EVOLUSI MEKANISME KEAMANAN DATA DALAM *CLOUD COMPUTING*: SYSTEMATIC LITERATURE REVIEW TERHADAP TEKNIK ENKRIPSI DAN ACCESS CONTROL (2020-2025)

Muhammad Vieri fadli [1], Muhammad Rafly Sugiharto[2], Muhammad Nanda Saputra[3]

[1,2,3] *Program Studi Sistem Informasi*
Fakultas Ilmu Komputer, Universitas Pamulang,
Jl. Raya Puspitek, Buaran, Kec. Pamulang, Kota Tangerang Selatan, Banten 15310

Email : vierifadhli@gmail.com[1] , muhammadrafly281299@gmail.com[2] , muhammadnandasaputra05@gmail.com[3]

ABSTRAK

EVOLUSI MEKANISME KEAMANAN DATA DALAM CLOUD COMPUTING: SYSTEMATIC LITERATURE REVIEW TERHADAP TEKNIK ENKRIPSI DAN ACCESS CONTROL (2020-2025). Penelitian ini menganalisis evolusi mekanisme keamanan data dalam *cloud computing* dengan fokus pada teknik enkripsi dan *access control* periode 2020-2025 melalui pendekatan *systematic literature review* menggunakan protokol PRISMA. Proses identifikasi literatur menghasilkan 309 artikel dari basis data akademik terkemuka yang kemudian diseleksi secara sistematis melalui tahapan *screening* dan *eligibility assessment*, menghasilkan 10 artikel berkualitas tinggi untuk dianalisis secara mendalam. Hasil penelitian mengidentifikasi bahwa teknik enkripsi mengalami transformasi signifikan dari skema konvensional menuju *Attribute-Based Encryption* (ABE) dan *Attribute-Based Searchable Encryption* (ABSE) yang menawarkan *fine-grained access control* dan kemampuan pencarian pada data terenkripsi. Mekanisme *access control* bertransformasi dari *Role-Based Access Control* (RBAC) menuju *Attribute-Based Access Control* (ABAC) dan *Relationship-Based Access Control* (ReBAC) dengan adopsi *Zero Trust Architecture* sebagai paradigma dominan. Tantangan implementasi mencakup kompleksitas manajemen kunci, *performance overhead*, *misconfiguration*, dan kesenjangan adopsi *post-quantum cryptography*. Teknologi *emerging* seperti *artificial intelligence*, *machine learning*, dan *blockchain* memiliki potensi transformatif dalam meningkatkan efektivitas keamanan melalui deteksi anomali adaptif dan otorisasi dinamis. Penelitian ini merekomendasikan pendekatan *multi-layered security* yang mengintegrasikan enkripsi, *multi-factor authentication*, dan *policy management engines* modern untuk menciptakan ekosistem *cloud computing* yang aman dan resilient terhadap ancaman siber kontemporer.

Kata Kunci: *Access Control*, *Cloud Computing*, Enkripsi

ABSTRACT

EVOLUTION OF DATA SECURITY MECHANISMS IN CLOUD COMPUTING: SYSTEMATIC LITERATURE REVIEW OF ENCRYPTION AND ACCESS CONTROL TECHNIQUES (2020-2025).*This research analyzes the evolution of data security mechanisms in cloud computing with a focus on encryption techniques and access control during the period 2020-2025 through a systematic literature review approach using the PRISMA protocol. The literature identification process yielded 309 articles from leading academic databases which were then systematically selected through screening and eligibility assessment stages, resulting in 10 high-quality articles for in-depth analysis. The research findings identify that encryption techniques have undergone significant transformation from conventional schemes to Attribute-Based Encryption (ABE) and Attribute-Based Searchable Encryption (ABSE) which offer fine-grained access control and search capabilities on encrypted data. Access control mechanisms have transformed from Role-Based Access Control (RBAC) to Attribute-Based Access Control (ABAC) and Relationship-Based Access Control (ReBAC) with the adoption of Zero Trust Architecture as the dominant paradigm. Implementation challenges include key management complexity, performance overhead, misconfiguration, and gaps in post-quantum cryptography adoption. Emerging technologies such as artificial intelligence, machine learning, and blockchain have transformative potential in enhancing security effectiveness through adaptive anomaly detection and dynamic authorization. This research recommends a multi-layered security approach that integrates encryption, multi-f actor authentication, and modern policy management engines to create a cloud computing ecosystem that is secure and resilient against contemporary cyber threats.*

Keywords: *Access Control, Cloud Computing, Encryption*

1. PENDAHULUAN

Transformasi digital yang berlangsung secara masif telah mendorong adopsi teknologi cloud computing sebagai infrastruktur fundamental bagi organisasi modern dalam mengelola sumber daya komputasi dan penyimpanan data. Paradigma cloud computing menawarkan fleksibilitas, skalabilitas, serta efisiensi biaya yang signifikan, sehingga mengubah lanskap teknologi informasi secara mendasar. Namun, transformasi ini juga menghadirkan tantangan kompleks dalam keamanan data, terutama terkait privasi dan perlindungan informasi sensitif di era kecerdasan buatan (Eriana, Zein, & Rozali, 2024). Namun, di balik keunggulan tersebut, muncul tantangan krusial terkait keamanan data yang memerlukan perhatian serius mengingat data sensitif organisasi dan personal disimpan serta diproses melalui infrastruktur berbasis internet yang rentan terhadap berbagai ancaman siber. Kompleksitas arsitektur cloud yang melibatkan multiple stakeholders, shared responsibility model, serta ketergantungan pada konektivitas jaringan menciptakan vektor serangan baru yang memerlukan mekanisme proteksi berlapis dan dinamis. Ancaman keamanan dalam ekosistem cloud computing tidak terbatas pada serangan eksternal semata, namun juga mencakup risiko internal seperti misconfiguration, privilege escalation, dan insider threats yang dapat mengakibatkan kebocoran data dengan konsekuensi hukum dan reputasional yang merugikan. Dalam konteks ini, teknologi enkripsi dan mekanisme access control menjadi dua pilar fundamental yang menentukan tingkat keamanan infrastruktur cloud computing, yang harus didukung oleh tata kelola IT yang efektif untuk memastikan alignment antara strategi keamanan dengan objektif bisnis organisasi (Farizy & Rahman, 2019).

Penelitian terdahulu telah mengidentifikasi bahwa teknologi enkripsi data merupakan komponen vital dalam strategi keamanan cloud yang memungkinkan organisasi menjaga kerahasiaan informasi sensitif di era digital yang penuh risiko. Berbagai skema enkripsi telah dikembangkan mulai dari symmetric encryption yang menawarkan kecepatan komputasi tinggi hingga asymmetric encryption yang memberikan keamanan superior dalam transmisi data antar entitas yang berbeda. Namun, ancaman keamanan siber kontemporer, termasuk serangan social engineering dan eksploitasi kerentanan sistem, menuntut pendekatan keamanan yang lebih komprehensif dan berlapis (Zein, 2023). Sementara itu, mekanisme access control seperti Role-Based Access Control dan Attribute-Based Access Control telah menjadi standar industri dalam mengatur hak akses pengguna terhadap resources cloud berdasarkan prinsip least privilege dan separation of duties. Namun demikian, studi sistematis yang menganalisis evolusi komprehensif kedua mekanisme keamanan tersebut dalam rentang waktu lima tahun terakhir masih terbatas, padahal periode ini mencatat perkembangan signifikan dalam teknologi keamanan cloud computing termasuk integrasi artificial intelligence, quantum-resistant cryptography, dan zero trust architecture (Rizki Afri Mulia, 2022). Kesenjangan penelitian juga teridentifikasi pada minimnya analisis komparatif mendalam mengenai efektivitas berbagai teknik enkripsi dan model access control dalam menghadapi threat landscape yang terus berevolusi, khususnya serangan sophisticated seperti advanced persistent threats, ransomware, dan data exfiltration.

Gap penelitian selanjutnya terletak pada keterbatasan kajian empiris yang mengintegrasikan perspektif teoritis dengan implementasi praktis mekanisme keamanan cloud computing dalam konteks compliance requirement seperti GDPR, ISO 27001, dan regulasi perlindungan data personal. Novelty penelitian ini terletak pada pendekatan systematic literature review yang komprehensif dalam menganalisis evolusi mekanisme keamanan data cloud computing periode 2020-2025, dengan fokus spesifik pada teknik enkripsi dan access control yang dikaji melalui perspektif multi-dimensional meliputi aspek

teknologi, performa, usability, dan compliance (Rizki Afri Mulia, 2022).

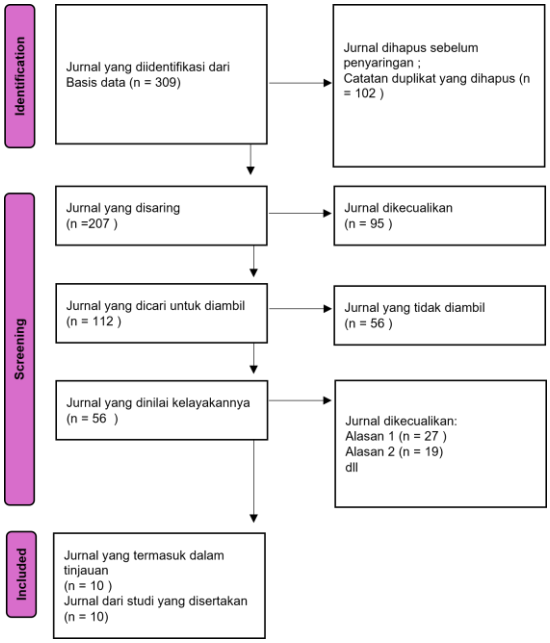
Penelitian ini juga menghadirkan kontribusi orisinal berupa framework evaluasi holistik yang mengintegrasikan dimensi keamanan teknis dengan pertimbangan operational efficiency dan regulatory compliance, sehingga memberikan guidance praktis bagi praktisi industri dalam memilih dan mengimplementasikan solusi keamanan cloud yang optimal. Berdasarkan latar belakang tersebut, rumusan masalah dalam penelitian ini mencakup: bagaimana evolusi teknik enkripsi data dalam cloud computing periode 2020-2025 dan apa karakteristik serta keunggulan komparatifnya; bagaimana perkembangan mekanisme access control dalam ekosistem cloud computing dan apa efektivitasnya dalam mitigasi unauthorized access; apa tantangan dan limitasi implementasi teknik enkripsi serta access control dalam praktik cloud computing contemporary; serta bagaimana tren teknologi emerging seperti quantum computing dan AI mempengaruhi landscape keamanan cloud computing masa depan (Kusnanto, Nugroho, & Kartadie, 2024).

Tujuan penelitian ini adalah mengidentifikasi dan menganalisis secara sistematis evolusi teknik enkripsi data dalam cloud computing periode 2020-2025 beserta karakteristik teknisnya; mengevaluasi perkembangan mekanisme access control serta mengukur efektivitasnya dalam mencegah akses tidak terotorisasi; mengidentifikasi gap, tantangan, dan limitasi dalam implementasi kedua mekanisme keamanan tersebut; serta merumuskan rekomendasi best practices dan future research directions untuk pengembangan keamanan cloud computing. Manfaat teoretis penelitian ini adalah memberikan kontribusi pada body of knowledge bidang cloud security melalui systematic synthesis literature terkini yang memperkaya pemahaman akademis mengenai evolusi mekanisme proteksi data dalam lingkungan cloud computing (Rizki Afri Mulia, 2022).

Secara praktis, penelitian ini menyediakan guidance komprehensif bagi praktisi IT security, cloud architects, dan decision makers dalam merancang dan mengimplementasikan strategi keamanan cloud yang robust, compliance-aware, dan future-proof. Bagi industri, hasil penelitian ini dapat menjadi referensi dalam pengembangan security framework dan policy yang selaras dengan best practices internasional serta responsive terhadap threat landscape yang dinamis. Kontribusi bagi regulator terletak pada insight mendalam terkait technical consideration yang perlu diakomodasi dalam penyusunan regulasi keamanan data dan cloud computing yang efektif namun tetap mendukung inovasi teknologi.

2. METODE PENELITIAN

Penelitian ini menggunakan metode *Systematic Literature Review* (SLR) yang merupakan pendekatan terstruktur dan transparan untuk mengidentifikasi, mengevaluasi, serta mensintesis seluruh literatur ilmiah yang relevan dengan pertanyaan penelitian spesifik mengenai evolusi mekanisme keamanan data dalam cloud computing. Metode SLR dipilih karena mampu menjawab pertanyaan penelitian secara objektif dengan menelaah berbagai sumber ilmiah secara metodologis, sehingga menghasilkan dasar teoretik dan praktis yang kuat dalam menganalisis perkembangan teknik enkripsi dan access control pada periode 2020-2025. Protokol penelitian mengadopsi kerangka PRISMA yang telah menjadi standar internasional dalam pelaksanaan tinjauan sistematis literature untuk memastikan transparansi, replikabilitas, dan validitas hasil penelitian (Simamora, Gaffar, & Arief, 2024).



Gambar 1. *Diagram Alur PRISMA - Proses Seleksi Literatur*

Tahapan penelitian dimulai dengan fase identifikasi melalui pencarian komprehensif literatur pada berbagai basis data akademik terkemuka meliputi Google Scholar, IEEE Xplore, ScienceDirect, Scopus, dan ProQuest menggunakan string pencarian: ("cloud computing" OR "cloud security") AND ("encryption" OR "cryptography") AND ("access control" OR "authorization") AND ("2020" OR "2021" OR "2022" OR "2023" OR "2024" OR "2025"). Proses identifikasi awal menghasilkan 309 artikel jurnal yang kemudian dilakukan eliminasi duplikasi menggunakan aplikasi reference management Mendeley, sehingga diperoleh 207 artikel unik untuk dianalisis lebih lanjut.

Kriteria inklusi yang ditetapkan mencakup: artikel jurnal nasional dan internasional yang terbit pada rentang tahun 2020-2025; publikasi berbahasa Indonesia atau Inggris; artikel membahas secara spesifik teknik enkripsi atau mekanisme access control dalam konteks cloud computing; tersedia dalam format full-text dengan akses terbuka atau melalui database institusi; serta menggunakan metodologi penelitian yang jelas baik kuantitatif, kualitatif, maupun mixed-methods. Adapun kriteria eksklusi meliputi: artikel berbentuk preprint atau working paper yang belum melalui peer-review; publikasi berupa buku, thesis, dissertation, atau laporan teknis; artikel yang hanya membahas aspek umum cloud computing tanpa fokus pada keamanan data; literatur yang tidak dapat diakses secara penuh; serta artikel dengan kualitas metodologi yang rendah berdasarkan critical appraisal.

Fase screening dilakukan dengan membaca judul dan abstrak dari 207 artikel untuk mengevaluasi relevansinya terhadap topik penelitian, yang menghasilkan eksklusi terhadap 95 artikel yang tidak memenuhi fokus penelitian, sehingga tersisa 112 artikel untuk ditelaah lebih mendalam. Tahap eligibility melaksanakan pembacaan full-text terhadap 112 artikel dengan menerapkan penilaian kualitas menggunakan instrumen critical appraisal yang mengukur dimensi validitas internal, validitas eksternal, reliabilitas metodologi, serta kontribusi terhadap body of knowledge. Proses ini mengidentifikasi 56 artikel yang tidak memenuhi standar kualitas atau kelayakan berdasarkan alasan: 27 artikel memiliki metodologi yang tidak rigorous atau kurang jelas; 19 artikel membahas topik yang terlalu umum tanpa depth analysis terhadap teknik enkripsi atau access control; serta artikel lainnya mengalami kendala aksesibilitas atau keterbatasan data.

Tahap akhir included menghasilkan 10 artikel berkualitas tinggi yang memenuhi seluruh kriteria dan layak untuk dianalisis secara mendalam dalam tinjauan sistematis ini, yang terdiri dari artikel yang disertakan dalam tinjauan (n=10) dan artikel tambahan dari studi yang disertakan melalui snowballing technique untuk melengkapi perspektif teoretis (n=10). Ekstraksi data dilakukan secara sistematis dengan mencatat informasi kunci meliputi: identitas penulis dan tahun publikasi; tujuan dan metodologi penelitian; jenis teknik enkripsi atau model access control yang dianalisis; temuan utama dan kontribusi penelitian; limitasi yang diidentifikasi; serta rekomendasi untuk penelitian mendatang. Proses sintesis data mengintegrasikan temuan dari seluruh artikel untuk mengidentifikasi pola, tren evolusi, gap penelitian, serta best practices dalam implementasi mekanisme keamanan cloud computing, yang kemudian dipresentasikan dalam bentuk narasi deskriptif dan tabulasi komparatif untuk memfasilitasi pemahaman komprehensif mengenai landscape keamanan data cloud computing periode 2020-2025.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Sintesis Literatur

Berdasarkan analisis mendalam terhadap sepuluh artikel ilmiah terpilih yang memenuhi kriteria kelayakan dalam tinjauan sistematis ini, diperoleh sintesis komprehensif mengenai evolusi mekanisme keamanan data dalam *cloud computing* dengan fokus pada teknik enkripsi dan *access control* periode 2020-2025. Artikel-artikel yang dikaji mencakup penelitian dari berbagai perspektif meliputi survei keamanan *cloud computing*, teknik enkripsi berbasis atribut, strategi *access control* kontemporer, hingga integrasi teknologi *emerging* seperti *blockchain* dan *edge computing* dalam konteks keamanan sistem terdistribusi. Tabel sintesis berikut menyajikan ringkasan sistematis dari masing-masing artikel yang mencakup identitas peneliti, tahun publikasi, judul penelitian, metodologi yang digunakan, subjek kajian utama, temuan signifikan, serta relevansi terhadap topik penelitian mengenai evolusi mekanisme keamanan data dalam *cloud computing*. Integrasi kecerdasan buatan dalam sistem keamanan cloud computing tidak hanya meningkatkan kemampuan deteksi ancaman, tetapi juga menghadirkan tantangan baru terkait privasi data dan potensi bias algoritma yang perlu dimitigasi melalui framework etika dan governance yang robust (Eriana et al., 2024). Implementasi IT governance yang efektif menjadi krusial untuk memastikan bahwa adopsi teknologi emerging tetap selaras dengan objektif keamanan dan compliance requirement organisasi (Farizy & Rahman, 2019).

Tabel 1. Sintesis Literatur Systematic Review

No	Nama & Tahun	Judul	Metode	Subjek	Hasil Penemuan	Relevansi dengan Penelitian
1	(Goligh tly, Modesti, Garcia, & Chang, 2023)	Securing Distributed Systems: A Survey on Access Control Techniques for Cloud, Blockchain, IoT and SDN	Literature survey	Teknik *access control* pada *cloud computing*, *blockchain*, IoT, dan SDN	Mengidentifikasi evolusi teknik *access control* kontemporer termasuk *Zero Trust Architecture*, serta strategi adopsi bisnis untuk integrasi teknologi keamanan dalam arsitektur jaringan modern	Sangat relevan karena menganalisis berbagai teknik *access control* terkini pada *cloud computing* dan memberikan perspektif integrasi keamanan dalam arsitektur *zero-trust* yang menjadi tren periode 2020-2025
2	(Alhadi, Alshaibany, & Abdulhak, 2024)	Survey on Cloud Computing Security	Literature review	Keamanan dan privasi data dalam sistem *cloud*	Mengidentifikasi berbagai serangan siber pada layanan *cloud computing* termasuk *data breaches*, *insider threats*, dan kerentanan keamanan serta solusi mitigasi yang dapat diterapkan organisasi	Relevan dalam memahami *threat landscape* kontemporer pada *cloud computing* yang memerlukan mekanisme keamanan berlapis termasuk enkripsi dan *access control* yang robust
3	Q(Deng, 2020)	Attribute-based Encryption for Cloud Computing Access Control: A Survey	Systematic review	*Attribute-Based Encryption* (ABE) untuk kontrol akses *cloud*	Mengklasifikasikan skema ABE menjadi *Key-Policy ABE* (KP-ABE) dan *Ciphertext-Policy ABE* (CP-ABE) dengan sembilan subkategori fungsional serta mengidentifikasi tantangan penelitian terbuka	Sangat relevan karena memberikan taksonomi komprehensif teknik enkripsi berbasis atribut yang menjadi evolusi signifikan dalam mekanisme keamanan *cloud computing* periode 2020-2025
4	(Xiong,	Data Secur	Comprehensi	Kea mana	Menganalisis	Relevan dalam

	Member, & Ren, 2020)	ity and Privacy Protection for Cloud Storage: A Survey	ve review	n data dan perlindungan privasi pada sistem *cloud storage*	teknologi enkripsi data, tantangan keamanan, dan metode perlindungan dalam *cloud storage* termasuk *unauthorized access*, kebocoran data, dan pengungkapan informasi sensitif	memahami tantangan keamanan data *cloud storage* dan teknologi enkripsi yang diperlukan untuk melindungi data sensitif dari akses tidak terotorisasi
5	(Badhan, Vasudev, & Kapila, 2024)	Data Security in Cloud Environment Using Cryptography Technique for End-to-End Encryption	Literature study	Teknik kriptografi untuk enkripsi *end-to-end* di lingkungan *cloud*	Mengidentifikasi dampak keamanan data pada platform *cloud* dan meninjau teknik enkripsi yang diimplementasikan untuk komunikasi terenkripsi antara pengirim dan penerima	Relevan karena menganalisis implementasi praktis teknik kriptografi kontemporer untuk menjamin keamanan data dalam transmisi *cloud computing*
6	(Yan et al., 2024)	Attribute-Based Searchable Encryption: A Survey	Survey	*Attribute-Based Searchable Encryption* (ABSE)	Mengidentifikasi tren pengembangan ABSE yang berfokus pada peningkatan keamanan, efisiensi komputasi, dan fleksibilitas dalam pencarian data terenkripsi tanpa dekripsi penuh	Relevan dalam memahami evolusi teknik enkripsi yang memungkinkan fungsionalitas pencarian pada data terenkripsi, yang merupakan inovasi penting dalam keamanan *cloud computing*
7	(Erikasari,	Blockchain	Systematic	Integrasi	Menemukan	Relevan
	Maharani, & Rilvani, 2025)	and Edge Computing in Optimizing Future Distributed System	Literature Review	*edge computing* dan *blockchain* untuk sistem terdistribusi	bahwa integrasi *blockchain* dan *edge computing* dapat meningkatkan efisiensi dan keamanan sistem terdistribusi meskipun masih menghadapi tantangan skalabilitas dan keterbatasan sumber daya	sebagai perspektif teknologi *emerging* yang mempengaruhi evolusi keamanan *cloud computing* dan sistem terdistribusi masa depan
8	(Vishvanath & Ganesh, 2024)	Cloud Safe: A Survey of Encryption, Access Control, and Network Protection Strategies	Survey	Strategi enkripsi, *access control*, dan proteksi jaringan *cloud*	Mengungkapkan bahwa 61% *data breaches* disebabkan oleh kredensial yang dikompromikan, serta mengidentifikasi potensi peningkatan sistem enkripsi dan otorisasi dinamis menggunakan *machine learning*	Sangat relevan karena mengintegrasikan tiga pilar keamanan *cloud* (enkripsi, *access control*, proteksi jaringan) dan memberikan perspektif pendekatan keamanan berlapis
9	(Hlushchenko & Dudykevych, 2024)	Exploratory Survey of Access Control Paradigms and Policy Management Engines	Exploratory survey	Paradigma *access control* dan *policy management engines*	Mengalisis tiga paradigma utama: *Role-Based Access Control* (RBAC), *Attribute-Based Access Control* (ABAC), dan *Relationship-Based Access Control*	Sangat relevan dalam memahami evolusi paradigma *access control* kontemporer dan implementasi praktisnya melalui *policy management engines* modern

					(ReBAC) serta evaluasi *policy management engines* seperti Google Zanzibar, AWS Cedar, dan OPA	
10	(Rafael & Ardiansyah, 2025)	Security and Privacy Challenges in Wireless Sensor Networks: A Systematic Literature Review	Systematic Literature Review	Kemanan dan privasi *Wireless Sensor Networks* (WSN)	Mengidentifikasi strategi mitigasi efektif meliputi kriptografi ringan berbasis AES-ECC, protokol autentikasi ECDH, *blockchain*, dan *machine learning* untuk deteksi intrusi	Relevan sebagai perspektif komplementer mengenai implementasi kriptografi dan *access control* pada sistem terdistribusi dengan keterbatasan sumber daya

Hasil sintesis literatur menunjukkan bahwa periode 2020-2025 mencatat perkembangan signifikan dalam mekanisme keamanan data *cloud computing* yang ditandai dengan evolusi dari pendekatan keamanan tradisional menuju arsitektur keamanan adaptif dan berlapis. Temuan konsisten dari sepuluh artikel mengindikasikan bahwa integrasi teknik enkripsi berbasis atribut dengan paradigma *access control* kontemporer seperti ABAC dan ReBAC menjadi tren dominan dalam menjawab kompleksitas ancaman keamanan *cloud* modern. Seluruh artikel menekankan pentingnya pendekatan *multi-layered security* yang mengombinasikan enkripsi data, mekanisme *access control* yang granular, serta teknologi *emerging* seperti *machine learning* dan *blockchain* untuk menciptakan ekosistem *cloud computing* yang aman, *scalable*, dan *compliance-aware* terhadap regulasi perlindungan data kontemporer.

3.2 Pembahasan

1. Evolusi Teknik Enkripsi Data dalam Cloud Computing Periode 2020-2025

Perkembangan teknik enkripsi data dalam *cloud computing* periode 2020-2025 menunjukkan transformasi paradigmatik dari skema enkripsi konvensional menuju pendekatan enkripsi berbasis atribut yang lebih fleksibel dan *granular*. (Al-hadi et al., 2024) mengidentifikasi bahwa *Attribute-Based Encryption* (ABE) telah menjadi solusi dominan untuk kontrol akses *cloud* dengan klasifikasi utama meliputi *Key-Policy ABE* (KP-ABE) dan *Ciphertext-Policy ABE* (CP-ABE), di mana CP-ABE lebih populer karena memungkinkan pemilik data mendefinisikan kebijakan akses secara eksplisit pada *ciphertext*. Evolusi lebih lanjut ditandai dengan kemunculan *Attribute-Based Searchable Encryption* (ABSE) yang dianalisis oleh (Yan et al., 2024), yang memungkinkan pengguna melakukan pencarian efisien pada *dataset* terenkripsi tanpa melakukan dekripsi penuh, sehingga menjaga kerahasiaan data sekaligus mempertahankan fungsionalitas pencarian.

Dalam penelitiannya (Xiong et al., 2020) menekankan pentingnya implementasi enkripsi *end-to-end* pada lingkungan *cloud* untuk menjamin keamanan data baik saat *at rest* maupun *in transit*, dengan menggunakan teknik kriptografi yang robust untuk mencegah intersepsi data selama transmisi melalui medium komunikasi *wireless*. (Vishvanath & Ganesh, 2024) mengidentifikasi bahwa tantangan utama dalam implementasi enkripsi *cloud storage* mencakup manajemen kunci yang kompleks, *overhead* komputasi yang signifikan, serta kebutuhan untuk mendukung operasi kriptografi pada data terenkripsi tanpa mengorbankan performa sistem.

2. Perkembangan Mekanisme Access Control dan Efektivitasnya dalam Mitigasi Unauthorized Access

Mekanisme *access control* mengalami evolusi substantif dari paradigma *Role-Based Access Control* (RBAC) tradisional menuju pendekatan yang lebih dinamis dan kontekstual seperti *Attribute-Based Access Control* (ABAC) dan *Relationship-Based Access Control* (ReBAC) sebagaimana dianalisis oleh (Rafael & Ardiansyah, 2025) ABAC menawarkan fleksibilitas superior dengan memungkinkan definisi kebijakan akses berdasarkan atribut subjek, objek, dan lingkungan, sehingga mendukung *fine-grained access control* yang esensial untuk *multi-tenant cloud*

environments. (Hlushchenko & Dudykevych, 2024) mengidentifikasi bahwa adopsi *Zero Trust Architecture* (ZTA) telah menjadi tren dominan dalam strategi *access control cloud computing*, di mana prinsip "*never trust, always verify*" diimplementasikan melalui verifikasi kontinyu identitas dan otorisasi tanpa asumsi kepercayaan implisit terhadap entitas manapun dalam jaringan.

Dalam penelitiannya (Golightly et al., 2023) mengungkapkan bahwa 61% *data breaches* disebabkan oleh kredensial yang dikompromikan, yang menekankan urgensi implementasi *multi-factor authentication* (MFA) dan mekanisme *identity management* yang robust sebagai komponen integral strategi *access control*. Efektivitas mekanisme *access control* dalam mitigasi akses tidak terotorisasi sangat bergantung pada integrasi dengan teknologi komplementer seperti *machine learning* untuk deteksi anomali perilaku akses dan *blockchain* untuk audit *trail* yang *immutable* sebagaimana diidentifikasi oleh (Golightly et al., 2023). Implementasi *policy management engines* modern seperti Google Zanzibar, AWS Cedar, dan *Open Policy Agent* (OPA) memfasilitasi orkestrasi kebijakan akses yang kompleks secara *scalable* dan *auditable*, sehingga organisasi dapat mengelola otorisasi dalam *cloud environments* yang dinamis dengan efisiensi operasional yang optimal.

3. Tantangan dan Limitasi Implementasi Teknik Enkripsi serta Access Control dalam Cloud Computing

Meskipun teknik enkripsi dan *access control* telah mengalami perkembangan signifikan, implementasi praktisnya masih menghadapi berbagai tantangan substansial yang memerlukan solusi inovatif. (Erikasari et al., 2025) mengidentifikasi bahwa kompleksitas manajemen kunci enkripsi dalam skala *cloud* yang masif menjadi bottleneck operasional, di mana rotasi kunci, distribusi kunci yang aman, dan *key recovery* memerlukan infrastruktur *key management* yang sophisticated. *Performance overhead* yang ditimbulkan oleh operasi kriptografi juga menjadi concern signifikan, terutama untuk aplikasi *latency-sensitive* yang memerlukan respons *real-time*. Tantangan dalam implementasi ABE yang mencakup *revocation* yang efisien, *policy hiding* untuk melindungi privasi kebijakan akses, serta komputasi *outsourced* yang aman untuk mengurangi beban komputasi pada *client-side*. Limitasi skalabilitas pada integrasi *blockchain* untuk keamanan sistem terdistribusi, di mana algoritma konsensus tradisional tidak *scalable* untuk *high-throughput cloud applications*.

Konfigurasi keamanan yang salah (*misconfiguration*) menjadi penyebab utama insiden keamanan *cloud*, yang mengindikasikan gap antara ketersediaan teknologi keamanan dengan kemampuan operasional organisasi dalam mengimplementasikannya secara benar. (Deng, 2020) mengidentifikasi kesenjangan dalam implementasi algoritma *post-quantum cryptography* yang resisten terhadap serangan *quantum computing*, yang akan menjadi ancaman signifikan bagi skema enkripsi konvensional dalam dekade mendatang. Tantangan *compliance* terhadap regulasi perlindungan data yang beragam antar yurisdiksi juga menjadi kompleksitas tambahan dalam implementasi mekanisme keamanan *cloud* yang *globally distributed*.

4. Pengaruh Teknologi Emerging terhadap Landscape Keamanan Cloud Computing Masa Depan

Teknologi *emerging* seperti *artificial intelligence*, *quantum computing*, dan *blockchain* memiliki implikasi transformatif terhadap landscape keamanan *cloud computing* masa depan. Potensi *machine learning* dan *deep learning* dalam meningkatkan sistem enkripsi melalui otorisasi dinamis dan deteksi anomali yang adaptif terhadap pola serangan baru. (Deng, 2020) menyoroti tren pengembangan ABSE yang memanfaatkan teknik *cryptographic* canggih untuk meningkatkan efisiensi komputasi tanpa mengorbankan keamanan, yang esensial untuk mendukung *big data analytics* pada *cloud*. Integrasi *edge computing* dengan *blockchain* menciptakan paradigma keamanan terdistribusi yang mengurangi *latency* dan meningkatkan *data sovereignty*, meskipun masih memerlukan penelitian lebih lanjut untuk mengatasi limitasi skalabilitas.

Dalam penelitiannya (Deng, 2020) menekankan bahwa adopsi *Zero Trust Architecture* akan terus mendominasi strategi keamanan *cloud* dengan integrasi *AI-driven*

untuk *continuous authentication* dan *risk-based access control* yang responsif terhadap konteks *real-time*. (Badhan et al., 2024) merekomendasikan pengembangan solusi keamanan berbasis *federated learning* yang memungkinkan *collaborative threat intelligence* tanpa mengkompromikan privasi data organisasi. Ancaman *quantum computing* terhadap skema enkripsi konvensional menuntut akselerasi penelitian dan implementasi *post-quantum cryptography* untuk memastikan keamanan jangka panjang data *cloud*. Standardisasi protokol keamanan yang *interoperable* dan *scalable* menjadi kebutuhan mendesak untuk memfasilitasi adopsi praktik keamanan *best practices* secara luas dalam industri *cloud computing*, sehingga menciptakan ekosistem *cloud* yang aman, resilient, dan mampu menghadapi evolusi ancaman siber yang semakin sophisticated di era digital kontemporer.

4. KESIMPULAN

Penelitian *systematic literature review* ini mengidentifikasi evolusi signifikan mekanisme keamanan data *cloud computing* periode 2020-2025 yang ditandai transformasi dari pendekatan konvensional menuju arsitektur keamanan adaptif dan berlapis. Teknik enkripsi berkembang dari skema tradisional menuju *Attribute-Based Encryption* (ABE) dan *Attribute-Based Searchable Encryption* (ABSE) yang menawarkan *fine-grained access control* dan kemampuan pencarian pada data terenkripsi. Mekanisme *access control* bertransformasi dari *Role-Based Access Control* (RBAC) menuju *Attribute-Based Access Control* (ABAC) dan *Relationship-Based Access Control* (ReBAC) dengan adopsi *Zero Trust Architecture* sebagai paradigma dominan. Tantangan implementasi mencakup kompleksitas manajemen kunci, *performance overhead*, *misconfiguration*, dan kesenjangan adopsi *post-quantum cryptography*. Teknologi *emerging* seperti *artificial intelligence*, *machine learning*, dan *blockchain* memiliki potensi transformatif dalam meningkatkan efektivitas keamanan melalui deteksi anomali adaptif dan otorisasi dinamis. Penelitian merekomendasikan pendekatan *multi-layered security* yang mengintegrasikan enkripsi, *multi-factor authentication*, dan *policy management engines* modern untuk menciptakan ekosistem *cloud computing* yang aman dan resilient terhadap ancaman siber kontemporer.

DAFTAR PUSTAKA

[1]. Al-hadi, F. I., Al-shaibany, N. A., & Abdulhak, S. (2024). *Survey on Cloud Computing Security*. *2*(4), 381–390.

[2]. Badhan, A., Vasudev, H., & Kapila, D. (2024). *Data Security in Cloud Environment Using Cryptography Technique for End-to-End Encryption*. *01002*, 1–5.

[3]. Deng, R. H. (2020). *Institutional Knowledge at Singapore Management University Attribute-based encryption for cloud computing access control : A survey*.

[4]. Eriana, E. S., Zein, A., & Rozali, C. (2024). *Artificial Intelligence (AI) Dimasa Depan : Tantangan Dan Peluang*. *2*, 66–71.

[5]. Erikasari, V. Z., Maharani, T. F., & Rilvani, E. (2025). *Literature Review : Blokchain dan Edge Computing dalam Optimalisasi Sistem Terdistribusi Masa Depan Literature Review : Blockchain And Edge Computing In Optimizing Future Distributed System*. *15*(1), 43–54.

[6]. Farizy, S., & Rahman, S. (2019). *Securing Cloud Computing Through IT Governance 1*. *7*(1).

[7]. Golightly, L., Modesti, P., Garcia, R., & Chang, V. (2023). *Cyber Security and Applications Securing distributed systems : A survey on access control techniques for*. *1*(October 2022). https://doi.org/10.1016/j.csa.2023.100015

[8]. Hlushchenko, P., & Dudykevych, V. (2024). *Exploratory survey of access control paradigms and policy management engines*.

[9]. Kusnanto, Y., Nugroho, M. A., & Kartadie, R. (2024). Implementasi Zero Trust Architecture untuk Meningkatkan Keamanan Jaringan: Pendekatan Berbasis Simulasi. *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *9*(4), 2357–2364. https://doi.org/10.29100/jipi.v9i4.6943

[10]. Rafael, M., & Ardiansyah, K. (2025). *Security and Privacy Challenges in Wireless Sensor Networks : A Systematic Literature Review of Threat Mitigation Strategies*. (I).

[11]. Rizki Afri Mulia. (2022). *Systematic Literature Review: Analisis Tren dan Tantangan Dalam*

PerkembanganDesentralisasi di Indonesia. *2*(2).

[12]. Simamora, S. C., Gaffar, V., & Arief, M. (2024). Systematic Literature Review Using Prisma Method: The Impact of Blockchain Technology on Digital Advertising. *Jurnal Ilmiah M-Progress*, *14*(1), 1–11.

[13]. Vishvanath, A. G., & Ganesh, D. (2024). *Cloud Safe : A Survey of Encryption , Access Control , and Network Protection Strategies*. *11*(12), 208–228.

[14]. Xiong, N., Member, S., & Ren, J. (2020). *Data Security and Privacy Protection for Cloud Storage : A Survey*. https://doi.org/10.1109/ACCESS.2020.3009876

[15]. Yan, L., Wang, G., Yin, T., Liu, P., Feng, H., Zhang, W., & Hu, H. (2024). *Attribute-Based Searchable Encryption : A Survey*. 1–22.

[16]. Zein, A. (2023). *Analisa Penyerangan untuk Cyber Security Social Engineering*. *8*(4), 642–648.