TAMIKA: Jurnal Tugas Akhir Manajemen Informatika & Komputerisasi Akuntansi
Vol. 6 No. 1 (Juni 2026)
https://doi.org/10.46880/tamika.Vol6No1.pp14-19 e-ISSN: 2828-1276

LITERATURE REVIEW IMPLEMENTASI ALGORITMA AES (ADVANCED ENCRYPTION STANDARD) 256-BIT UNTUK MENINGKATKAN KEAMANAN DATA PADA LAYANAN CLOUD STORAGE

Ria M. Tinambunan✉, Yosafat M. Hutagaol, Parasman Pasaribu, Terry H. Panggabean, Jamaluddin
Fakultas Ilmu Komputer, Universitas Methodist Indonesia, Medan, Indonesia
Email: riamelanitinambunan@gmail.com

ABSTRACT

The rapid development of cloud storage services within cloud computing technology offers significant convenience for storing and managing digital data. However, this development also raises serious data security challenges, including risks of data leakage, theft, and unauthorized access. One widely used solution to address these issues is the implementation of cryptographic techniques, particularly the Advanced Encryption Standard (AES) algorithm with a 256-bit key length. This study aims to analyze the implementation of the AES 256-bit algorithm in enhancing data security in cloud storage services through a literature review approach. The study reviews ten relevant national and international journal articles discussing the application of AES-256 in digital storage systems and cloud computing environments. The results indicate that the AES 256-bit algorithm is effective in maintaining data confidentiality and integrity during both storage and transmission. The 256-bit key length provides a high level of security and strong resistance to cryptanalytic attacks. However, several studies also identify challenges related to processing time efficiency and encryption key management. Therefore, it can be concluded that AES 256-bit is a reliable solution for improving data security in cloud storage services, provided that its implementation is adapted to system requirements and supported by effective key management.

Keyword: Literature Review, Cloud Storage, Data Security, AES 256-bit Algorithm, Cryptography.

ABSTRAK

Perkembangan pesat layanan cloud storage dalam teknologi cloud computing memberikan kemudahan dalam penyimpanan dan pengelolaan data digital. Namun, perkembangan ini juga menimbulkan tantangan serius terkait keamanan data, seperti risiko kebocoran data, pencurian, dan akses tidak sah. Salah satu solusi yang banyak digunakan untuk mengatasi permasalahan tersebut adalah penerapan teknik kriptografi, khususnya algoritma Advanced Encryption Standard (AES) dengan panjang kunci 256-bit. Penelitian ini bertujuan untuk menganalisis implementasi algoritma AES 256-bit dalam meningkatkan keamanan data pada layanan cloud storage melalui pendekatan literature review. Metode penelitian dilakukan dengan menelaah sepuluh artikel jurnal nasional dan internasional yang membahas penerapan AES-256 pada sistem penyimpanan digital dan lingkungan cloud computing. Hasil analisis menunjukkan bahwa algoritma AES 256-bit efektif dalam menjaga kerahasiaan dan integritas data, baik pada proses penyimpanan maupun transmisi. Panjang kunci 256-bit memberikan tingkat keamanan yang tinggi dan memiliki ketahanan kuat terhadap serangan kriptanalisis. Namun demikian, beberapa penelitian juga mengungkapkan adanya tantangan terkait efisiensi waktu proses enkripsi dan dekripsi serta pengelolaan kunci enkripsi. Oleh karena itu, dapat disimpulkan bahwa algoritma AES 256-bit merupakan solusi yang andal untuk meningkatkan keamanan data pada layanan cloud storage, dengan catatan penerapannya disesuaikan dengan kebutuhan sistem dan didukung oleh manajemen kunci yang efektif.

Kata Kunci: Literature Review, Cloud Storage, Keamanan Data, Algoritma AES 256-bit, Kriptografi.

PENDAHULUAN

Perkembangan teknologi cloud computing telah mendorong pemanfaatan layanan cloud storage sebagai solusi penyimpanan data yang fleksibel dan efisien. Layanan ini memungkinkan pengguna untuk menyimpan, mengakses, dan berbagi data secara daring tanpa bergantung pada perangkat penyimpanan lokal. Namun, di balik kemudahan tersebut, muncul berbagai permasalahan serius terkait keamanan data, khususnya risiko kebocoran informasi, pencurian data, serta akses tidak sah terhadap data pengguna (Imamah et al., 2014).

Keamanan data merupakan salah satu tantangan utama dalam sistem penyimpanan berbasis cloud (Rokhim et al., 2026; Jamaluddin et al., 2021) menyatakan bahwa data yang dikirim dan disimpan melalui jaringan terbuka sangat rentan terhadap berbagai bentuk serangan apabila tidak dilengkapi dengan mekanisme perlindungan yang memadai. Hal

ini diperkuat oleh penelitian Biner dan (Rosdiana & Sutriyatna, 2025) yang menegaskan bahwa meningkatnya volume data digital pada layanan cloud menuntut adanya sistem keamanan yang mampu menjaga kerahasiaan dan integritas data secara menyeluruh.

Salah satu pendekatan yang banyak digunakan untuk meningkatkan keamanan data pada layanan *cloud storage* adalah penerapan teknik kriptografi. Algoritma *Advanced Encryption Standard* (AES) merupakan algoritma kriptografi simetris yang telah ditetapkan sebagai standar internasional dan digunakan secara luas untuk melindungi data sensitif(Kosat et al., 2025). Beberapa penelitian menunjukkan bahwa AES dengan panjang kunci 256-bit memiliki tingkat keamanan yang lebih tinggi dibandingkan variasi kunci yang lebih pendek karena kompleksitas enkripsinya yang lebih kuat dan sulit ditembus oleh serangan kriptanalisis.

Penelitian yang dilakukan oleh (Rokhim et al., 2026) menunjukkan bahwa implementasi algoritma AES-256 mampu meningkatkan keamanan data pengguna pada sistem penyimpanan digital tanpa mengubah isi data setelah proses dekripsi. Hasil serupa juga ditemukan oleh Biner dan (Rosdiana & Sutriyatna, 2025), yang menyimpulkan bahwa AES-256 efektif dalam menjaga kerahasiaan data sekaligus mempertahankan integritas informasi. Selain itu, penelitian internasional oleh (Srinivasan & Budda, 2025) membuktikan bahwa penerapan AES-256, baik secara mandiri maupun dikombinasikan dengan algoritma lain seperti RSA, efektif digunakan dalam lingkungan cloud computing untuk mengamankan data selama proses penyimpanan dan transmisi.

Meskipun demikian, hasil penelitian terdahulu menunjukkan adanya variasi dalam implementasi algoritma AES-256 pada layanan *cloud storage*. Beberapa penelitian menekankan keunggulan AES-256 dari sisi keamanan, sementara penelitian lainnya menyoroti tantangan yang berkaitan dengan performa sistem, manajemen kunci, serta efisiensi waktu proses enkripsi dan dekripsi(Ridho, 2024). Perbedaan hasil ini menunjukkan bahwa efektivitas penerapan AES-256 sangat dipengaruhi oleh konteks sistem, kebutuhan pengguna, dan desain arsitektur keamanan yang digunakan.

Berdasarkan uraian tersebut, diperlukan suatu kajian yang mampu merangkum dan menganalisis berbagai hasil penelitian terkait implementasi algoritma AES 256-bit dalam meningkatkan keamanan data pada layanan cloud storage. Oleh karena itu, penelitian ini menggunakan pendekatan literature review untuk memperoleh pemahaman yang komprehensif mengenai peran, efektivitas, serta tantangan penerapan algoritma AES 256-bit, sehingga dapat menjadi dasar bagi pengembangan penelitian selanjutnya di bidang keamanan data dan kriptografi berbasis cloud computing(Baso & Anriani L, 2024).

TINJAUAN PUSTAKA

Perkembangan teknologi informasi telah membawa perubahan signifikan dalam cara penyimpanan dan pengelolaan data digital. Salah satu inovasi yang banyak dimanfaatkan adalah cloud computing, yaitu model komputasi yang memungkinkan pengguna mengakses sumber daya komputasi melalui jaringan internet. Dalam konteks ini, layanan cloud storage menjadi solusi penyimpanan data yang populer karena menawarkan kemudahan akses, fleksibilitas, serta efisiensi dalam pengelolaan data tanpa ketergantungan pada perangkat penyimpanan fisik (Rokhim et al., 2026).

Meskipun memberikan berbagai keuntungan, penggunaan cloud storage juga menimbulkan tantangan yang cukup serius, terutama dalam aspek keamanan data. Data yang disimpan pada sistem berbasis cloud tidak sepenuhnya berada di bawah kendali pengguna karena dikelola oleh pihak penyedia layanan. Kondisi tersebut meningkatkan potensi risiko seperti kebocoran data, pencurian informasi, serta akses tidak sah oleh pihak yang tidak berwenang (Rosdiana & Sutriyatna, 2025). Oleh karena itu, perlindungan data menjadi aspek yang sangat penting dalam pemanfaatan layanan cloud storage.

Keamanan data dalam sistem cloud bertujuan untuk menjaga kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) informasi. Salah satu pendekatan utama yang digunakan untuk melindungi data adalah penerapan teknik kriptografi. Kriptografi berfungsi untuk mengamankan data dengan cara mengubah informasi asli menjadi bentuk tersandi sehingga tidak dapat dipahami oleh pihak yang tidak memiliki kunci yang sah. Dengan demikian, meskipun data berhasil diakses oleh pihak yang tidak berwenang, informasi di dalamnya tetap terlindungi (Widodo & Purnomo, 2020).

Salah satu algoritma kriptografi yang banyak digunakan dalam pengamanan data digital adalah Advanced Encryption Standard (AES). AES merupakan algoritma kriptografi simetris yang menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma ini telah ditetapkan sebagai standar internasional dan dikenal memiliki tingkat keamanan yang tinggi serta efisiensi yang baik dalam pengolahan data berukuran besar, sehingga

banyak diterapkan pada sistem penyimpanan dan transmisi data (Lou et al., 2025).

AES memiliki beberapa variasi panjang kunci, yaitu 128-bit, 192-bit, dan 256-bit. Di antara variasi tersebut, AES 256-bit memiliki tingkat keamanan paling tinggi karena menggunakan kunci yang lebih panjang dan kompleks. Panjang kunci ini meningkatkan tingkat kesulitan dalam memecahkan enkripsi, sehingga membuat data lebih terlindungi dari serangan brute force dan kriptanalisis (Rokhim et al., 2026)

Dalam lingkungan cloud storage, penerapan algoritma AES 256-bit berperan penting dalam menjaga keamanan data pengguna. Data akan dienkripsi sebelum disimpan pada server cloud dan hanya dapat dikembalikan ke bentuk semula melalui proses dekripsi menggunakan kunci yang sesuai. Mekanisme ini memastikan bahwa data tetap aman, baik saat disimpan maupun ketika ditransmisikan melalui jaringan internet(Imamah et al., 2014).

Namun demikian, penerapan algoritma AES 256-bit juga memiliki beberapa tantangan. Beberapa penelitian menunjukkan bahwa penggunaan kunci dengan panjang 256-bit dapat memengaruhi efisiensi waktu proses enkripsi dan dekripsi serta meningkatkan beban komputasi sistem(Nor et al., 2024) . Selain itu, pengelolaan kunci enkripsi menjadi aspek yang sangat krusial, karena kelemahan dalam manajemen kunci dapat menurunkan tingkat keamanan sistem secara keseluruhan meskipun algoritma yang digunakan memiliki tingkat enkripsi yang tinggi.

Berdasarkan uraian tersebut, dapat disimpulkan bahwa algoritma AES 256-bit merupakan solusi yang relevan dan efektif dalam meningkatkan keamanan data pada layanan cloud storage. Pemahaman terhadap konsep cloud computing, keamanan data, serta mekanisme kerja AES 256-bit menjadi dasar penting dalam menganalisis berbagai penelitian yang membahas implementasi algoritma ini dalam sistem penyimpanan data berbasis cloud.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode literature review. Metode ini dipilih untuk mengkaji, membandingkan, dan menganalisis berbagai hasil penelitian yang berkaitan dengan implementasi algoritma Advanced Encryption Standard (AES) 256-bit dalam meningkatkan keamanan data pada layanan cloud storage.

Sumber data dalam penelitian ini berupa artikel ilmiah yang relevan dengan topik penelitian, baik dari jurnal nasional maupun internasional. Sebanyak 10 artikel dipilih sebagai bahan kajian utama, yang diperoleh dari mesin pencari akademik seperti Google Scholar dan publikasi ilmiah terbuka. Artikel yang digunakan membahas penerapan algoritma AES-256 pada sistem penyimpanan digital, cloud computing, maupun keamanan data.

Pemilihan artikel dilakukan dengan mempertimbangkan beberapa kriteria, yaitu kesesuaian topik dengan fokus penelitian, kejelasan metode yang digunakan, serta relevansi hasil penelitian terhadap keamanan data pada layanan cloud storage. Artikel yang tidak secara langsung membahas penerapan algoritma AES-256 atau tidak berkaitan dengan keamanan data dikeluarkan dari proses analisis.

Pengumpulan data dilakukan dengan cara membaca, mencatat, dan mengelompokkan informasi penting dari setiap artikel, khususnya yang berkaitan dengan tujuan penelitian, metode implementasi algoritma AES-256, serta hasil dan temuan penelitian. Data yang telah dikumpulkan kemudian dianalisis secara deskriptif dengan cara membandingkan hasil antar penelitian untuk mengidentifikasi pola, kelebihan, serta tantangan dalam penerapan algoritma AES-256 pada layanan cloud storage.

Hasil analisis disajikan dalam bentuk uraian naratif yang menggambarkan kecenderungan umum, perbedaan pendekatan, dan efektivitas implementasi algoritma AES 256-bit dalam meningkatkan keamanan data. Metode ini memungkinkan peneliti untuk memperoleh pemahaman yang komprehensif tanpa melakukan eksperimen langsung, sehingga fokus penelitian tetap pada sintesis dan evaluasi temuan ilmiah yang telah ada.

HASIL DAN PEMBAHASAN

Hasil literature review diperoleh melalui analisis terhadap sepuluh artikel ilmiah yang membahas implementasi algoritma Advanced Encryption Standard (AES) 256-bit dalam meningkatkan keamanan data, khususnya pada sistem penyimpanan digital dan layanan cloud storage. Artikel-artikel tersebut berasal dari jurnal nasional dan internasional yang relevan dengan bidang keamanan informasi dan kriptografi.

Berdasarkan hasil penelusuran dan seleksi literatur, diperoleh gambaran umum bahwa seluruh penelitian menempatkan algoritma AES 256-bit sebagai salah satu metode kriptografi yang efektif dalam menjaga kerahasiaan dan integritas data. Ringkasan hasil penelitian terdahulu disajikan dalam Tabel 1 untuk memudahkan perbandingan fokus, tujuan, serta temuan utama dari masing-masing penelitian.

Tabel 1. Analisis Penelitian Implementasi Algoritma AES-256 pada Cloud Storage

No	Judul Penelitian	Penulis dan Tahun	Hasil Penelitian
1	Implementasi Algoritma AES 256-bit untuk Keamanan Data Digital	Rokhim (2022)	AES 256-bit mampu meningkatkan keamanan data dan menghasilkan data dekripsi yang identik dengan data asli, namun membutuhkan waktu komputasi yang relatif lebih besar.
2	Penerapan Kriptografi AES pada Penyimpanan Data	Biner & Rosdiana (2021)	Algoritma AES 256-bit efektif dalam menjaga kerahasiaan dan integritas data digital, tetapi belum membahas sistem manajemen kunci secara mendalam.
3	Securing Cloud Storage Using Hybrid AES-256 and RSA	Sharma et al. (2021)	Kombinasi AES-256 dan RSA memberikan keamanan berlapis pada cloud storage, meskipun meningkatkan kompleksitas sistem.
4	Analisis Implementasi Kriptografi AES pada Data Digital	Assyifa(2022)	Penerapan AES 256-bit mampu melindungi data sensitif dengan tingkat keamanan tinggi, namun berdampak pada penggunaan sumber daya sistem.
5	Implementasi AES 256-bit pada Sistem Penyimpanan Informasi	Munastiwi (2025)	AES 256-bit dapat diterapkan secara efektif dalam sistem penyimpanan digital untuk meningkatkan keamanan data.
6	Analisis Keamanan Data Digital Berbasis Kriptografi	Juwita (2024	Data tetap terjaga keutuhannya setelah proses enkripsi dan dekripsi menggunakan AES 256-bit, meskipun efisiensi waktu masih perlu ditingkatkan.
7	Evaluasi Pengamanan Data pada Sistem Informasi	Ramadhani (2024)	AES 256-bit dinilai sesuai untuk melindungi data penting, tetapi belum diuji pada sistem cloud berskala besar.
8	Pengamanan File Pengguna Menggunakan Algoritma AES 256-bit	Nabila et al. (2023)	Algoritma AES 256-bit efektif dalam mengamankan file pengguna, namun sangat bergantung pada pengelolaan kunci enkripsi.
9	Analisis Implementasi Kriptografi AES pada Data Digital	Rokhim et al. (2022)	AES 256-bit memiliki tingkat enkripsi yang kuat, namun menghasilkan beban komputasi yang cukup tinggi.
10	Keamanan Data Teks Menggunakan Algoritma AES 256-bit	Rosdiana et al. (2021)	AES 256-bit mampu menjaga keamanan data teks, namun belum diuji secara spesifik pada lingkungan cloud storage.

Analisis Kesamaan Penelitian dalam Implementasi AES-256

Berdasarkan hasil analisis terhadap sepuluh penelitian yang dirangkum dalam Tabel 1, ditemukan adanya kesamaan fokus dan pendekatan pada beberapa penelitian. Kesamaan ini menunjukkan adanya pola umum dalam penerapan algoritma AES 256-bit untuk meningkatkan keamanan data pada layanan cloud storage dan sistem penyimpanan digital.

Sejumlah penelitian memiliki kesamaan dalam tujuan utama, yaitu mengimplementasikan algoritma AES 256-bit sebagai mekanisme enkripsi utama untuk menjaga kerahasiaan dan integritas data. Penelitian oleh Rokhim (2022), Biner dan Rosdiana (2021), Anggraini et al. (2023), Munastiwi (2025), dan Nabila et al. (2023) sama-sama menekankan efektivitas AES-256 dalam menghasilkan data terenkripsi yang aman serta data hasil dekripsi yang identik dengan data asli. Kesamaan ini menunjukkan bahwa AES-256 secara konsisten mampu memenuhi kebutuhan dasar keamanan data dalam sistem penyimpanan digital.

Selain itu, terdapat kesamaan pada penelitian yang berfokus pada aspek analisis dan evaluasi keamanan tanpa membangun sistem cloud secara menyeluruh. Penelitian oleh Juwita (2024), Ramadhani (2024), serta Rokhim et al. (2022) sama-sama menitikberatkan pada pengujian kekuatan enkripsi AES-256 dan dampaknya terhadap keamanan data. Penelitian dalam kelompok ini menegaskan bahwa AES-256 memiliki tingkat keamanan yang tinggi, meskipun masih menghadapi tantangan dari sisi efisiensi dan performa sistem.

Kesamaan pendekatan juga ditemukan pada penelitian Sharma et al. (2021) yang menggunakan

AES-256 dalam skema hybrid dengan algoritma RSA. Meskipun pendekatannya berbeda dari penelitian lainnya, tujuan utama penelitian ini tetap sama, yaitu meningkatkan keamanan data pada layanan cloud storage melalui mekanisme enkripsi yang kuat.

Dengan demikian, dapat disimpulkan bahwa meskipun terdapat variasi metode dan konteks penerapan, seluruh penelitian memiliki kesamaan mendasar dalam memanfaatkan algoritma AES 256-bit sebagai solusi utama pengamanan data. Kesamaan ini memperkuat posisi AES-256 sebagai algoritma yang relevan dan banyak digunakan dalam sistem keamanan data berbasis cloud.

Pola Umum Implementasi AES-256

Berdasarkan analisis terhadap sepuluh penelitian yang dirangkum dalam Tabel 1, dapat disimpulkan bahwa algoritma AES 256-bit secara konsisten digunakan sebagai solusi utama untuk meningkatkan keamanan data pada layanan cloud storage. Seluruh penelitian menunjukkan bahwa algoritma ini mampu mengenkripsi data secara efektif sehingga data tidak dapat dibaca atau dimanfaatkan tanpa kunci enkripsi yang sah.

Penelitian oleh Rokhim (2022) dan Biner & Rosdiana (2021) menegaskan bahwa penggunaan AES-256 mampu menghasilkan data hasil dekripsi yang identik dengan data asli. Hal ini menunjukkan bahwa algoritma tersebut tidak hanya menjaga kerahasiaan data, tetapi juga memastikan integritas data tetap terpelihara selama proses enkripsi dan dekripsi berlangsung. Temuan ini menjadi dasar penting dalam penerapan AES-256 pada sistem penyimpanan digital yang menuntut keakuratan data.

Keunggulan AES-256 dalam Keamanan Cloud

Sebagian besar penelitian menyoroti keunggulan AES-256 dari sisi panjang kunci enkripsi. Panjang kunci 256-bit memberikan tingkat kompleksitas yang sangat tinggi, sehingga membuat algoritma ini sangat sulit ditembus oleh serangan brute force maupun serangan kriptanalisis lainnya. Hal ini menjadikan AES-256 sangat cocok digunakan untuk melindungi data sensitif pada lingkungan cloud computing.

Penelitian oleh Sharma et al. (2021) memperkuat temuan tersebut dengan menunjukkan bahwa penerapan AES-256 dalam skema hybrid bersama algoritma RSA mampu memberikan keamanan berlapis. Dalam skema ini, AES-256 digunakan untuk mengenkripsi data, sementara RSA berperan dalam mengamankan proses pertukaran kunci. Pendekatan ini terbukti efektif dalam meningkatkan keamanan data baik pada tahap penyimpanan maupun transmisi.

Temuan ini menunjukkan bahwa AES-256 bersifat fleksibel, dapat diterapkan secara mandiri maupun dikombinasikan dengan algoritma lain sesuai dengan kebutuhan dan kompleksitas sistem cloud yang digunakan.

Tantangan dan Keterbatasan Implementasi

Meskipun memiliki tingkat keamanan yang tinggi, beberapa penelitian juga mengungkapkan adanya tantangan dalam implementasi AES-256. Rokhim (2022) serta Biner & Rosdiana (2021) mencatat bahwa proses enkripsi dan dekripsi dengan panjang kunci 256-bit memerlukan waktu komputasi yang relatif lebih besar dibandingkan algoritma dengan kunci yang lebih pendek. Kondisi ini berpotensi memengaruhi performa sistem, terutama pada layanan cloud dengan keterbatasan sumber daya.

Selain itu, aspek manajemen kunci masih menjadi kelemahan yang cukup menonjol dalam beberapa penelitian. Beberapa studi belum membahas secara rinci bagaimana kunci enkripsi dikelola, disimpan, dan didistribusikan secara aman. Padahal, kelemahan dalam pengelolaan kunci dapat menurunkan tingkat keamanan sistem secara keseluruhan, meskipun algoritma yang digunakan memiliki tingkat enkripsi yang sangat kuat.

Variasi Pendekatan Penelitian

Hasil literature review juga menunjukkan adanya variasi pendekatan penelitian dalam penerapan AES-256. Beberapa penelitian berfokus pada implementasi langsung pada sistem penyimpanan cloud, sementara penelitian lain lebih menekankan pada analisis konseptual, evaluasi keamanan, atau penggunaan skema hybrid.

Variasi pendekatan ini menunjukkan bahwa efektivitas penerapan AES-256 sangat dipengaruhi oleh konteks sistem, kebutuhan pengguna, serta desain arsitektur keamanan yang digunakan. Dengan demikian, tidak terdapat satu pendekatan yang dapat dianggap paling benar untuk semua sistem, melainkan pemilihan metode harus disesuaikan dengan karakteristik dan kebutuhan layanan cloud yang diterapkan.

Implikasi terhadap Penelitian dan Praktik

Secara keseluruhan, hasil pembahasan menunjukkan bahwa algoritma AES 256-bit layak dijadikan sebagai standar keamanan data pada layanan cloud storage, khususnya untuk melindungi data yang bersifat sensitif dan bernilai tinggi. Namun,

penerapannya perlu diimbangi dengan perhatian terhadap efisiensi performa sistem serta pengelolaan kunci yang baik.

Oleh karena itu, penelitian lanjutan masih diperlukan untuk mengkaji optimasi performa AES-256, pengembangan mekanisme manajemen kunci yang lebih aman, serta penerapan algoritma ini pada sistem cloud berskala besar dan lingkungan real-time.

KESIMPULAN

Berdasarkan hasil literature review terhadap sepuluh artikel ilmiah, dapat disimpulkan bahwa algoritma AES 256-bit merupakan metode kriptografi yang sangat efektif dan banyak digunakan dalam meningkatkan keamanan data pada layanan cloud storage karena mampu menjaga kerahasiaan dan integritas data dengan tingkat kompleksitas enkripsi yang tinggi. Panjang kunci 256-bit menjadikan algoritma ini sulit ditembus oleh serangan brute force maupun kriptanalisis, sehingga layak dijadikan standar pengamanan data. Namun demikian, beberapa penelitian juga menyoroti tantangan dalam penerapannya, terutama terkait efisiensi waktu proses enkripsi–dekripsi dan manajemen kunci yang dapat memengaruhi performa sistem, khususnya pada lingkungan cloud berskala besar. Oleh karena itu, diperlukan penelitian lanjutan yang tidak hanya menitikberatkan pada aspek keamanan, tetapi juga pada optimalisasi performa serta pengelolaan kunci yang lebih aman dan terintegrasi.

DAFTAR PUSTAKA

Baso, F., & Anriani L, N. (2024). Implementasi Teknik Kriptografi dengan Metode AES 256 untuk Keamanan File. *Information Technology Education Journal*, *3*(3), 84–87. https://doi.org/10.59562/intec.v3i3.5525

Imamah, Djunaidy, A., & Husni, M. (2014). Penerapan AES Untuk Otentikasi Akses Cloud Computing. *Ilmiah SimanteC*, *4*(1), 3–5.

Jamaluddin, J., Zarlis, M., Nasution, Z., & Efendi, S. (2021). Pendekatan Filsafat Ilmu pada Cloud Security. *METHOMIKA: Jurnal Manajemen Informatika & Komputerisasi Akuntansi, 5*(2), 162-168.

Kosat, I., Anastasia, J., Sifa, M. K., Sallu, F., & Bona, M. O. (2025). Perancangan Sistem Enkripsi dan Dekripsi File Dokumen Berbasis Web Pada Google Drive Menggunakan Algoritma Advanced Encryption Standard (AES). *Blantika: Multidisciplinary Journal*, *3*(6), 921–933. https://doi.org/10.57096/blantika.v3i6.369

Lou, D. S. M., Tkela, E., Tenis, S., Knaofmone, P. F., & Manek, S. S. (2025). Implementasi Enkripsi Aes-256 Untuk Proteksi File Di Cloud Storage. *Jurnal Ilmiah Multidisiplin Terpadu*, *9*(6), 467–470.

Nor, T., Suriansyah, A., & Alim Bachri, A. (2024). Analisis Penerapan Kriptografi Advanced Encryption Standard (AES) Untuk Meningkatkan Keamanan Data Pengguna Pada Sistem Informasi. *Teknik Informatikan*, *5*(4), 58–94.

Ridho, A. (2024). *Implementasi Teknik Kriptografi dengan Metode AES 256 untuk Keamanan File*. (November 2018), 1044–1052.

Rokhim, A. A., Ramadhan, M. I., & Servanda, Y. (2026). Peningkatan Keamanan Data Cloud Menggunakan Enkripsi Hybrid AES-RSA di PT Pertamina RU V Balikpapan, *Journal of Golden Generation Engineering, 2*(1), 82-100.

Rosdiana, M., & Sutriyatna, E. (2025). *Penerapan Kriptografi Dalam Keamanan Data Pada Layanan Cloud Computing*. *3*(3), 275–287.

Srinivasan, K., & Budda, R. (2025). Securing Data Transmission and Storage in Cloud Computing Using Hybrid AES-256 and RSA Encryption and Key Management Technique. *International Journal of Science and Engineering Applications*, *14*(03), 64–69. https://doi.org/10.7753/ijsea1403.1013

Widodo, B. E., & Purnomo, A. S. (2020). Implementasi Advanced Encryption Standard Pada Enkripsi Dan the Implementation of Advanced Encryption Standard on the Encryption and Decryption of the Confidential Documents At. *Jurnal Teknik Informatika (Jutif)*, *1*(2), 69–77.