Journal of Information and Information Security (JIFORTY)
Vol. 6, No. 2, Desember 2025, *105-114*
e-ISSN : 2722-4058
Available Online at http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Studi Perbandingan Model Keamanan Data pada Cloud Computing

Allan Desi Alexander [1,*]

[1]Informatika; Fakultas Ilmu Komputer; Universitas Bhayangkara Jakarta Raya; Jl. Raya Perjuangan No.81 Margamulya, Kota Bekasi, Jawa Barat, Telp. (021) 7231948; e-mail: allan@ubharajaya.ac.id

* Korespondensi: allan@ubharajaya.ac.id

Diterima:5 Jan 2026; Review: 7 Jan 2026; Disetujui: 9 Jan 2026; Diterbitkan: 9 Jan 2026

Abstract

Cloud computing services have become the backbone of global digital transformation, offering unprecedented scalability, cost efficiency, and flexibility. However, migrating data to third-party multi-tenant environments raises serious concerns regarding data security and privacy. This research report presents a comprehensive analysis of data security models in the cloud ecosystem, covering cryptographic aspects, access control mechanisms, and risk management strategies. Through a systematic literature review of Scopus and SINTA-indexed studies between 2013 and 2025, this study evaluates the performance of encryption algorithms such as AES, RSA, and ECC, and compares the effectiveness of Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) models. Key findings indicate that symmetric algorithms like AES excel in speed and memory efficiency for bulk data, while asymmetric models like RSA are more optimal for key management. In terms of access control, ABAC offers higher flexibility for dynamic environments compared to static RBAC, despite its greater implementation complexity. This study also highlights the role of cutting-edge technologies such as blockchain, machine learning, and federated learning in strengthening cloud security posture and provides a risk management framework for organizations undergoing data migration.
***Keywords**: Cloud Computing, Data Security, Encryption, Access Control, Risk Management, Hybrid Cryptography.*

Abstrak

Layanan komputasi awan (cloud computing) telah menjadi tulang punggung transformasi digital global, menawarkan skalabilitas, efisiensi biaya, dan fleksibilitas yang belum pernah ada sebelumnya. Namun, perpindahan data dari infrastruktur lokal ke lingkungan pihak ketiga yang bersifat multi-tenant menimbulkan kekhawatiran serius terhadap keamanan dan privasi data. Laporan penelitian ini menyajikan analisis komprehensif mengenai perbandingan model keamanan data dalam ekosistem cloud, mencakup aspek kriptografi, mekanisme kontrol akses, dan strategi manajemen risiko. Melalui tinjauan literatur sistematis terhadap studi yang terindeks Scopus dan SINTA antara tahun 2013 hingga 2025, penelitian ini mengevaluasi kinerja algoritma enkripsi seperti AES, RSA, dan ECC, serta membandingkan efektivitas model Role-Based Access Control (RBAC) dan Attribute-Based Access Control (ABAC). Temuan utama menunjukkan bahwa algoritma simetris seperti AES unggul dalam kecepatan dan efisiensi memori untuk data massal, sementara model asimetris seperti RSA lebih optimal untuk manajemen kunci. Dalam hal kontrol akses, ABAC menawarkan fleksibilitas yang lebih tinggi untuk lingkungan dinamis dibandingkan RBAC yang bersifat statis, meskipun memiliki kompleksitas implementasi yang lebih besar. Penelitian ini juga menyoroti peran teknologi mutakhir seperti blockchain, machine learning, dan federated learning dalam memperkuat postur keamanan cloud serta memberikan kerangka kerja manajemen risiko bagi organisasi yang melakukan migrasi data..

Kata kunci: Cloud Computing, Keamanan Data, Enkripsi, Kontrol Akses, Manajemen Risiko, Kriptografi Hybrid.

1. Pendahuluan

Pesatnya perkembangan teknologi informasi telah membawa paradigma baru dalam pengelolaan data melalui implementasi cloud computing. Teknologi ini memungkinkan akses on-demand ke sumber daya komputasi yang dapat dikonfigurasi secara cepat dengan upaya manajemen yang minimal. Transformasi digital ini tidak hanya menyentuh sektor bisnis skala besar, tetapi juga telah merambah ke berbagai platform hiburan dan media sosial populer seperti Instagram, WhatsApp, TikTok, Netflix, dan Spotify. Dalam konteks industri, cloud computing berfungsi sebagai fasilitas pembelajaran di sektor pendidikan, penyedia layanan konsultasi di sektor kesehatan, dan pendukung operasional di sektor transportasi. Meskipun manfaat ekonomis dan operasionalnya sangat signifikan, tantangan keamanan tetap menjadi hambatan utama bagi adopsi luas teknologi ini.(Pandu et al., 2025)(Zahra et al., 2023)

Keamanan cloud bukan sekadar masalah teknis, melainkan isu multidimensi yang mencakup aspek kerahasiaan *(confidentiality)*, integritas *(integrity)*, dan ketersediaan (availability) data.(Alkadrie & Fitroh, 2024) Organisasi yang memindahkan data sensitif mereka ke cloud sering kali menghadapi risiko kehilangan kendali *(loss of governance)*, di mana pelanggan tidak dapat secara langsung mengontrol sistem yang memproses data mereka karena server berada di luar domain internal perusahaan. Selain itu, sifat *multi-tenancy* pada cloud, yang memungkinkan beberapa pengguna berbagi infrastruktur fisik yang sama, menciptakan potensi kebocoran privasi antar pengguna *(inter-user privacy leaks)* yang sangat berbahaya.(Kusyanti2 et al., 2018)

Berbagai model keamanan telah dikembangkan untuk memitigasi risiko ini. Kriptografi, sebagai studi tentang pengamanan data, telah mengintegrasikan algoritma-algoritma baru untuk memastikan bahwa hanya pihak yang berwenang yang dapat mengakses informasi yang disimpan secara online. Di sisi lain, mekanisme kontrol akses berkembang dari model tradisional berbasis peran menuju model yang lebih cerdas dan adaptif terhadap konteks. Namun, efektivitas model-model ini sangat bergantung pada skenario aplikasi dan karakteristik beban kerja masing-masing organisasi.(Umar et al., 2023)

Pentingnya pemahaman mendalam mengenai perbandingan model keamanan data ini ditekankan oleh fakta bahwa ancaman siber terus berevolusi. Serangan seperti *Distributed Denial-of-Service (DDoS), malware*, dan pembajakan akun tetap menjadi ancaman persisten.(Ahmadi, 2024) Selain itu, kerentanan pada antarmuka pemrograman aplikasi (API) dan kurangnya literasi digital pengguna sering kali menjadi celah yang dieksploitasi oleh penyerang.(Rozi et al., 2024) Oleh karena itu, penelitian ini bertujuan untuk menyajikan analisis mendalam mengenai efektivitas berbagai teknik perlindungan data saat ini, keunggulan dan keterbatasan masing-masing metode, serta tren masa depan dalam penguatan keamanan cloud storage.(Mutiara Dewi et al., 2025)

2. Metode Penelitian

Penelitian ini mengadopsi metodologi tinjauan literatur sistematis *(Systematic Literature Review - SLR)* yang berpedoman pada protokol PRISMA *(Preferred Reporting Items for Systematic Reviews and Meta-Analyses)* (Le et al., 2025). Langkah pertama melibatkan identifikasi kebutuhan penelitian dan perumusan pertanyaan kunci mengenai teknik perlindungan data yang paling efektif, perbandingan keuntungan dan keterbatasan masing-masing teknik, serta kerentanan utama yang terkait dengan setiap model.(El Moudni & Ziyati, 2025)

Proses pencarian literatur dilakukan melalui pangkalan data akademik bereputasi, termasuk IEEE Xplore, ScienceDirect, ACM, SpringerLink, Scopus, dan jurnal-jurnal yang terakreditasi SINTA. Kata kunci yang digunakan dalam pencarian meliputi "*Cloud Computing Security", "Data Encryption Models", "Access Control Comparison*", "RBAC vs ABAC in *Cloud*", dan "*Cloud Risk Management Framework*". Pemilihan studi dilakukan secara ketat dengan kriteria inklusi berupa artikel jurnal dan makalah konferensi yang diterbitkan antara tahun 2013 hingga 2025, dengan fokus utama pada penelitian terbaru (2020-2024) untuk memastikan relevansi terhadap ancaman siber kontemporer.(Diningrat et al., 2025)

Tahap penyaringan awal melibatkan analisis terhadap ribuan makalah, yang kemudian dikerucutkan menjadi studi-studi yang secara spesifik membahas mekanisme keamanan, ancaman siber, dan solusi mitigasi dalam konteks cloud. Data yang diekstraksi dari literatur yang terpilih mencakup parameter kinerja algoritma kriptografi (waktu eksekusi, penggunaan CPU, konsumsi memori), karakteristik model kontrol akses, serta efektivitas teknologi integrasi seperti *blockchain* dan *machine learning*. Analisis data dilakukan dengan pendekatan deskriptif kualitatif untuk mensintesis teori dan pendekatan komparatif untuk mengevaluasi hasil *benchmarking* algoritma.(Pandu et al., 2025)

3. Hasil dan Pembahasan.

3.1 Proses Seleksi Literatur

Proses tinjauan literatur sistematis ini dilakukan secara terstruktur untuk memastikan objektivitas temuan. Pencarian awal menggunakan kata kunci yang luas menghasilkan lebih dari 1.000 artikel potensial. Melalui beberapa tahap penyaringan yang meliputi evaluasi judul, abstrak, dan pemeriksaan teks lengkap (*full-text*), literatur disaring secara ketat untuk menyisakan studi yang paling relevan dengan konteks keamanan cloud tingkat perusahaan.

Rincian langkah seleksi literatur disajikan sebagai berikut:

1. Tahap Penemuan: Identifikasi awal melalui basis data akademik dengan kriteria "*cybersecurity analytics*" dan "*cloud security threats*".
2. Tahap Penyaringan: Penghapusan duplikasi dan penilaian relevansi judul/abstrak.
3. Tahap Penilaian Kualitas: Analisis mendalam terhadap metodologi penelitian dan hasil eksperimen yang disajikan dalam makalah.

4. Tahap Sintesis: Pengelompokan studi ke dalam kategori tematik seperti kriptografi simetris/asimetris, model kontrol akses (RBAC vs ABAC), dan integrasi teknologi AI/Blockchain.

Staistik seleksi literatur untuk melakukan analisis dapat dilihat pada tabel berikut

Tabel 1. Tahapan seleksi literatur

Tahapan Seleksi	Deskripsi Aktivitas	Jumlah Literatur
Pencarian Awal	Pencarian berbasis kata kunci pada 6 basis data utama (Scopus, SINTA, IEEE, dll).	> 1.000
Penyaringan Awal	Penghapusan artikel duplikat dan judul yang tidak relevan.	400
Penilaian Kelayakan	Peninjauan abstrak dan teks lengkap berdasarkan kriteria inklusi/eksklusi.	150
Studi Akhir (Inklusi)	Literatur terpilih yang dianalisis secara mendalam untuk sintesis data.	65 - 87

Sumber: Hasil Penelitian (2025)

Pada tabel 1 menjelaskan diidentifikasi adanya transisi industri dari alat deteksi berbasis tanda tangan tradisional menuju teknik bertenaga kecerdasan buatan dan analisis big data yang lebih proaktif.

3.2 Taksonomi Ancaman dan Kerentanan pada Komputasi Awan

Lingkungan komputasi awan menghadapi spektrum ancaman yang luas yang menargetkan berbagai lapisan infrastruktur dan aplikasi. Analisis terhadap literatur menunjukkan bahwa ancaman ini dapat dikategorikan menjadi risiko teknis dan risiko organisasional. Keamanan pada cloud secara konsisten menjadi kekhawatiran nomor satu dibandingkan isu reliabilitas atau ketersediaan jaringan, mengingat besarnya dampak yang ditimbulkan oleh pelanggaran data.

Tabel 2. Dampak ancaman terhadap organisasi

Jenis Ancaman	Deskripsi Mekanisme	Dampak pada Organisasi
Kebocoran Data (Data Breach)	Pengungkapan informasi sensitif kepada pihak yang tidak berwenang akibat kesalahan konfigurasi atau eksploitasi sistem.	Kehilangan kepercayaan pelanggan, sanksi hukum (GDPR/HIPAA), dan denda finansial.

Serangan DDoS	Membanjiri server dengan lalu lintas palsu untuk melumpuhkan ketersediaan layanan cloud.	Gangguan operasional total, penurunan produktivitas, dan kerugian pendapatan.
Insecure APIs	Kerentanan pada antarmuka pihak ketiga yang memungkinkan akses ilegal ke data cloud.	Eksposisi kunci akses, modifikasi data tidak sah, dan manipulasi layanan.
Insider Threats	Penyalahgunaan hak akses oleh karyawan atau pihak internal yang memiliki kredensial sah.	Sabotase sistem dan pencurian kekayaan intelektual yang sulit dideteksi.
Lock-in & Loss of Governance	Ketergantungan pada vendor tertentu dan hilangnya kontrol langsung atas tata kelola data.	Kesulitan migrasi data dan ketidakmampuan memastikan kepatuhan regulasi secara mandiri.

Sumber: Hasil Penelitian (2025)

Pada tabel 2 menjelaskan klasifikasi risiko keamanan menjadi dimensi teknis dan organisasional yang muncul akibat sifat fundamental infrastruktur cloud. Kebocoran data dan kehilangan data sering kali dipicu oleh kesalahan konfigurasi sistem atau serangan siber canggih yang mengeksploitasi kerentanan perangkat keras. Selain itu, mekanisme multi-tenancy yang memungkinkan pembagian sumber daya fisik antar pengguna yang berbeda menciptakan celah bagi aktor jahat untuk menyusup melalui mesin virtual (VM) yang tidak dikenal, yang pada akhirnya dapat memicu kebocoran privasi antar pengguna. Kerentanan pada antarmuka pemrograman aplikasi (API) juga menjadi titik kritis karena eksposisi kunci akses sering kali tidak diamankan secara memadai oleh pelanggan cloud saat mengakses layanan pihak ketiga.

Dampak yang ditimbulkan dari ancaman-ancaman ini bersifat multidimensi, mulai dari gangguan operasional total hingga konsekuensi hukum yang berat bagi perusahaan. Serangan DDoS, misalnya, dapat melumpuhkan layanan secara real-time dan menyebabkan kerugian pendapatan serta penurunan produktivitas yang signifikan bagi organisasi. Di sisi lain, hilangnya tata kelola (*loss of governance*) karena data berada di luar domain internal perusahaan menyulitkan organisasi dalam memastikan kepatuhan terhadap regulasi ketat seperti GDPR, HIPAA, atau PCI DSS. Kegagalan dalam memitigasi risiko ini tidak hanya berujung pada denda finansial, tetapi juga menyebabkan erosi kepercayaan pelanggan secara permanen akibat pelanggaran kerahasiaan data sensitif.

3.3 Analisis Komparatif Model Kriptografi dalam Perlindungan Data

Kriptografi merupakan pilar utama dalam memastikan kerahasiaan dan integritas data di cloud. Berdasarkan mekanisme kuncinya, algoritma dibagi menjadi kriptografi simetris dan asimetris, masing-masing dengan karakteristik kinerja yang unik.(Parekh & Maru, 2025)

Algoritma Simetris: AES dan DES

Advanced Encryption Standard (AES) saat ini diakui sebagai standar global untuk enkripsi data massal. AES menggunakan kunci dengan panjang 128, 192, atau 256 bit dan beroperasi pada blok berukuran 16 byte. (SR et al., 2025) Penelitian menunjukkan bahwa AES menawarkan kecepatan enkripsi dan dekripsi yang superior dibandingkan algoritma lainnya, dengan beban komputasi CPU yang minimal. Sebaliknya, Data Encryption Standard (DES) sudah dianggap tidak aman untuk sistem modern karena ukuran kuncinya yang kecil dan kerentanannya terhadap brute force. (Commey et al., 2020)

Algoritma Asimetris: RSA dan ECC

Rivest-Shamir-Adleman (RSA) adalah algoritma asimetris populer yang menggunakan pasangan kunci publik dan privat. Secara matematis, enkripsi dilakukan dengan rumus:

$$C = P^e mod\ n$$

dan deksripsi dengan;

$$P = C^d mod\ n$$

Analisis performa menunjukkan bahwa RSA memiliki latensi yang jauh lebih tinggi dan penggunaan memori yang lebih besar dibandingkan AES, terutama karena kompleksitas waktu asimtotiknya yang mencapai.

$$O((\log n)^3)$$

Untuk operasi kunci privat Sebagai alternatif, *Elliptic Curve Cryptography* (ECC) menawarkan tingkat keamanan yang setara dengan RSA namun dengan ukuran kunci yang jauh lebih kecil, memberikan efisiensi yang lebih baik pada perangkat dengan sumber daya terbatas.

Tabel 3. Perbandingan Kinerja Algoritma Kriptografi

Metrik Kinerja	AES (Advanced Encryption Standard)	RSA (Rivest-Shamir-Adleman)	DES (Data Encryption Standard)
Kecepatan Eksekusi	Sangat Tinggi	Rendah	Sedang
Penggunaan CPU	Sangat Efisien	Intensif	Tidak Efisien (Sistem Baru)
Kebutuhan Memori	Rendah	Tinggi	Sedang
Tingkat Keamanan	Sangat Tinggi	Tinggi (Tergantung Panjang Kunci)	Rendah (Rentan)

Sumber: Hasil Penelitian (2025)

Pada tabel 3 menjelaskan kecenderungan saat ini adalah penggunaan model hybrid yang memanfaatkan kecepatan AES untuk enkripsi data utama, sementara kunci AES tersebut diamankan menggunakan algoritma RSA atau ECC.

3.4 Evolusi Model Kontrol Akses: Dari RBAC ke ABAC

Kontrol akses kritis mengatur interaksi antara pengguna dan sumber daya. Dua model utama adalah *Role-Based Access Control* (RBAC) dan *Attribute-Based Access Control* (ABAC).

***Role-Based Access Control* (RBAC)**

RBAC memberikan hak akses berdasarkan peran pekerjaan. Dalam aplikasi ERP berbasis *cloud*, implementasi RBAC yang dikombinasikan dengan *machine learning* telah terbukti meningkatkan keamanan hingga 37% dan mengurangi biaya operasional sebesar 42%. Namun, RBAC memiliki keterbatasan berupa "*role explosion*", di mana jumlah peran menjadi terlalu banyak dan sulit dikelola seiring pertumbuhan organisasi, serta tidak mampu mempertimbangkan faktor kontekstual. (Zahra et al., 2023)

***Attribute-Based Access Control* (ABAC)**

ABAC menawarkan kontrol lebih halus (*fine-grained*) dengan mengevaluasi atribut dari subjek, sumber daya, tindakan, dan lingkungan secara real-time. Dalam skenario medis yang kritis seperti perawatan stroke akut (*Acute Care*), model AC-ABAC memungkinkan tim medis mendapatkan akses instan ke data pasien selama masa darurat dan mencabutnya secara otomatis setelah perawatan berakhir. Meskipun evaluasi kebijakan ABAC lebih kompleks dan memakan waktu rata-rata 194,89 ms, nilai tambah keselamatannya dianggap sepadan.(Priyambodo et al., 2024)

Tabel 4. Analisis Perbandingan RBAC dan ABAC

Kriteria Perbandingan	Role-Based Access Control (RBAC)	Attribute-Based Access Control (ABAC)
Basis Keputusan Akses	Peran statis (Admin, Perawat).	Atribut dinamis (Subjek, Objek, Konteks).
Tingkat Fleksibilitas	Rendah; kaku terhadap perubahan konteks.	Sangat Tinggi; adaptasi real-time.
Keamanan	Satu lapis (Single-layer).	Multi-lapis (berbasis konteks).

Sumber: Hasil Penelitian (2025)

Pada tabel 4 menjelaskan ilustrasi pergeseran paradigma dari pendekatan berbasis peran yang statis menuju kebijakan yang lebih granular dan berbasis atribut. RBAC berfungsi sebagai model keamanan "satu lapis" di mana izin dikaitkan secara kaku dengan jabatan pekerjaan, yang

meskipun menyederhanakan manajemen di lingkungan stabil, sering kali menciptakan kendala besar di *cloud* yang dinamis. Seiring pertumbuhan organisasi, model ini rentan terhadap fenomena "*role explosion*", di mana jumlah peran yang ditentukan menjadi tidak terkendali karena ketidakmampuannya untuk mempertimbangkan variabel lingkungan yang berubah-ubah. Hal ini menyebabkan kontrol akses yang bersifat umum (*coarse-grained*) yang sering kali tidak memadai untuk melindungi data sensitif pada platform multi-tenant.

Sebaliknya, ABAC memperkenalkan keamanan "multi-lapis" dengan mengevaluasi kumpulan atribut yang kaya termasuk identitas pengguna, *sensitivitas* sumber daya, dan data lingkungan *real-time* seperti waktu dan Lokasi untuk membuat keputusan akses pada saat *runtime*. Pendekatan "halus" (*fine-grained*) ini memungkinkan penerapan aturan bisnis yang sangat spesifik, seperti pembatasan akses ke catatan keuangan hanya pada jam kerja atau pemberian akses darurat sementara bagi tim medis seperti yang terlihat pada model AC-ABAC. Meskipun hal ini menyebabkan kompleksitas kebijakan yang lebih tinggi dan peningkatan latensi evaluasi (rata-rata mencapai 194,89 ms untuk kebijakan kompleks), data menunjukkan bahwa pertukaran ini sangat diperlukan bagi industri yang teregulasi ketat guna memenuhi kepatuhan terhadap standar seperti GDPR atau HIPAA.

3.5 Implementasi Teknologi Mutakhir dalam Penguatan Manajemen Risiko

Integrasi teknologi baru telah memperluas kapabilitas keamanan cloud. Blockchain digunakan untuk meningkatkan transparansi dan kepercayaan dengan mencatat aktivitas otorisasi pada buku besar yang tidak dapat diubah (*immutable*). Sementara itu, *Machine Learning* (ML) dan *Deep Learning* (DL) memainkan peran krusial dalam melakukan analisis risiko proaktif dan deteksi anomali pada lalu lintas jaringan. Di sisi lain, *Federated Learning* (FL) menawarkan solusi untuk melatih model AI secara lokal di berbagai sumber data tanpa perlu memindahkan data mentah, yang sangat penting bagi pelestarian privasi.(Drissi et al., 2025)

3.6 Kerangka Kerja Manajemen Risiko dan Migrasi Cloud

Proses manajemen risiko yang terstruktur mencakup identifikasi, penilaian, mitigasi, dan pemantauan risiko. Penelitian mengenai migrasi aplikasi logistik menunjukkan bahwa nilai risiko sistem sering kali meningkat selama proses migrasi dibandingkan dengan kondisi sebelum migrasi karena kompleksitas integrasi antar domain.

Tabel 5. Fokus resiko tiap fase migrasi

Fase Migrasi	Fokus Risiko
Sebelum Migrasi	Kesiapan infrastruktur dan kebijakan privasi.
Selama Migrasi	Gangguan layanan dan kegagalan integritas data.
Setelah Migrasi	Kebocoran data akibat multi-tenancy dan insider threats.

Sumber: Hasil Penelitian (2025)

Pada tabel 5 menjelaskan Fokus resiko tiap fase migrasi.

4. Kesimpulan

Penelitian ini menyimpulkan bahwa perlindungan data yang optimal dalam ekosistem cloud memerlukan integrasi berbagai model keamanan secara berlapis. Algoritma kriptografi simetris AES terbukti paling efisien untuk pengamanan data massal karena keunggulan kecepatan dan penggunaan memori yang rendah, sementara algoritma asimetris seperti RSA atau ECC lebih tepat digunakan untuk manajemen kunci melalui skema hybrid guna memastikan keamanan pertukaran data. Dalam aspek kontrol akses, transisi dari model RBAC yang statis menuju ABAC yang dinamis menjadi krusial untuk menangani kompleksitas lingkungan cloud modern, terutama dalam skenario khusus seperti layanan kesehatan darurat yang membutuhkan otorisasi berbasis konteks. Selain itu, efektivitas keamanan jangka panjang sangat bergantung pada adopsi teknologi proaktif seperti blockchain untuk menjamin transparansi serta machine learning untuk analisis risiko dan deteksi anomali yang presisi.

Berdasarkan temuan tersebut, direkomendasikan agar penelitian selanjutnya mengeksplorasi pengembangan analitik keamanan yang dapat diskalakan secara real-time dan penciptaan bahasa kebijakan terpadu untuk memudahkan implementasi ABAC di berbagai platform cloud heterogen. Mengingat munculnya ancaman komputasi kuantum terhadap algoritma asimetris tradisional, transisi menuju kriptografi pasca-kuantum (PQC) menjadi area penelitian mendesak untuk menjaga ketahanan sistem di masa depan. Pengembangan solusi keamanan yang lebih terjangkau dan berorientasi pada usaha kecil dan menengah (UKM) juga diperlukan untuk menjembatani kesenjangan kompetensi dan biaya implementasi. Terakhir, integrasi teknik *Federated Learning* (FL) perlu terus dikembangkan dalam sistem cloud terdistribusi (DCC) agar organisasi dapat melakukan pelatihan model kecerdasan buatan secara kolaboratif tanpa harus memindahkan data mentah pengguna, sehingga kepatuhan terhadap privasi data tetap terjaga secara optimal.

Daftar Pustaka

Ahmadi, S. (2024). Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *Journal of Information Security*, *15*(02), 148–167. https://doi.org/10.4236/jis.2024.152010

Alkadrie, S. A., & Fitroh. (2024). Keamanan Cloud Computing di Era Industri 4.0: Systematic Literature Review. *KONSTELASI: Konvergensi Teknologi Dan Sistem Informasi*, *4*(2), 1–15. https://doi.org/10.24002/konstelasi.v4i2.10277

Commey, D., Griffith, S., & Dzisi, J. (2020). Performance comparison of 3DES, AES, Blowfish and RSA for Dataset Classification and Encryption in Cloud Data Storage. *International Journal of Computer Applications*, *177*(40), 17–22. https://doi.org/10.5120/ijca2020919897

Diningrat, D. C., Suhardi, & Rahardjo, B. (2025). Security Issues in Multi-Cloud: A Systematic Literature Review. *IEEE Access*, *13*, 70006–70017. https://doi.org/10.1109/ACCESS.2025.3561352

Drissi, S., Chergui, M., & Khatar, Z. (2025). A Systematic Literature Review on Risk Assessment

in Cloud Computing: Recent Research Advancements. *IEEE Access*, *13*(March), 76289–76307. https://doi.org/10.1109/ACCESS.2025.3561123

El Moudni, M., & Ziyati, E. (2025). Advances and Challenges in Cloud Data Storage Security: A Systematic Review. *International Journal of Safety and Security Engineering*, *15*(4), 653–675. https://doi.org/10.18280/ijsse.150403

Kusyanti2, A., Amron, K., & Mohammad, F. (2018). Pengamanan Data pada Media Penyimpanan Cloud Menggunakan Teknik Enkripsi dan Secret Sharing. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *Vol. 2*, *No*(11), 4863–4869. http://j-ptiik.ub.ac.id

Le, T. D., Le-Dinh, T., & Uwizeyemungu, S. (2025). Cybersecurity Analytics for the Enterprise Environment: A Systematic Literature Review. *Electronics*, *14*(11), 2252. https://doi.org/10.3390/electronics14112252

Mutiara Dewi, E., Surur, M., Izaki, M., Informatika, T., YMI Tegal, S., Pendidikan No, J., & Pesurungan Lor, K. (2025). Analisis Keamanan Data pada Layanan Cloud Computing: Studi Kasus Penyimpanan File di Google Drive. *Jurnal BATIRSI*, *9*(1), 9–12.

Pandu, R. M., Muttaqin, H. A., & Dias, D. S. A. W. (2025). Manajemen Keamanan Data Dalam Era Tansformasi Digital Dan Cloud Computing. *Journal of Informatic and Information Security*, *5*(2), 145–154. https://doi.org/10.31599/f4h0nv04

Parekh, S., & Maru, M. J. (2025). AES, DES, and RSA in Data Security: A Review. *International Journal of Scientific Research and Engineering Development*, *8*(5). www.ijsred.com

Priyambodo, T. K., Prayudi, Y., & Budiarto, R. (2024). ABAC as Access Control Solution for Digital Evidence Storage. *International Journal on Advanced Science, Engineering and Information Technology*, *14*(1), 37–44. https://doi.org/10.18517/ijaseit.14.1.17502

Rozi, F., Ibrahim, anton maulana, & Pujiastuti, E. (2024). Analisis Ancaman Keamanan dalam Penggunaan Teknologi Cloud Computing. *Jurnal Sistem Informasi, Teknologi Informasi Dan Komputer*, *14*(3), 150–233. https://jurnal.umj.ac.id/index.php/just-it/index

SR, S., N, U., R, C., & CM, A. (2025). Comparison Between Encryption Algorithms: A Performance and Security Perspective. *International Journal on Science and Technology*, *16*(3). https://doi.org/10.71097/IJSAT.v16.i3.7986

Umar, D. S., Veeramachineni, V. R., Thummala, R., Ginjupalli, S., & Safare, D. R. (2023). Role-Based Access Control (RBAC) Vs. Attribute-Based Access Control (ABAC) For Cloud Security. *Educational Administration: Theory and Practice*, *29*(3), 1398–1406. https://doi.org/10.53555/kuey.v29i3.9454

Zahra, A. F., Kusuma, Z. H., Putra, I. D., Arifin, R. F., Fadhila, Z. N., Amrozi, Y., & Rozzika, C. (2023). Penelitian Cloud computing pada Industri, Pendidikan, Kesehatan, Transportasi, dan Perbankan. *Jurnal Teknologi Informasi*, *9*(2), 163–171. https://doi.org/10.52643/jti.v9i2.2658