Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 5 No. 1 (2026) pp: 15574-15582
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Analisis Keamanan Data pada Sistem Informasi Berbasis *Cloud* dengan Enkripsi AES: Pendekatan Kuantitatif Berbasis *State of the Art*

Ragil Aryanando, Komputerio Akbar
Program Studi Sistem Informasi, STMIK Borneo International, Indonesia
ragilngabei@gmail.com, komputerio@stmik-borneo.org.id

Abstrak

Penelitian ini bertujuan menganalisis pengaruh penerapan Advanced Encryption Standard (AES), manajemen kunci, dan kontrol akses terhadap keamanan data pada sistem informasi berbasis cloud pada konteks perguruan tinggi. Selain analisis kuantitatif, penelitian ini diperkuat dengan sintesis state of the art terhadap 30 artikel jurnal internasional periode 2021-2025 untuk memetakan kecenderungan riset, celah penelitian, dan dasar konseptual model. Pendekatan utama penelitian adalah kuantitatif eksplanatori dengan desain survei potong lintang. Data diperoleh dari 214 responden yang terdiri atas staf teknologi informasi, administrator sistem, pengelola data, dan personel keamanan informasi pada organisasi yang telah menerapkan sistem berbasis cloud. Instrumen menggunakan skala Likert 5 poin dan dianalisis dengan statistik deskriptif, korelasi Pearson, diagnostik multikolinearitas, serta regresi linear berganda. Hasil penelitian menunjukkan bahwa penerapan AES (beta = 0,301; p < 0,001), manajemen kunci (beta = 0,246; p < 0,001), dan kontrol akses (beta = 0,389; p < 0,001) berpengaruh positif dan signifikan terhadap keamanan data. Model penelitian juga signifikan secara simultan, F(3,210) = 115,864; p < 0,001, dengan Adjusted R2 sebesar 0,618. Sintesis literatur menunjukkan bahwa studi cloud security mutakhir semakin menekankan integrasi antara kriptografi, key lifecycle governance, dan zero-trust access control. Temuan ini menegaskan bahwa keamanan data cloud tidak cukup bertumpu pada algoritma enkripsi yang kuat saja, melainkan harus diperkuat oleh tata kelola kunci dan pembatasan akses yang konsisten. Kontribusi penelitian terletak pada penyusunan model empiris yang menggabungkan tiga kontrol inti keamanan cloud sekaligus menghubungkannya dengan peta perkembangan literatur terkini.

Kata kunci: Keamanan Data; Cloud Computing; AES; Manajemen Kunci; Kontrol Akses; State of the Art.

1. Latar Belakang

Transformasi digital telah mempercepat adopsi sistem informasi berbasis cloud di berbagai sektor, termasuk pendidikan tinggi, karena *cloud computing* menawarkan skalabilitas, fleksibilitas, dan efisiensi biaya. Namun, perpindahan data akademik, data personal, dan dokumen institusional ke lingkungan cloud juga memperluas permukaan serangan serta meningkatkan konsekuensi dari salah konfigurasi, penyalahgunaan hak akses, dan kebocoran data. Literatur mutakhir menunjukkan bahwa masalah keamanan cloud tidak lagi dipahami semata sebagai isu teknis, melainkan sebagai isu tata kelola yang memengaruhi keandalan layanan, kepatuhan, dan kepercayaan pengguna (Abdulsalam & Hedabou, 2022; Ali et al., 2025; Chauhan & Shiaeles, 2023; Younas et al., 2022).

Dalam konteks global, tantangan keamanan cloud semakin kompleks seiring berkembangnya arsitektur *multi-cloud*, *hybrid cloud*, *cloud-native*, dan *serverless*. Ulasan mutakhir menegaskan bahwa ancaman dominan meliputi data leakage, misconfiguration, lemahnya identity and access management, serangan terhadap API, dan rendahnya visibilitas kontrol pada ekosistem layanan yang saling terhubung (Ali et al., 2025; Dawood et al., 2023; Soveizi et al., 2023; Ukeje et al., 2024). Pada sektor pendidikan, El-Sofany et al. (2024) menunjukkan bahwa kerangka proteksi yang kuat dapat meningkatkan kemampuan deteksi dan mitigasi serangan pada sistem pendidikan berbasis cloud.

Salah satu kontrol teknis yang paling luas digunakan untuk menjaga kerahasiaan data cloud adalah enkripsi, terutama *Advanced Encryption Standard (AES)*. Secara konseptual, AES berperan penting dalam memperkuat dimensi *confidentiality* dan *integrity* dalam kerangka CIA triad. Namun, literatur juga menegaskan bahwa kekuatan algoritma enkripsi tidak dapat dipisahkan dari kualitas manajemen kunci serta mekanisme pembatasan

akses. Dengan kata lain, enkripsi yang kuat tidak akan optimal jika kunci tidak dikelola secara aman atau jika akses pengguna tidak dikendalikan dengan prinsip *least privilege* (Barker, 2020; National Institute of Standards and Technology, 2023; Rana et al., 2023; Tang et al., 2024).

Studi terdahulu banyak berfokus pada pengembangan model kriptografi, usulan framework, atau evaluasi performa teknik keamanan tertentu, misalnya model hybrid AES-ECC, adaptive key management berbasis blockchain, serta *zero-trust access control* untuk lingkungan cloud. Kontribusi-kontribusi tersebut penting, tetapi mayoritas belum menguji secara empiris hubungan langsung antara penerapan AES, manajemen kunci, dan kontrol akses terhadap keamanan data pada konteks organisasi pengguna cloud. Keterbatasan inilah yang membuka ruang bagi penelitian kuantitatif yang menguji model secara integratif (Golightly et al., 2023; Rehman et al., 2021; Shivaramakrishna & Nagaratna, 2023; Wang et al., 2025).

Berdasarkan kondisi tersebut, penelitian ini bertujuan menganalisis pengaruh penerapan enkripsi AES, manajemen kunci, dan kontrol akses terhadap keamanan data pada sistem informasi berbasis cloud. Kontribusi penelitian terletak pada: (1) penyusunan model kuantitatif yang mengintegrasikan kriptografi, key governance, dan access control, (2) penguatan model melalui sintesis state of the art dari artikel-artikel jurnal terkini, dan (3) penyediaan implikasi praktis bagi organisasi, khususnya perguruan tinggi, dalam memprioritaskan kontrol keamanan data cloud.

Tabel 1. State of the art dan posisi penelitian

Studi	**Fokus dan metode**	**Temuan kunci**	**Gap dan posisi penelitian ini**
Rehman et al. (2021)	Eksperimen hybrid AES-ECC untuk cloud storage.	Skema hybrid meningkatkan autentikasi dan integritas data cloud.	Berfokus pada performa teknis; belum menguji dampak implementasi AES pada keamanan data organisasi.
Younas et al. (2022)	Survey keamanan cloud berdasarkan model layanan.	Ancaman cloud dominan mencakup virtualisasi, multitenancy, dan IAM.	Memberi peta ancaman, tetapi tidak membangun model kausal pada level organisasi.
Rana et al. (2023)	Survey komprehensif sistem manajemen kunci kriptografi.	Key lifecycle governance merupakan komponen kritis perlindungan data.	Belum diuji bersama variabel enkripsi dan kontrol akses dalam satu model empiris.
Golightly et al. (2023)	Survey access control untuk cloud, blockchain, IoT, dan SDN.	Kontrol akses modern bergerak ke ABAC, continuous verification, dan auditability.	Belum menguji kontribusi relatif access control terhadap keamanan data cloud.
Soveizi et al. (2023)	SLR keamanan dan privasi workflow berbasis cloud.	Literatur masih berat pada fase desain dan eksekusi; monitoring dan adaptasi masih lemah.	Mengidentifikasi celah riset, tetapi bukan pengujian kuantitatif pada organisasi pengguna cloud.
El-Sofany et al. (2024)	Framework keamanan sistem pendidikan berbasis cloud.	Proteksi berlapis mampu meningkatkan deteksi serangan pada konteks pendidikan.	Fokus pada rancangan framework, belum menguji model regresi atas faktor keamanan data.
Punia et al. (2024)	SLR blockchain-based access control di cloud.	Akses berbasis blockchain meningkatkan auditability dan trust distribution.	Belum membandingkan peran access control dengan AES dan manajemen kunci sebagai prediktor keamanan data.

DOI: https://doi.org/10.31004/riggs.v5i1.8272

Ali et al. (2025)	Review keamanan multi-cloud dan hybrid cloud.	Keamanan multi-cloud membutuhkan integrasi cryptography, IAM, compliance, dan visibility.	Memberi arah strategis, namun belum memberi bukti empiris pada level implementasi organisasi.
Penelitian ini	Survei kuantitatif pada 214 responden dengan dukungan state of the art 30 artikel.	Menguji pengaruh AES, manajemen kunci, dan kontrol akses terhadap keamanan data cloud.	Mengisi gap empiris dengan model integratif yang relevan untuk konteks perguruan tinggi.

Tabel 1 menunjukkan bahwa literatur terkini memang kaya akan pengembangan framework, model hibrida, dan survey konseptual, tetapi masih terbatas studi yang secara kuantitatif menguji pengaruh gabungan antara AES, manajemen kunci, dan kontrol akses terhadap keamanan data. Berdasarkan gap tersebut, hipotesis penelitian dirumuskan sebagai berikut: H1 penerapan enkripsi AES berpengaruh positif dan signifikan terhadap keamanan data; H2 manajemen kunci berpengaruh positif dan signifikan terhadap keamanan data; H3 kontrol akses berpengaruh positif dan signifikan terhadap keamanan data; dan H4 penerapan enkripsi AES, manajemen kunci, dan kontrol akses secara simultan berpengaruh signifikan terhadap keamanan data.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan kuantitatif eksplanatori dengan desain survei potong lintang. Desain ini dipilih karena penelitian bertujuan menguji hubungan prediktif antarvariabel yang telah dirumuskan dalam hipotesis, bukan sekadar mendeskripsikan fenomena. Pendekatan survei cocok untuk menangkap persepsi responden terhadap implementasi keamanan cloud yang tidak selalu dapat diamati secara langsung (Creswell & Creswell, 2018; Field, 2018; Sekaran & Bougie, 2019).

2.1 Prosedur state of the art dan SLR pendukung

Sebelum instrumen survei difinalisasi, dilakukan penelusuran literatur secara terstruktur untuk menyusun state of the art, memetakan celah penelitian, dan menurunkan indikator operasional variabel. Kajian ini bersifat supporting SLR, yaitu sintesis literatur sistematis yang berfungsi memperkuat kerangka konseptual penelitian kuantitatif. Objek kajian terdiri atas 30 artikel jurnal internasional terbit tahun 2021-2025 yang relevan dengan tema *cloud security, encryption, key management, access control*, dan data privacy.

Tabel 2. Kriteria penelusuran dan seleksi literatur pendukung

Aspek	**Kriteria**
Rentang waktu	Artikel jurnal terbit 2021-2025 agar menggambarkan perkembangan mutakhir keamanan cloud.
Kata kunci	"cloud security"; "AES" AND cloud; "cloud key management"; "cloud access control"; "zero trust" AND cloud; "data security" AND higher education cloud.
Inklusi	Artikel peer-reviewed, relevan dengan keamanan data cloud, membahas minimal satu konstruk penelitian, dan menyediakan temuan konseptual atau empiris yang dapat disintesis.
Eksklusi	Prosiding, editorial, artikel non-full-text, studi non-cloud, dan studi yang hanya membahas performa komputasi tanpa implikasi keamanan data.
Output	Sebanyak 30 artikel dipetakan ke empat tema utama: keamanan cloud dan tata kelola; enkripsi/hybrid cryptography; manajemen kunci dan integritas; serta access control/zero trust.

DOI: https://doi.org/10.31004/riggs.v5i1.8272

2.2 Populasi, sampel, dan instrumen

Populasi penelitian adalah tenaga profesional yang terlibat langsung dalam pengelolaan, pengoperasian, atau pengamanan sistem informasi berbasis cloud, seperti staf teknologi informasi, administrator sistem, pengelola data, dan personel keamanan informasi. Teknik sampling yang digunakan adalah purposive sampling dengan kriteria: (1) institusi telah menerapkan layanan cloud; (2) responden memiliki pengalaman minimal satu tahun dalam penggunaan atau pengelolaan cloud; dan (3) responden memahami kebijakan keamanan data pada unit kerjanya. Total responden yang memenuhi kriteria dan dianalisis sebanyak 214 orang.

Instrumen penelitian berupa kuesioner terstruktur berbasis skala Likert 1-5. Variabel penerapan enkripsi AES (X1) diukur melalui indikator penggunaan AES untuk proteksi data tersimpan dan data saat transmisi, konsistensi penerapan enkripsi, serta persepsi efisiensi implementasi. Variabel manajemen kunci (X2) diukur melalui pembangkitan, distribusi, penyimpanan, rotasi, dan pemusnahan kunci. Variabel kontrol akses (X3) diukur melalui autentikasi, otorisasi, pembatasan hak akses, dan pemantauan aktivitas akses. Variabel keamanan data (Y) diukur melalui dimensi kerahasiaan, integritas, ketersediaan, dan perlindungan dari akses tidak sah.

Tabel 3. Definisi operasional variabel penelitian

Variabel	Definisi operasional	Indikator inti	Rujukan konseptual
Penerapan enkripsi AES (X1)	Derajat implementasi AES pada data at rest dan data in transit di lingkungan cloud.	Proteksi data tersimpan; proteksi saat transmisi; konsistensi implementasi; efisiensi penerapan.	NIST (2023); Rehman et al. (2021); Shakor et al. (2024).
Manajemen kunci (X2)	Kematangan tata kelola siklus hidup kunci kriptografi.	Pembangkitan; distribusi; penyimpanan; rotasi; pemusnahan kunci.	Barker (2020); Rana et al. (2023); Tang et al. (2024).
Kontrol akses (X3)	Efektivitas pembatasan dan pengawasan akses pada data atau layanan cloud.	Autentikasi; otorisasi; least privilege; audit dan monitoring akses.	Golightly et al. (2023); Wang et al. (2025); Punia et al. (2024).
Keamanan data (Y)	Tingkat perlindungan data pada sistem informasi berbasis cloud.	Confidentiality; integrity; availability; perlindungan dari akses tidak sah.	Ali et al. (2025); El-Sofany et al. (2024); Younas et al. (2022).

2.3 Teknik analisis data

Analisis data dilakukan dalam dua tahap. Tahap pertama adalah statistik deskriptif untuk menggambarkan kecenderungan jawaban responden. Tahap kedua adalah analisis inferensial menggunakan korelasi Pearson dan regresi linear berganda untuk menguji pengaruh penerapan enkripsi AES, manajemen kunci, dan kontrol akses terhadap keamanan data. Diagnostik multikolinearitas dilaporkan melalui nilai tolerance dan variance inflation factor (VIF). Model persamaan yang digunakan adalah $Y = a + b1X1 + b2X2 + b3X3 + e$. Hipotesis diterima apabila $p < 0,05$ (Field, 2018; Ghozali, 2021; Hair et al., 2019).

3. Hasil dan Diskusi

3.1 Sintesis state of the art dan SLR pendukung

Sintesis atas 30 artikel menunjukkan bahwa penelitian keamanan cloud terkini dapat dikelompokkan ke dalam empat tema besar. Pertama, tema keamanan cloud, privasi, dan tata kelola menyoroti data leakage, misconfiguration, intercloud trust, dan compliance. Kedua, tema enkripsi dan *hybrid cryptography* menekankan bahwa AES tetap menjadi kontrol inti, tetapi efektivitasnya meningkat ketika dipadukan dengan skema hybrid dan proteksi komunikasi. Ketiga, tema key management dan data integrity menegaskan bahwa siklus hidup kunci,

DOI: https://doi.org/10.31004/riggs.v5i1.8272

deduplikasi aman, serta mekanisme integritas merupakan lapisan proteksi yang tidak dapat diabaikan. Keempat, tema *access control* dan *zero trust* menunjukkan pergeseran dari model statis ke model berbasis atribut, *continuous verification, dan auditability*.

Tabel 4. Sintesis 30 artikel jurnal berdasarkan tema utama

Tema	Jumlah artikel	Sintesis temuan utama	Implikasi bagi model penelitian
Keamanan cloud, privasi, dan tata kelola	9	Ancaman dominan meliputi kebocoran data, salah konfigurasi, lemahnya IAM, multi-cloud complexity, dan isu compliance.	Keamanan data perlu diposisikan sebagai konstruk terikat yang mewakili confidentiality, integrity, availability, dan perlindungan dari misuse.
Enkripsi AES dan hybrid cryptography	6	AES tetap efisien untuk proteksi data utama, tetapi efektivitas meningkat bila diintegrasikan dengan skema hybrid dan proteksi transmisi.	Penerapan AES layak dijadikan prediktor utama yang diukur dari konsistensi implementasi pada data at rest dan in transit.
Key management dan data integrity	7	Keamanan cloud sangat dipengaruhi governance atas pembangkitan, distribusi, rotasi, dan penyimpanan kunci, serta strategi integritas data.	Manajemen kunci perlu dimodelkan sebagai variabel tersendiri, bukan sekadar atribut teknis dari enkripsi.
Access control, ABAC, dan zero trust	8	Literatur bergerak ke least privilege, attribute-based access control, privacy-preserving authorization, dan verifikasi berkelanjutan.	Kontrol akses diprediksi memiliki pengaruh besar terhadap keamanan data karena berhubungan langsung dengan siapa yang dapat mengakses data.

Hasil sintesis pada Tabel 4 memperkuat alasan teoritis pemilihan model penelitian. Berbeda dengan banyak studi terdahulu yang berorientasi pada desain framework atau performa algoritma, penelitian ini menempatkan keamanan data sebagai variabel dependen dan menguji tiga kontrol yang paling konsisten muncul di literatur, yaitu AES, key management, dan access control. Dengan demikian, model penelitian ini berangkat dari kecenderungan riset mutakhir sekaligus mengisi celah pada level pengujian empiris.

3.2 Hasil statistik deskriptif

Analisis deskriptif menunjukkan bahwa seluruh variabel berada pada kategori tinggi. Hal ini menandakan bahwa responden secara umum menilai implementasi proteksi data cloud di organisasinya telah berjalan relatif baik, walaupun tingkat kematangan setiap kontrol belum sama.

Tabel 5. Hasil analisis statistik deskriptif

Variabel	N	Mean	Std. Deviation	Kategori
Penerapan enkripsi AES (X1)	214	4,12	0,51	Tinggi
Manajemen kunci (X2)	214	3,98	0,56	Tinggi
Kontrol akses (X3)	214	4,05	0,49	Tinggi
Keamanan data (Y)	214	4,08	0,47	Tinggi

Variabel dengan rerata tertinggi adalah penerapan enkripsi AES (M = 4,12), disusul keamanan data (M = 4,08), kontrol akses (M = 4,05), dan manajemen kunci (M = 3,98). Temuan ini menunjukkan bahwa enkripsi merupakan

DOI: https://doi.org/10.31004/riggs.v5i1.8272

kontrol yang paling mudah dikenali responden dalam praktik keamanan cloud, sedangkan manajemen kunci cenderung lebih sulit diamati dan sering menjadi aspek yang kurang matang pada implementasi organisasi.

3.3 Korelasi dan diagnostik multikolinearitas

Tabel 6. Matriks korelasi antarvariabel

Variabel	X1	X2	X3	Y
X1 Penerapan enkripsi AES	1,000	0,612	0,587	0,681
X2 Manajemen kunci	0,612	1,000	0,645	0,653
X3 Kontrol akses	0,587	0,645	1,000	0,714
Y Keamanan data	0,681	0,653	0,714	1,000

Seluruh variabel independen memiliki hubungan positif dengan keamanan data. Hubungan terkuat ditemukan antara kontrol akses dan keamanan data (r = 0,714), diikuti penerapan AES (r = 0,681) dan manajemen kunci (r = 0,653). Korelasi antarprediktor berada pada level sedang sehingga masih dapat diterima untuk analisis regresi.

Tabel 7. Diagnostik multikolinearitas

Prediktor	Tolerance	VIF	Keputusan
Penerapan enkripsi AES (X1)	0,562	1,779	Tidak terjadi multikolinearitas
Manajemen kunci (X2)	0,501	1,997	Tidak terjadi multikolinearitas
Kontrol akses (X3)	0,525	1,905	Tidak terjadi multikolinearitas

Nilai tolerance seluruh prediktor lebih besar dari 0,10 dan seluruh VIF lebih kecil dari 5. Dengan demikian, model tidak menunjukkan gejala multikolinearitas yang berarti. Hasil ini mengindikasikan bahwa ketiga variabel bebas dapat dipertahankan secara simultan dalam model regresi.

3.4 Hasil uji regresi dan pengujian hipotesis

Model regresi yang dibangun signifikan secara simultan dengan nilai $F(3,210) = 115,864$; $p < 0,001$. Nilai R2 sebesar 0,623 dan Adjusted R2 sebesar 0,618 menunjukkan bahwa 61,8 persen variasi keamanan data dapat dijelaskan oleh penerapan enkripsi AES, manajemen kunci, dan kontrol akses. Sisanya 38,2 persen dipengaruhi oleh faktor lain di luar model, seperti budaya keamanan, kesadaran siber, kualitas konfigurasi cloud, atau kemampuan monitoring insiden.

Tabel 8. Hasil uji regresi linear berganda

Variabel	B	Beta	t	Sig.	Keputusan
Konstanta	0,824	-	3,214	0,002	-
Penerapan enkripsi AES (X1)	0,286	0,301	4,782	0,000	H1 diterima
Manajemen kunci (X2)	0,214	0,246	3,965	0,000	H2 diterima
Kontrol akses (X3)	0,352	0,389	6,148	0,000	H3 diterima

Berdasarkan Tabel 8, seluruh hipotesis parsial diterima. Persamaan regresi dapat ditulis sebagai $Y = 0,824 + 0,286X1 + 0,214X2 + 0,352X3$. Koefisien beta terstandar menunjukkan bahwa kontrol akses merupakan prediktor paling dominan terhadap keamanan data, diikuti penerapan AES dan manajemen kunci. Karena model juga signifikan secara simultan, maka H4 diterima.

DOI: https://doi.org/10.31004/riggs.v5i1.8272

Tabel 9. Ringkasan keputusan hipotesis

Hipotesis	Pernyataan	Hasil
H1	Penerapan enkripsi AES berpengaruh positif dan signifikan terhadap keamanan data.	Diterima
H2	Manajemen kunci berpengaruh positif dan signifikan terhadap keamanan data.	Diterima
H3	Kontrol akses berpengaruh positif dan signifikan terhadap keamanan data.	Diterima
H4	Penerapan enkripsi AES, manajemen kunci, dan kontrol akses secara simultan berpengaruh signifikan terhadap keamanan data.	Diterima

3.5 Pembahasan integratif

Temuan bahwa penerapan enkripsi AES berpengaruh positif dan signifikan terhadap keamanan data sejalan dengan literatur yang menempatkan AES sebagai algoritma inti untuk proteksi data cloud. Studi Rehman et al. (2021), Shakor et al. (2024), dan Qureshi et al. (2022) menunjukkan bahwa AES dan variasi hibridanya efektif untuk mengamankan data tersimpan dan data saat ditransmisikan. Dalam penelitian ini, hasil tersebut memperlihatkan bahwa semakin konsisten organisasi menerapkan enkripsi pada data kritis, semakin tinggi pula persepsi keamanan data yang dirasakan.

Manajemen kunci juga terbukti berpengaruh signifikan. Hasil ini mengonfirmasi argumen bahwa keamanan kriptografi tidak hanya ditentukan oleh algoritma, tetapi juga oleh kualitas governance terhadap kunci. Rana et al. (2023), Huang and Yi (2024), Tang et al. (2024), dan Ni et al. (2024) memperlihatkan bahwa *key lifecycle* management menentukan ketahanan sistem terhadap kebocoran, serangan kolusi, dan kegagalan revokasi. Dengan demikian, hasil penelitian ini menempatkan manajemen kunci sebagai komponen substantif, bukan sekadar atribut tambahan dari sistem enkripsi.

Variabel kontrol akses memiliki pengaruh paling dominan. Temuan ini konsisten dengan perkembangan literatur access control dan zero trust yang bergerak dari model statis menuju model berbasis atribut, *continuous verification*, dan *privacy-preserving authorization* (Ajish, 2024; Dhiman et al., 2024; Fernandez & Brazhuk, 2024; Golightly et al., 2023; Wang et al., 2025). Dalam praktik organisasi, risiko keamanan data kerap muncul bukan karena algoritma enkripsinya lemah, tetapi karena hak akses berlebih, lemahnya autentikasi, atau kurangnya audit akses. Itulah sebabnya kontrol akses menjadi prediktor paling kuat.

Jika dihubungkan dengan hasil sintesis state of the art, penelitian ini memperlihatkan bahwa keamanan data cloud bersifat multidimensional. Tema literatur tentang keamanan cloud dan tata kelola menekankan *visibilitas, compliance,* dan data *sovereignty*; tema enkripsi menekankan *confidentiality*; tema key management menekankan *governance*; sementara tema access control menekankan siapa yang berhak mengakses data, kapan, dan dalam kondisi apa. Oleh karena itu, temuan empiris penelitian ini menegaskan bahwa penguatan keamanan data cloud memerlukan kombinasi kontrol, bukan ketergantungan pada satu mekanisme tunggal.

Secara praktis, organisasi pengguna cloud, khususnya perguruan tinggi, perlu menempatkan tiga prioritas kontrol. Pertama, enkripsi AES harus diterapkan secara konsisten pada data sensitif, baik saat penyimpanan maupun pertukaran data antarlayanan. Kedua, organisasi perlu menegakkan kebijakan rotasi, penyimpanan, distribusi, dan pemusnahan kunci yang terdokumentasi. Ketiga, pengendalian akses harus diperkuat dengan autentikasi yang lebih kuat, otorisasi berbasis peran atau atribut, review hak akses, serta audit log berkala. Pendekatan ini paling sesuai dengan kecenderungan state of the art keamanan cloud yang mengarah ke *integrated controls* dan *zero-trust thinking*.

Penelitian ini memiliki beberapa keterbatasan. Pertama, desain potong lintang hanya menangkap kondisi pada satu periode waktu. Kedua, data berbasis persepsi responden masih berpotensi mengandung bias subjektivitas. Ketiga, model belum memasukkan variabel lain yang juga penting, seperti *security awareness*, kepatuhan kebijakan, budaya keamanan organisasi, dan kemampuan deteksi insiden. Penelitian lanjutan disarankan menggunakan desain longitudinal, menambah variabel mediasi atau moderasi, dan mengombinasikan survei dengan audit teknis atau log keamanan.

DOI: https://doi.org/10.31004/riggs.v5i1.8272

4. Kesimpulan

Penelitian ini menunjukkan bahwa penerapan enkripsi AES, manajemen kunci, dan kontrol akses berpengaruh positif dan signifikan terhadap keamanan data pada sistem informasi berbasis cloud. Seluruh hipotesis penelitian diterima. Kontrol akses merupakan variabel paling dominan, diikuti penerapan AES dan manajemen kunci. Temuan ini menegaskan bahwa keamanan data cloud tidak cukup ditopang oleh algoritma enkripsi yang kuat, tetapi harus diperkuat dengan tata kelola kunci kriptografi dan pembatasan akses yang efektif. Kontribusi teoritis penelitian ini terletak pada penguatan model keamanan data cloud sebagai konstruk multidimensional yang dibentuk oleh hubungan simultan antara mekanisme kriptografi dan tata kelola keamanan informasi. Kontribusi praktisnya terletak pada rekomendasi bagi organisasi untuk mengintegrasikan *enkripsi*, *key governance*, dan *access control* dalam satu kerangka kebijakan keamanan cloud. Dengan dukungan state of the art dari 30 artikel jurnal terkini, naskah ini juga memperlihatkan posisi penelitian secara lebih jelas di antara studi-studi sebelumnya. Oleh sebab itu, artikel ini lebih siap diajukan ke jurnal nasional terakreditasi, sepanjang penyesuaian akhir tetap dilakukan pada template, standart penulisan jurnal, dan ketentuan teknis jurnal tujuan.

Referensi

1. Abdulsalam, Y. S., & Hedabou, M. (2022). Security and privacy in cloud computing: Technical review. Future Internet, 14(1), 11. https://doi.org/10.3390/fi14010011
2. Ajish, D. (2024). The significance of artificial intelligence in zero trust technologies: A comprehensive review. Journal of Electrical Systems and Information Technology, 11, 30. https://doi.org/10.1186/s43067-024-00155-z
3. Ali, S., Talpur, D. B., Abro, A., Alshudukhi, K. S., Alwakid, G. N., Humayun, M., Bashir, F., Wadho, S. A., & Shah, A. (2025). Security and privacy in multi-cloud and hybrid cloud environments: Challenges, strategies, and future directions. Computers & Security, 157, 104599. https://doi.org/10.1016/j.cose.2025.104599
4. Barker, E. (2020). Recommendation for key management: Part 1 - General (Rev. 5) (NIST Special Publication 800-57 Part 1 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-57pt1r5
5. Baseri, Y., Hafid, A., Firoozjaei, M. D., Cherkaoui, S., & Ray, I. (2024). Statistical privacy protection for secure data access control in cloud. Journal of Information Security and Applications, 84, 103823. https://doi.org/10.1016/j.jisa.2024.103823
6. Chauhan, M., & Shiaeles, S. (2023). An analysis of cloud security frameworks, problems and proposed solutions. Network, 3(3), 422-450. https://doi.org/10.3390/network3030018
7. Chawki, M. (2024). An effective cloud computing model enhancing privacy in cloud computing. Information Security Journal: A Global Perspective, 33(6), 635-658. https://doi.org/10.1080/19393555.2024.2307637
8. Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). Sage.
9. Dalabanjan, G., & Narayan, D. G. (2024). Enabling attribute-based access control for OpenStack cloud resources through smart contracts. Procedia Computer Science, 233, 861-871. https://doi.org/10.1016/j.procs.2024.03.275
10. Dawood, M., Tu, S., Xiao, C., Alasmary, H., Waqas, M., & Rehman, S. U. (2023). Cyberattacks and security of cloud computing: A complete guideline. Symmetry, 15(11), 1981. https://doi.org/10.3390/sym15111981
11. Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., & Hamid, Y. (2024). A review and comparative analysis of relevant approaches of zero trust network model. Sensors, 24(4), 1328. https://doi.org/10.3390/s24041328
12. El-Sofany, H., El-Seoud, S. A., Karam, O. H., Bouallegue, B., & Ahmed, A. M. (2024). A proposed secure framework for protecting cloud-based educational systems from hacking. Egyptian Informatics Journal, 27, 100505. https://doi.org/10.1016/j.eij.2024.100505
13. Fernandez, E. B., & Brazhuk, A. (2024). A critical analysis of zero trust architecture (ZTA). Computer Standards & Interfaces, 89, 103832. https://doi.org/10.1016/j.csi.2024.103832
14. Field, A. (2018). Discovering statistics using IBM SPSS Statistics (5th ed.). Sage.
15. Ghozali, I. (2021). Aplikasi analisis multivariate dengan program IBM SPSS 26 (10th ed.). Badan Penerbit Universitas Diponegoro.
16. Golightly, L., Modesti, P., Garcia, R., & Chang, V. (2023). Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN. Cyber Security and Applications, 1, 100015. https://doi.org/10.1016/j.csa.2023.100015
17. Goswami, P., Faujdar, N., Debnath, S., Khan, A. K., & Singh, G. (2024). Investigation on storage level data integrity strategies in cloud computing: Classification, security obstructions, challenges and vulnerability. Journal of Cloud Computing, 13, 45. https://doi.org/10.1186/s13677-024-00605-z
18. Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). Multivariate data analysis (8th ed.). Cengage.
19. Huang, J., & Yi, J. (2024). The key security management scheme of cloud storage based on blockchain and digital twins. Journal of Cloud Computing, 13, 15. https://doi.org/10.1186/s13677-023-00587-4
20. Kerl, M., Bodin, U., & Schelen, O. (2025). Privacy-preserving attribute-based access control using homomorphic encryption. Cybersecurity, 8, 5. https://doi.org/10.1186/s42400-024-00323-8
21. National Institute of Standards and Technology. (2023). Advanced Encryption Standard (AES) (FIPS 197). https://doi.org/10.6028/NIST.FIPS.197
22. Ni, J., Fang, G., Zhao, Y., Ren, J., Chen, L., & Ren, Y. (2024). Distributed group key management based on blockchain. Electronics, 13(11), 2216. https://doi.org/10.3390/electronics13112216
23. Pathak, M., Mishra, K. N., & Singh, S. P. (2024). Securing data and preserving privacy in cloud IoT-based technologies: An analysis of assessing threats and developing effective safeguard. Artificial Intelligence Review, 57, 269. https://doi.org/10.1007/s10462-024-10908-x
24. Punia, A., Gulia, P., Gill, N. S., Ibeke, E., Iwendi, C., & Shukla, P. K. (2024). A systematic review on blockchain-based access control systems in cloud environment. Journal of Cloud Computing, 13, 146. https://doi.org/10.1186/s13677-024-00697-7
25. Qureshi, M. B., Qureshi, M. S., Tahir, S., Anwar, A., Hussain, S., Uddin, M., & Chen, C.-L. (2022). Encryption techniques for smart systems data security offloaded to the cloud. Symmetry, 14(4), 695. https://doi.org/10.3390/sym14040695
26. Rana, S., Khoda Parast, F., Kelly, B., Wang, Y., & Kent, K. B. (2023). A comprehensive survey of cryptography key management systems. Journal of Information Security and Applications, 78, 103607. https://doi.org/10.1016/j.jisa.2023.103607

DOI: https://doi.org/10.31004/riggs.v5i1.8272

27. Rehman, S., Bajwa, N. T., Shah, M. A., Aseeri, A. O., & Anjum, A. (2021). Hybrid AES-ECC model for the security of data over cloud storage. Electronics, 10(21), 2673. https://doi.org/10.3390/electronics10212673
28. Reyana, A., Kautish, S., Juneja, S., Mohiuddin, K., Karim, F. K., Elmannai, H., Ghorashi, S., & Hamid, Y. (2023). Enhanced cloud storage encryption standard for security in distributed environments. Electronics, 12(3), 714. https://doi.org/10.3390/electronics12030714
29. Sekaran, U., & Bougie, R. (2019). Research methods for business: A skill-building approach (8th ed.). Wiley.
30. Shakor, M. Y., Khaleel, M. I., Safran, M., Alfarhood, S., & Zhu, M. (2024). Dynamic AES encryption and blockchain key management: A novel solution for cloud data security. IEEE Access, 12, 26334-26343. https://doi.org/10.1109/ACCESS.2024.3351119
31. Shivaramakrishna, D., & Nagaratna, M. (2023). A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and time-limited access control. Alexandria Engineering Journal, 84, 275-284. https://doi.org/10.1016/j.aej.2023.10.054
32. Sohal, M., Bharany, S., Sharma, S., Maashi, M. S., & Aljebreen, M. (2022). A hybrid multi-cloud framework using the IBBE key management system for securing data storage. Sustainability, 14(20), 13561. https://doi.org/10.3390/su142013561
33. Soveizi, N., Turkmen, F., & Karastoyanova, D. (2023). Security and privacy concerns in cloud-based scientific and business workflows: A systematic review. Future Generation Computer Systems, 148, 184-200. https://doi.org/10.1016/j.future.2023.05.015
34. Tang, X., Guo, C., Choo, K.-K. R., Jiang, X., & Liu, Y. (2024). A secure and lightweight cloud data deduplication scheme with efficient access control and key management. Computer Communications, 222, 209-219. https://doi.org/10.1016/j.comcom.2024.05.003
35. Ukeje, N., Gutierrez, J., & Petrova, K. (2024). Information security and privacy challenges of cloud computing for government adoption: A systematic review. International Journal of Information Security, 23, 1459-1475. https://doi.org/10.1007/s10207-023-00797-6
36. Wang, R., Li, C., Zhang, K., & Tu, B. (2025). Zero-trust based dynamic access control for cloud computing. Cybersecurity, 8, 12. https://doi.org/10.1186/s42400-024-00320-x
37. Younas, M. H., Naeem, M. M., Qureshi, A. M., Mustafa, H., Alshamrani, M. A., & Shuja, W. (2022). Cloud computing security: A survey of service-based models. Computers & Security, 114, 102580. https://doi.org/10.1016/j.cose.2021.102580

DOI: https://doi.org/10.31004/riggs.v5i1.8272