik pengguna teknis maupun non-teknis dapat membuat keputusan yang terinformasi untuk melindungi data mereka yang tersimpan di *Google Drive.*

4 Kesimpulan

Penelitian ini menyimpulkan adanya *trade-off* fundamental antara performa dan kemudahan penggunaan pada perangkat lunak enkripsi sisi-klien. *Rclone Crypt* terbukti superior dalam hal performa, menawarkan kecepatan proses yang secara statistik signifikan lebih tinggi dan efisiensi penyimpanan yang lebih baik, sehingga ideal untuk pengguna teknis. Sebaliknya, *Cryptomator* unggul dalam kemudahan penggunaan, dengan antarmuka intuitif dan portabilitas yang praktis bagi pengguna umum, serta memberikan lapisan privasi yang lebih kuat dengan menyamarkan struktur folder.

Oleh karena itu, pemilihan perangkat lunak sangat bergantung pada prioritas pengguna. Sebagai saran, penelitian selanjutnya dapat diperluas dengan menguji lebih banyak jenis file dan kondisi jaringan, melakukan audit keamanan yang lebih mendalam serta menguji kompatibilitas dengan layanan *cloud storage* lain seperti OneDrive dan Dropbox. Secara praktis, hasil ini dapat digunakan sebagai dasar bagi institusi untuk menyusun panduan keamanan data di *cloud storage*.

Referensi

[1] G. S. Santyadiputra and S. Hadi, “Vilanets: Inovasi Media Pembelajaran Jaringan Komputer,” J. Pendidik. Teknol. dan Kejuru., vol. 20, no. 1, pp. 57–67, 2023, doi.org/10.23887/jptkundiksha.v20i1.55087.

[2] K. A. Seputra, A. A. G. Y. Paramartha, and I. N. S. W. Wijaya, “Implementasi Google Drive Cloud Storage pada Sistem Repositori Al-Daring,” SINTECH (Science Inf. Technol. J.), vol. 5, no. 1, pp. 49–57, 2022, doi.org/10.31598/sintechjournal.v5i1.1000.

[3] I. D. A. M. Diantari, N. M. R. Wisudariani, and I. W. Artika, “Pemanfaatan Portal Google Classroom dalam Pembelajaran Teks Persuasif di Kelas VIII C SMP Negeri 1 Bangli Tahun Pelajaran 2020/2021,” J. Pendidik. Bhasa dan Sastra Indones., vol. 11, no. 2, pp. 260–269, 2021, ejournal.undiksha.ac.id/index.php/JJPBS/article/view/36575.

[4] B. M. Gupta, S. M. Dhawan, and R. Gupta, “Mobile Cloud Computing: A Scientometric Assessment of Global Publications Output during 2007-16,” J. Scientometr. Res., vol. 6, no. 3, pp. 186–194, 2017, doi.org/10.5530/jscires.6.3.26.

[5] Tesso, R., Novando, K., and Cahyaningtyas, C., “Menganalisa Foto Hoax Dengan Menggunakan Metode Reverse Image Search,” J. Informatik, vol. 19, no. 3, pp. 172-176, 2023, doi.org/10.5530/jscires.6.3.26.

[6] M. Y. Puspawan, M. S. Hartono, and S. N. Ardhya, “Analisis Yuridis Terhadap Perlindungan Data Pribadi Dalam Penggunaan Facebook Advertising Ditinjau dari Undang-Undang Informasi dan Transaksi Elektronik,” J. Komunitas Yustisia, vol. 4, no. 2, pp. 255-263, Aug. 2021, ejournal.undiksha.ac.id/index.php/jatayu/article/view/38077.

[7] R. Deng, “Toward Practical Client-Side Encryption in Cloud Computing”, in Proc. 19th ACM Asia Conf. Comput. Commun. Secur. (ASIA CCS ’24), 2024, doi.org/10.1145/3634737.3665023.

[8] P. Kaur and R. Kumar, “Emerging trends in cloud computing security a bibliometric analyses,” Artif. Intell. Rev., vol. 54, no. 7, pp. 5325-5370, 2021, doi.org/10.1049/iet-sen.2018.5222.

[9] F. Saraya, G. S. Santyadiputra, and I. M. D. Maysanjaya, “SIMOD: Sistem Monitoring Dashboard Konsumsi Daya Peralatan Listrik Rumah Berbasis Internet of Things,” Inser. Inf. Syst. Emerg. Technol. J., vol. 3, no. 2, pp. 62–74, 2022, doi.org/10.23887/insert.v3i2.50910.

[10] Z. Masyhur, A. Rizaldy, and P. Kartini, “Studi Literatur Keamanan dan Privasi Data Sistem Cloud Computing pada Platform Google Drive,” J. Software, Hardw. Inf. Technol., vol. 1, no. 2, pp. 31–38, 2021, doi.org/10.24252/shift.v1i2.15.

[11] F. S. Riyadi, S. Syefudin, G. Gunawan, and A. A. Murtopo, “Analisis Keamanan dan Privasi Data pada Layanan Cloud Computing dengan Menggunakan Teknik Kriptografi,” J. Technopreneur, vol. 11, no. 2, pp. 93–100, 2023, doi.org/10.30869/jtech.v11i2.1241.

[12] ISO/IEC, "ISO/IEC 25010:2023 - Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models," 2023.

[13] M. R. Manesh and J. G. Singh, “Resource allocation mechanisms in cloud computing: a systematic litarature review,” IET Commun., vol. 15, no. 1, pp. 105-117, 2021, doi.org/10.1049/iet-sen.2019.0338.

[14] Anjelina, R., and Noviyanti, P., Analisis Forensik Dengan Menerapkan Metadata Dan Hash Studi Kasus Pada Rekaman Video, J. Informatik, vol. 20, no. 3, pp. 118-124, 2024, doi.org/10.52958/iftk.v20i3.8770.

ISSN: 2655-139X (ONLINE)

ISSN: 0216-4221 (PRINT)

[15] R. Reza, F. Fitriani, L. Lifanda, L. W. Mardan, and L. Hasimu, "Kesadaran Pengguna Terhadap Keamanan Penyimpanan Data dalam Google Drive Studi Kasus Pada Dinas Komunikasi Kabupaten Wakatobi," J. Multidisipliner Kapalamada, vol. 1, no. 1, pp. 39–46, 2022, doi.org/10.62668/kapalamada.v1i01.56.
[16] K. Safitri and I. P. Nasution, "Analisis Penggunaan Aplikasi Google Drive Sebagai Media Penyimpanan Data," J. Sains dan Teknol., vol. 3, no. 3, pp. 220–223, 2023, doi.org/10.47233/jsit.v3i2.891.
[17] E. Henziger and N. Carlsson, "The Overhead of Confidentiality and Client-side Encryption in Cloud Storage Systems", in Proc. 12th IEEE/ACM Int. Conf. Util. Cloud Comput. (UCC '19), pp. 209-217, 2019, doi.org/10.1145/3344341.3368808
[18] N. Anwar, M. Munawwar, M. Abduh, and N. B. Santosa, "Komparatif Performance Model Keamanan Menggunakan Metode Algoritma AES 256 BIT dan RSA," J. RESTI (Rekayasa Sist. dan Teknol. Informasi), vol. 2, no. 3, pp. 783–791, 2018, doi.org/10.29207/resti.v2i3.606.
[19] Z. Arif and A. Nurokhman, "Analisis Perbandingan Algoritma Kriptografi Simetris dan Asimetris dalam Meningkatkan Keamanan Sistem Informasi," J. Teknol. Sist. Inf., vol. 4, no. 2, pp. 394–405, 2023, doi.org/10.35957/jtsi.v4i2.6077.
[20] I. M. P. Utama et al., "Analisis Perbandingan Kinerja Tool Website Directory Brute Force dengan Target Website DVWA," Inform. J. Ilmu Komput., vol. 18, no. 3, p. 278, 2022, doi.org/10.52958/iftk.v18i3.5256.
[21] I. M. E. Listartha, I. M. A. P. Mitha, M. W. A. Arta, and I. K. W. Y. Arimika, "Analisis Kerentanan Website SMA Negeri 2 Amlapura Menggunakan Metode OWASP (Open Web Application Security Project)," Simkom, vol. 7, no. 1, pp. 23–27, 2022, doi.org/10.51717/simkom.v7i1.63.

ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)