

Tantangan Keamanan dan Strategi Adopsi Cloud Computing dalam Mendukung Transformasi Digital

Slamet Rahayu ^{1*}, Noor Latifah ²

^{1, 2} Universitas Muria Kudus, Indonesia

* 202253065@std.umk.ac.id

Abstract

Urgensi penelitian ini terletak pada kebutuhan untuk mengatasi risiko keamanan sekaligus merumuskan strategi adopsi yang tepat agar cloud computing dapat dimanfaatkan secara optimal dalam mendukung transformasi digital yang efisien, aman, dan berkelanjutan. Penelitian ini bertujuan untuk mengidentifikasi tantangan keamanan krusial dalam lingkungan *cloud computing* serta merumuskan strategi adopsi yang efektif melalui metode *Systematic Literature Review* (SLR). Penelitian ini menggunakan *Systematic Literature Review* (SLR) dengan pendekatan deskriptif kualitatif untuk mengkaji tantangan keamanan dan strategi adopsi cloud computing. Sumber data diperoleh dari tiga basis data bereputasi, yaitu Google Scholar, IEEE Xplore, dan ScienceDirect, dengan rentang publikasi 2020–2025. Strategi pencarian menggunakan kata kunci “Cloud Computing Security”, “Digital Transformation”, “Cloud Adoption Strategy”, dan “Private Cloud”. Kriteria inklusi meliputi artikel yang membahas risiko keamanan, strategi adopsi (manajerial/teknis), dan efisiensi operasional, sedangkan eksklusi mencakup studi di luar topik, tidak membahas arsitektur cloud, atau di luar periode. Proses seleksi mengikuti pedoman PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) melalui tahap identifikasi, screening, dan eligibility hingga diperoleh 20 artikel. Data dianalisis dengan pengelompokan tematik dan disintesis secara deskriptif untuk menghasilkan rekomendasi strategis berbasis analisis SWOT.. Hasil penelitian menunjukkan bahwa tantangan keamanan utama didominasi oleh serangan *Denial of Service* (DoS) berbasis HTTP/XML dan risiko kedaulatan data akibat *vendor lock-in*. Temuan utama studi ini merekomendasikan strategi mitigasi hibrida yang menggabungkan pendekatan manajerial dan teknis. Dari sisi manajerial, perencanaan berbasis analisis SWOT terbukti efektif memetakan kesiapan internal organisasi. Dari sisi teknis, implementasi *Private Cloud* menggunakan platform mandiri seperti Nextcloud atau OwnCloud teridentifikasi sebagai solusi paling optimal untuk memberikan kontrol penuh terhadap enkripsi dan hak akses pengguna. Implementasi strategi ini terbukti mampu menggeser model biaya dari *Capex* ke *Opex* serta meningkatkan efisiensi operasional tanpa mengorbankan keamanan data sensitif.

Keywords: Cloud Computing, Transformasi Digital, Keamanan Informasi, Private Cloud, Analisis SWOT

Pendahuluan

Era globalisasi saat ini, perkembangan teknologi yang pesat dan semakin canggih menuntut suatu organisasi untuk beradaptasi terhadap transformasi digital untuk mempertahankan daya saing antar organisasi dan menjadi katalis utama perubahan dalam tatanan operasional organisasi (Barus et al., 2024). Dinamika ini menuntut setiap organisasi, baik di sektor swasta maupun pemerintahan, untuk beradaptasi melalui transformasi digital guna mempertahankan daya saing dan relevansi mereka. Transformasi digital bukan sekadar pendigitalan proses manual, melainkan perubahan mendasar dalam

cara bisnis beroperasi untuk meningkatkan efisiensi dan menciptakan peluang inovasi baru (Simamora et al., 2024). Salah satu pendorong utama dalam ekosistem transformasi ini adalah teknologi komputasi awan (*cloud computing*), yang memungkinkan akses sumber daya dan aplikasi dari mana saja melalui jaringan internet (Febrianti, 2024; Purba & Nasution, 2025).

Pada ekosistem ini, data telah berevolusi menjadi aset strategis baru yang nilainya setara dengan modal finansial, sehingga ketersediaan dan keamanan akses terhadap data tersebut menjadi krusial. *Cloud computing* didefinisikan oleh *National Institute of Standards and Technology* (NIST) sebagai model yang memungkinkan akses jaringan *ubiquitous*, nyaman, dan *on-demand* ke sekumpulan sumber daya komputasi bersama yang dapat dikonfigurasi dengan cepat (Apriliani et al., 2022). Teknologi ini menawarkan berbagai model layanan seperti *Software as a Service* (SaaS), *Platform as a Service* (PaaS), dan *Infrastructure as a Service* (IaaS) yang memberikan fleksibilitas tinggi bagi pengguna hal ini menjadi kebutuhan pokok di era kerja hibrida saat ini (Putri et al., 2022; Mehrtak et al., 2021).

Manfaat utamanya meliputi efisiensi biaya operasional karena meniadakan investasi perangkat keras fisik, skalabilitas yang mudah, serta kemampuan kolaborasi data secara *real-time* dan dapat diakses darimana saja melalui jaringan internet tanpa batasan geografis (Prasetya et al., 2024; Kurniawan et al., 2025). Namun, implementasi teknologi ini di negara berkembang seperti Indonesia menghadapi tantangan yang unik (Pakkaja et al., 2026). Selain masalah infrastruktur, sektor-sektor vital seperti pendidikan dan pemerintahan sering kali terkendala oleh keterbatasan anggaran untuk pengadaan server fisik yang mahal serta tingginya kebutuhan akan digitalisasi arsip yang aman (Putri et al., 2022; Rozi et al., 2023; Pratama & Prasetyo, 2024). Di sisi lain, adopsi *public cloud* sering kali terhambat oleh kekhawatiran mengenai keamanan dan privasi data (Istiqomah & Nasution, 2024). Keamanan informasi tetap menjadi perhatian utama, mengingat data disimpan dan diproses di lokasi eksternal yang sering kali tidak transparan bagi pengguna, menimbulkan risiko kedaulatan data dan kepatuhan terhadap regulasi.

Tantangan keamanan ini mencakup risiko serangan siber seperti *HTTP Denial of Service* atau *XML-Based Denial of Service*, pembajakan akun, hingga kebocoran data sensitif akibat celah keamanan pada penyedia layanan (Tu et al., 2023). Meskipun adopsi *cloud computing* menawarkan berbagai keuntungan, implementasinya masih menghadapi hambatan signifikan terkait keamanan dan privasi data, terutama karena data dikelola pada infrastruktur pihak ketiga. Ancaman seperti kebocoran data, serangan siber, dan keterbatasan kontrol pengguna menjadi perhatian utama, sementara kurangnya kesiapan organisasi dalam strategi migrasi dan manajemen risiko turut memperlambat adopsi *cloud* secara optimal (Zhang et al., 2022; Ali et al., 2021; Khan et al., 2022; Alshamrani, 2021).

Permasalahan mendasar yang menjadi fokus penelitian ini adalah adanya kesenjangan (*gap*) antara tuntutan kebutuhan transformasi digital yang mendesak dengan minimnya kerangka kerja adopsi yang aman dan terjangkau bagi organisasi berkembang. Banyak organisasi terjebak dalam dilema: menggunakan *public cloud* yang efisien namun rentan isu privasi, atau membangun server fisik yang aman namun membebani biaya investasi (*Capex*). Literatur yang ada saat ini cenderung membahas aspek ini secara terpisah baik fokus murni pada teknis keamanan jaringan atau fokus murni pada manajemen strategi bisnis. Masih sedikit penelitian yang mengintegrasikan kedua perspektif tersebut untuk menawarkan solusi jalan tengah yang konkret bagi organisasi dengan sumber daya

terbatas. Ketiadaan kerangka kerja adopsi yang holistik ini menyebabkan banyak organisasi ragu untuk beralih ke *cloud* sepenuhnya, atau justru nekat bermigrasi tanpa proteksi memadai yang berujung pada insiden keamanan.

Lebih jauh lagi, tantangan adopsi *cloud* tidak hanya bersumber dari aspek teknis infrastruktur, tetapi juga dari faktor sumber daya manusia (SDM) dan manajerial. Minimnya pemahaman dan literasi digital pengguna sering kali menjadi titik lemah dalam rantai keamanan sistem informasi. Kurangnya edukasi mengenai prosedur keamanan *cloud* dan manajemen kelola risiko yang jelas menyebabkan organisasi ragu untuk beralih ke *cloud* sepenuhnya, atau justru mengadopsinya tanpa proteksi yang memadai. Ketidaksiapan budaya kerja dan resistensi terhadap perubahan prosedur operasional standar sering kali membuat investasi teknologi menjadi sia – sia atau justru membuka cela kerentanan baru.

Hal ini menegaskan bahwa solusi teknologi semata tidak cukup, diperlukan pendekatan holistik yang mencakup aspek manusia dan manajerial. Penting untuk dicatat bahwa keberhasilan adopsi teknologi awan tidak hanya bergantung pada kecanggihan infrastruktur semata, tetapi juga pada keselarasan antara strategi bisnis dan mitigasi risiko teknis. Literatur menunjukkan bahwa adopsi yang dilakukan secara parsial hanya berfokus pada efisiensi tanpa memperhitungkan arsitektur keamanan yang memadai justru meningkatkan kerentanan organisasi terhadap ancaman siber yang serius. Sebaliknya, pendekatan yang terlalu protektif tanpa mempertimbangkan fleksibilitas operasional dapat menghambat inovasi dan kolaborasi yang menjadi inti dari transformasi digital itu sendiri (Apriliani et al., 2022).

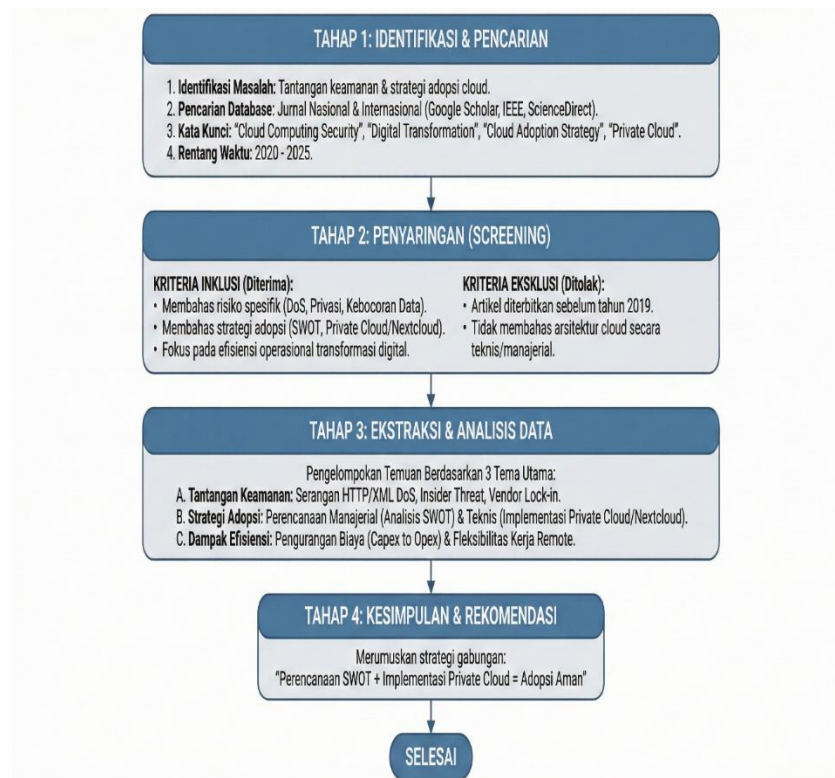
Oleh karena itu, diperlukan sebuah kajian komprehensif yang mensintesiskan berbagai perspektif, mulai dari evaluasi manajerial hingga solusi teknis praktis, guna menghasilkan kerangka kerja adopsi yang seimbang dan berkelanjutan bagi organisasi di era digital. Penelitian ini hadir untuk mengatasi permasalahan tersebut dengan menawarkan pendekatan komprehensif yang menggabungkan evaluasi manajerial dan solusi teknis praktis. Secara spesifik, penelitian ini bertujuan untuk melakukan tinjauan literatur sistematis (*Systematic Literature Review*) guna mengidentifikasi tantangan keamanan utama serta merumuskan strategi adopsi *cloud computing* yang efektif dalam mendukung keberhasilan transformasi digital.

Strategi adopsi yang efektif dimulai dari perencanaan berbasis analisis SWOT (*Strengths, Weaknesses, Opportunities, Threats*) hingga pemilihan model implementasi yang tepat (Istiqomah & Nasution, 2024). Analisis SWOT ini bertujuan untuk memetakan kesiapan internal, dengan implementasi teknis berupa *Private Cloud* mandiri berbasis platform open source seperti OwnCloud atau Nextcloud, yang memberikan kontrol penuh atas data kepada organisasi. Pendekatan hibrida ini diharapkan mampu memberikan solusi di mana organisasi dapat menikmati efisiensi dan fleksibilitas teknologi *cloud* tanpa harus mengorbankan kontrol penuh atas keamanan, privasi, dan kedaulatan data mereka, sehingga mendukung keberhasilan transformasi digital yang berkelanjutan.

Metode

Penelitian ini menerapkan metode *Systematic Literature Review* (SLR) dengan pendekatan deskriptif kualitatif untuk mengkaji secara mendalam literatur terkait tantangan keamanan dan strategi adopsi *cloud computing*. Guna menjamin standar pelaporan yang berkualitas tinggi, transparansi, serta replikabilitas studi, protokol

penelitian ini disusun mengikuti pedoman PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*). Penggunaan standar PRISMA dipilih karena menyediakan kerangka kerja sistematis yang meminimalkan bias subjektif peneliti dalam proses seleksi artikel, serta memastikan bahwa setiap tahapan mulai dari identifikasi, penyaringan (*screening*), hingga kelayakan (*eligibility*) terdokumentasi secara auditabel. Melalui pendekatan ini, data yang diperoleh tidak hanya sekadar dikumpulkan, tetapi dievaluasi dan diinterpretasikan secara kritis untuk menghasilkan sintesis strategi baru yang valid.



Gambar 1. Bagan alur penelitian menggunakan metode SLR

Strategi Pencarian dan Sumber Data Merujuk pada Tahap 1 alur penelitian, pengumpulan data dilakukan dengan menelusuri artikel ilmiah dari tiga pangkalan data utama bereputasi, yaitu Google Scholar, IEEE Xplore, dan ScienceDirect. Penelusuran dibatasi pada artikel yang diterbitkan dalam rentang waktu 2020 hingga 2025 untuk memastikan relevansi temuan dengan perkembangan teknologi terkini. Pencarian literatur menggunakan kombinasi kata kunci spesifik (*search string*) yang meliputi: "Cloud Computing Security", "Digital Transformation", "Cloud Adoption Strategy", dan "Private Cloud". Data yang telah lolos seleksi kemudian dianalisis dan disintesis menggunakan metode deskriptif kualitatif.

Analisis data dilakukan dengan seleksi studi (PRISMA Flow), proses seleksi dilakukan melalui tahap penyaringan bertingkat untuk menjamin validitas data (Tahap 2). Pada tahap identifikasi awal, ditemukan total 30 artikel. Setelah dilakukan pemeriksaan duplikasi, sebanyak 4 artikel yang sama dihapus. Tahap selanjutnya adalah penyaringan (*screening*) berdasarkan relevansi judul dan abstrak, di mana 6 artikel dieksklusi karena tidak relevan dengan topik. Sebanyak 20 artikel tersisa kemudian dianalisis secara *full-text*. Dari 20 artikel tersisa difokuskan pada artikel yang: (1) Membahas risiko keamanan spesifik seperti siber atau privasi data; (2) Menawarkan solusi strategi adopsi melalui pendekatan manajerial

(SWOT) maupun teknis (*Private Cloud*); dan (3) Berfokus pada efisiensi operasional transformasi digital. Sebaliknya, literatur yang tidak membahas arsitektur layanan *cloud* secara mendalam atau diterbitkan di luar rentang waktu yang ditentukan akan dieksklusi dari tinjauan ini. Berdasarkan kriteria tersebut, total 20 artikel final dipilih untuk ekstraksi data.

Ekstraksi dan Analisis Data Ekstraksi data dilakukan menggunakan instrumen pengelompokan tematik (Tahap 3) yang membagi temuan ke dalam tiga tema utama: 1). Tantangan Keamanan: Mencakup analisis serangan *HTTP/XML DoS*, *insider threat*, dan risiko *vendor lock-in*; 2). Strategi Adopsi: Mencakup perencanaan manajerial menggunakan analisis SWOT dan strategi teknis melalui implementasi *Private Cloud* berbasis platform seperti Nextcloud atau OwnCloud; 3). Dampak Efisiensi: Mencakup analisis pengurangan biaya (*Capex to Opex*) dan fleksibilitas kerja jarak jauh (*remote work*).

Data yang terkumpul kemudian disintesis secara deskriptif kualitatif untuk merumuskan rekomendasi strategi yang adaptif. Formulasi strategi ini disusun dengan mengadaptasi kerangka pikir strategi pencocokan (*matching strategy*) dalam analisis SWOT, yaitu mempertemukan kelemahan infrastruktur internal dengan ancaman eksternal untuk menghasilkan rekomendasi mitigasi yang komprehensif (Tahap 4). Pendekatan integratif ini memastikan bahwa solusi yang ditawarkan tidak hanya bersifat teoritis, tetapi juga aplikatif dan sesuai dengan dinamika kebutuhan organisasi modern.

Hasil

Berdasarkan tahapan seleksi dan ekstraksi data yang dilakukan mengikuti kriteria PRISMA, diperoleh 20 artikel utama yang relevan dengan kriteria inklusi. Seluruh literatur terpilih diterbitkan dalam rentang waktu 2020 hingga 2025, yang menjamin kebaruan (*novelty*) data terkait perkembangan teknologi *cloud*. Ringkasan ekstraksi data yang mencakup fokus penelitian dan temuan utama disajikan secara rinci dalam tabel 1.

Tabel 1. Fokus dan Temuan penelitian

Penulis	Fokus	Temuan Utama / Isu yang Diangkat	Temuan
Darmawan (2024)	Keamanan Nextcloud	Mengidentifikasi kerentanan serangan Denial of Service (DoS) berbasis HTTP/XML dan pentingnya manajemen file terpusat	Tantangan dan Keamanan
Musanto et al., (2025)	Analisis SWOT & Storage	Menyoroti resiko internal seperti pembajakan akun dan urgensi perencanaan strategis menggunakan analisis SWOT sebelum pengadaan storage	Keamanan dan Strategi
Muhammad Rizki Suryawijaya (2024)	Pengarsipan dan Privasi	Mengangkat isu privasi data dan kedaulatan data (<i>data sovereignty</i>) akibat ketidakjelasan lokasi fisik server pada public cloud.	Tantangan Privasi
Rachmat et al., (2021)	OwnCloud Security	Implementasi Private Cloud dengan OwnCloud memberikan kontrol penuh atas enkripsi dan keamanan data dibanding layanan publik.	Stratei Teknis
Liga et al., (2025)	Implementasi Nextcloud	Studi kasus implementasi Nextcloud (SiMAS) terbukti efektif untuk manajemen berkas yang aman di lingkungan akademik.	Strategi Teknis
Widarma et al., (2023)	Peranan Bisnis Cloud	Adopsi cloud mengubah struktur biaya dari investasi modal (Capex) menjadi biaya operasional (Opex) yang lebih efisien.	Dampak Efisiensi

Penulis	Fokus	Temuan Utama / Isu yang Diangkat	Temuan
Lisy Tantowi (2023)	Cloud Storage & Dokumen	Cloud storage mempercepat <i>information retrieval</i> (temu kembali informasi) dan mendukung inisiatif kantor nir-kertas (<i>paperless</i>).	Dampak Efisiensi
Barus (2024)	Efisiensi Akuntansi	Transformasi digital melalui cloud meningkatkan efisiensi dan akurasi dalam proses pencatatan akuntansi organisasi	Dampak Efisiensi
Liga et al (2025)	Implementasi Nextcloud	Studi kasus di FEB UNCEN menunjukkan implementasi sistem penyimpanan berkas (SiMAS) berbasis Nextcloud meningkatkan kecepatan akses data, keamanan informasi, dan kemudahan kolaborasi akademik.	Implementasi Teknis & Transformasi Digital
Barus et al. (2024)	Efisiensi Akuntansi dengan Cloud	Teknologi <i>cloud computing</i> meningkatkan efisiensi akuntansi melalui percepatan pemrosesan transaksi, peningkatan akurasi pencatatan otomatis, dan pengurangan biaya operasional infrastruktur fisik.	Efisiensi Operasional & Akuntansi
Sljabat & Widjaja (2025)	Kesadaran Keamanan Google Drive	Studi pada Dinas Komunikasi Wakatobi menunjukkan tingkat kesadaran pengguna terhadap keamanan data bervariasi. Diperlukan keseimbangan antara inovasi teknologi dan kebijakan keamanan informasi.	Keamanan & Perilaku Pengguna
Alkadrie & Fitroh (2024)	Keamanan Cloud di Industri 4.0	Integrasi <i>Blockchain</i> , <i>Artificial Intelligence</i> (AI), dan <i>Edge Computing</i> terbukti efektif meningkatkan keamanan cloud dibanding metode tradisional, terutama untuk perlindungan data IoT di sektor industri.	Keamanan Siber & Teknologi Maju
Wulan et al. (2024)	Keamanan IoT & Cloud pada E-Commerce	Ancaman siber seperti <i>malware</i> dan serangan DDoS pada sistem IoT berbasis cloud sangat mengganggu operasional e-commerce. Solusi enkripsi <i>end-to-end</i> dan kebijakan akses ketat sangat krusial.	Keamanan E-Commerce & IoT
Simamora et al. (2024)	Blockchain & Periklanan Digital	Teknologi <i>blockchain</i> mampu menghilangkan ketergantungan pada pihak ketiga dalam periklanan digital, meningkatkan transparansi, serta meminimalisir penipuan iklan (<i>ad fraud</i>).	Blockchain & Pemasaran Digital
Candra et al. (2025)	Efisiensi Cloud di Perguruan Tinggi	Pemanfaatan <i>cloud computing</i> di Institut Teknologi dan Bisnis Bina Adinata terbukti meningkatkan efisiensi pengolahan data akademik sebesar 82,7%, namun memerlukan peningkatan pelatihan pengguna.	Efisiensi Operasional & Pendidikan
Tantowi & Wijayanti (2023)	Peluang & Tantangan Cloud Storage	<i>Cloud storage</i> mendukung preservasi dokumen digital dan mitigasi bencana data. Tantangan utamanya adalah kesiapan SDM dan risiko penyalahgunaan data yang memerlukan edukasi intensif.	Manajemen Dokumen & Adopsi
Ang'udi (2023)	Analisis Komprehensif Keamanan Cloud	Identifikasi tantangan keamanan mendalam (kebocoran data, kepatuhan regulasi). Rekomendasi solusi meliputi model keamanan <i>Zero Trust</i> , autentikasi multi-faktor (MFA), dan deteksi ancaman berbasis AI.	Analisis Keamanan & Strategi
Duha et al. (2022)	Analisa Layanan Cloud Era Digital	Tinjauan karakteristik (<i>on-demand</i> , <i>elasticity</i>) dan model layanan (<i>SaaS</i> , <i>PaaS</i> , <i>IaaS</i>) menegaskan bahwa cloud memungkinkan fleksibilitas akses sumber daya tanpa batasan geografis.	Tinjauan Konseptual & Layanan
Musantono et al. (2025)	Strategi Pengadaan Cloud Storage (SWOT)	Analisis SWOT pada PT Lokabyte merekomendasikan tiga opsi strategi: penggunaan <i>Public Cloud</i> (Google Drive), <i>Private Cloud</i> (NAS), atau <i>Hybrid</i> untuk mendukung transformasi digital perusahaan rintisan.	Strategi Bisnis & Transformasi Digital
Ilahi et al., (2024)	Potensi vs Tantangan Cloud Computing	Potensi efisiensi operasional dan skalabilitas cloud sangat besar, namun berhadapan dengan tantangan biaya implementasi dan ketersediaan layanan yang harus diatasi dengan pemilihan model layanan yang tepat.	Potensi & Tantangan Implementasi

Hasil analisis literatur memperlihatkan pola ancaman yang kompleks, bergerak dari serangan teknis eksternal hingga kerentanan internal. Secara teknis, penelitian terdahulu mengidentifikasi bahwa infrastruktur *cloud* dan IoT masih sangat rentan terhadap serangan *Denial of Service* (DoS) berbasis HTTP/XML dan penyusupan *malware* yang menargetkan ketersediaan layanan (Darmawan, 2024; Wulan et al., 2024). Namun, kerentanan sistem tidak hanya bersumber dari serangan luar. Temuan Agus Eko penelitian lainnya menegaskan bahwa faktor internal seperti pembajakan akun akibat lemahnya manajemen identitas dan rendahnya kesadaran keamanan (*security awareness*) pengguna di instansi pemerintahan justru menjadi celah keamanan yang krusial (Musantono, 2025).

Penelitian lain menyoroti isu legalitas, di mana ketidakjelasan lokasi fisik server pada layanan *public cloud* memicu masalah kedaulatan data (*data sovereignty*) yang berbenturan dengan regulasi privasi lokal (Suryawijaya, 2024). Untuk mengatasi ragam tantangan di atas, literatur yang dikaji merumuskan strategi mitigasi yang terbagi ke dalam lapisan manajerial dan teknis, di luar aspek teknis dan perilaku. Pada lapisan manajerial, penelitian terdahulu menemukan bahwa penggunaan analisis SWOT menjadi langkah awal yang vital bagi perusahaan rintisan untuk memetakan kebutuhan sebelum memilih model layanan (*Public, Private, atau Hybrid*) (Musantono et al., 2025). Melengkapi perencanaan tersebut, solusi teknis yang paling dominan ditemukan adalah implementasi *Private Cloud*. Studi terdahulu membuktikan bahwa penggunaan platform mandiri seperti OwnCloud atau Nextcloud memberikan organisasi kendali mutlak atas kunci enkripsi, yang tidak dimiliki pada layanan publik (Rachmat, 2021; Liga et al., 2025).

Lebih lanjut, tren keamanan mutakhir mulai mengadopsi pendekatan arsitektur *Zero Trust* dan autentikasi multi-faktor (MFA) sebagaimana disarankan oleh penelitian sebelumnya serta integrasi teknologi *Blockchain* untuk transparansi data di sektor industri 4.0 menurut temuan (Ang'udi, 2023; Alkadrie & Fitroh, 2024). Penerapan strategi yang tepat terbukti berkorelasi langsung dengan peningkatan efisiensi organisasi di berbagai sektor. Dampak finansial yang paling mendasar yaitu terjadinya pergeseran struktur pembiayaan dari belanja modal infrastruktur fisik (*Capex*) menjadi biaya operasional layanan (*Opex*) yang lebih fleksibel. Efisiensi biaya ini diikuti oleh lonjakan produktivitas operasional. Penelitian terdahulu melaporkan data kuantitatif berupa peningkatan efisiensi pengolahan data akademik sebesar 82,7% di perguruan tinggi pasca-adopsi *cloud* (Candra et al., 2025). Dalam konteks administrasi, penelitian terdahulu menemukan bahwa teknologi ini mempercepat proses temu kembali informasi (*information retrieval*) dan meningkatkan akurasi pencatatan akuntansi, sekaligus mendukung terwujudnya ekosistem kantor nir-kertas (*paperless office*) yang ramah lingkungan (Tantowi, 2023; Barus, 2024).

Pembahasan

Temuan-temuan dalam penelitian ini mengindikasikan sebuah fenomena krusial: meskipun *cloud computing* bertindak sebagai pendorong utama transformasi digital, aspek keamanan tetap menjadi paradoks yang harus diselesaikan. Berdasarkan hasil ekstraksi data literatur, risiko serangan siber seperti *HTTP Denial of Service* (DoS) dan isu privasi data masih menjadi ancaman dominan yang paling sering dilaporkan. Secara teoritis, hal ini sejalan dengan konsep "paradoks keamanan siber" (*cybersecurity paradox*), di mana semakin tinggi tingkat konektivitas dan kemudahan akses data yang dibuka oleh organisasi

untuk efisiensi, semakin lebar pula permukaan serangan (*attack surface*) yang terekspos terhadap ancaman eksternal.

Teori manajemen risiko modern menegaskan bahwa mekanisme pertahanan perimeter tradisional seperti *firewall* tidak lagi cukup untuk membendung serangan lapisan aplikasi yang *kompleks* ini. Oleh karena itu, dalam tataran praktik, organisasi dituntut untuk tidak sekadar menjadi pengguna pasif. Implikasi praktis dari temuan ini mengharuskan organisasi untuk memahami *Service Level Agreement* (SLA) dan arsitektur keamanan secara mendalam sebelum melakukan migrasi. SLA tidak boleh hanya dipandang sebagai dokumen administratif, melainkan sebagai instrumen mitigasi risiko legal yang wajib. Organisasi harus memastikan bahwa SLA mencakup jaminan ketersediaan layanan (*availability*), mekanisme pemulihan bencana (*disaster recovery*), serta klausul penalti yang jelas jika terjadi kebocoran data.

Implikasi praktis dari pergeseran lanskap ancaman ini menuntut organisasi untuk tidak lagi bersikap pasif sebagai konsumen teknologi. Organisasi wajib mengadopsi postur pertahanan berlapis (*Defense-in-Depth*). Namun, solusi teknis saja tidak cukup. Temuan penelitian menegaskan bahwa pemahaman mendalam mengenai *Service Level Agreement* (SLA) adalah instrumen mitigasi risiko yang paling fundamental namun sering diabaikan. Dalam tataran praktik, organisasi harus melakukan audit ketat terhadap dokumen SLA sebelum menyepakati kontrak. SLA tidak boleh hanya dipandang sebagai dokumen administratif, melainkan sebagai kontrak legal yang mengikat. Organisasi harus menuntut klausul yang spesifik mengenai *Recovery Point Objective* (RPO) dan *Recovery Time Objective* (RTO) untuk menjamin kelangsungan bisnis saat bencana terjadi, serta memastikan adanya transparansi penuh dan penalti finansial yang tegas jika penyedia layanan gagal melindungi kerahasiaan data.

Selain aspek teknis, hasil tinjauan literatur menyoroti dua elemen vital yang sering terabaikan: faktor manusia dan kepatuhan hukum (*compliance*). Temuan menunjukkan bahwa "minimnya pemahaman" pengguna sering kali menjadi celah keamanan terbesar, melebihi kerentanan sistem itu sendiri. Fenomena ini mengonfirmasi teori keamanan informasi klasik mengenai "Mata Rantai Terlemah" (*The Weakest Link*), yang menyatakan bahwa keamanan sebuah sistem hanyalah sekuat pengguna yang mengoperasikannya. Ancaman seperti *phishing* atau pengelolaan kata sandi yang lemah adalah masalah perilaku (*behavioral issue*), bukan sekadar masalah teknologi (Khan et al., 2024). Di sisi lain, dari perspektif hukum, ketidaktahuan mengenai lokasi fisik penyimpanan data pada *public cloud* menimbulkan risiko pelanggaran kedaulatan data, mengingat data adalah aset yang terikat pada yurisdiksi hukum tempat data tersebut berada. Implikasi praktis dari analisis ini menuntut pendekatan holistik dalam strategi adopsi.

Solusi teknologi harus disertai dengan investasi pada sumber daya manusia melalui program pelatihan dan edukasi yang berkelanjutan. Tujuannya adalah membangun budaya "sadar keamanan" (*security awareness*), memastikan pengguna memahami prosedur berbagi data yang aman. Secara manajerial, organisasi wajib melakukan audit kepatuhan regulasi sebelum memilih vendor, memastikan lokasi server mematuhi undang-undang perlindungan data pribadi yang berlaku (Candra et al., 2025). Sebagai respons strategis untuk memitigasi dilema ini, temuan penelitian memperlihatkan preferensi kuat terhadap implementasi *Private Cloud* menggunakan platform mandiri seperti Nextcloud atau OwnCloud. Temuan ini merespons risiko "vendor lock-in" dan hilangnya kendali data yang sering terjadi pada layanan *public cloud* (Fauzi dkk., t.t.). Dalam teori strategi sistem

informasi, konsep Kedaulatan Data (*Data Sovereignty*) menekankan bahwa kepemilikan penuh atas kunci enkripsi dan kontrol fisik terhadap data adalah syarat mutlak untuk menjamin keamanan aset strategis (Alkadrie et al., 2024).

Meskipun *Public Cloud* unggul dalam efisiensi biaya (*economies of scale*), model ini memiliki kelemahan inheren dalam transparansi kontrol yang berisiko bagi data sensitif. Sebagai solusi jalan tengah atau praktik terbaik (*best practice*), penelitian merekomendasikan implementasi *Private Cloud* menggunakan platform mandiri dan terbuka seperti Nextcloud atau OwnCloud. Solusi ini memberikan jaminan mutlak bahwa organisasi memegang kendali penuh atas kunci enkripsi dan siklus hidup data. Namun, menyadari bahwa *Private Cloud* membutuhkan investasi awal yang lebih tinggi, praktik terbaik (*best practice*) yang disarankan adalah model *Hybrid Cloud*. Strategi ini menawarkan keseimbangan optimal: data yang bersifat sangat rahasia (*confidential*) dan terikat regulasi ketat disimpan di infrastruktur *private on-premise*, sementara data umum yang membutuhkan kolaborasi masif dan skalabilitas tinggi ditempatkan di *public cloud*.

Implementasi strategi ini harus didahului dengan klasifikasi data yang ketat dan analisis SWOT (*Strengths, Weaknesses, Opportunities, Threats*) untuk menyelaraskan kapabilitas infrastruktur internal dengan kebutuhan bisnis. Pada aspek dampak ekonomi, literatur secara konsisten menunjukkan bahwa adopsi *cloud* yang terencana mampu mengubah model bisnis secara fundamental, terutama melalui pergeseran dari belanja modal (*Capex*) ke belanja operasional (*Opex*). Temuan ini mendukung teori ekonomi digital tentang Agilitas Bisnis (*Business Agility*). Teori ini menyatakan bahwa kemampuan organisasi untuk mengubah biaya tetap (infrastruktur fisik) menjadi biaya variabel (layanan *cloud*) akan meningkatkan likuiditas dan kemampuan adaptasi organisasi terhadap perubahan pasar yang cepat.

Secara praktis, transformasi digital melalui *cloud computing* bukan lagi sekadar pilihan opsional, melainkan kebutuhan strategis untuk keberlanjutan organisasi (*business continuity*) (Zaki et al., 2023). Organisasi disarankan untuk melakukan migrasi bertahap menuju ekosistem kantor nir-kertas (*paperless office*) yang didukung kolaborasi *real-time*. Dengan kombinasi pemilihan arsitektur yang tepat dan perencanaan manajerial yang matang, organisasi dapat memanfaatkan potensi penuh komputasi awan untuk meningkatkan keunggulan kompetitif tanpa harus mengorbankan keamanan aset informasi mereka. Pemilihan model layanan *cloud* merupakan keputusan strategis yang paling krusial. Literatur menunjukkan bahwa *Public Cloud* memang unggul dalam hal efisiensi biaya karena model *pay-as-you-go* dan tidak adanya investasi infrastruktur awal. Namun, untuk organisasi yang menangani data sensitif seperti data kependudukan atau rahasia dagang, *Private Cloud* dengan platform mandiri seperti Nextcloud atau OwnCloud adalah solusi yang tak bisa ditawar.

Solusi ini memberikan jaminan kedaulatan data di mana organisasi memegang kendali penuh atas kunci enkripsi dan lokasi fisik data, memitigasi risiko "vendor lock-in" dan ketidakpastian yurisdiksi hukum yang sering terjadi pada penyedia *cloud* global. Alternatif lain yang muncul sebagai jalan tengah adalah strategi *Hybrid Cloud*, yang memungkinkan organisasi menyimpan data kritis di *private server* dan data umum di *public cloud*, sehingga tercapai keseimbangan antara keamanan ketat dan skalabilitas tinggi. Secara keseluruhan, transformasi digital melalui *cloud computing* bukan lagi sekadar pilihan, melainkan kebutuhan strategis untuk keberlanjutan organisasi.

Efisiensi yang ditawarkan dalam bentuk skalabilitas dan pengurangan biaya operasional memberikan keunggulan kompetitif yang signifikan di era digital (SImamora et al., 2024). Meskipun tantangan keamanan bersifat nyata, pembahasan ini menyimpulkan bahwa risiko tersebut dapat dikelola melalui kombinasi pemilihan arsitektur yang tepat (seperti *Private Cloud*) dan perencanaan strategis yang matang. Dengan demikian, organisasi dapat memanfaatkan potensi penuh dari komputasi awan untuk meningkatkan kinerja operasional tanpa mengorbankan keamanan aset informasi mereka.

Kesimpulan

Penelitian ini menyimpulkan bahwa *cloud computing* memegang peranan vital dalam akselerasi transformasi digital organisasi, terutama terkait efisiensi biaya (*Capex to Opex*) dan fleksibilitas akses, namun tetap dihadapkan pada paradoks keamanan serius seperti ancaman *Denial of Service* (DoS), kerentanan perilaku pengguna, serta risiko legalitas kedaulatan data. Sebagai kontribusi utama, penelitian ini merumuskan bahwa strategi adopsi yang efektif tidak boleh dilakukan secara impulsif, melainkan memerlukan pendekatan hibrida yang mengintegrasikan aspek manajerial dan teknis. Kombinasi antara perencanaan strategis berbasis analisis SWOT, pemahaman mendalam terhadap *Service Level Agreement* (SLA), dan implementasi arsitektur *Private Cloud* mandiri (seperti *Nextcloud* atau *OwnCloud*) terbukti menjadi solusi paling optimal untuk menyeimbangkan kebutuhan efisiensi operasional dengan kontrol keamanan data yang ketat.

Kendati demikian, penelitian ini memiliki keterbatasan karena hanya berbasis pada metode *Systematic Literature Review* (SLR) terhadap artikel dari Google Scholar, IEEE Xplore, dan ScienceDirect dalam rentang waktu 2020–2025, tanpa melakukan pengujian empiris langsung pada objek spesifik. Berdasarkan keterbatasan tersebut, penelitian selanjutnya disarankan untuk memperluas cakupan melalui studi eksperimental atau analisis kuantitatif di dunia nyata. Topik krusial untuk dikaji lebih lanjut meliputi analisis biaya-manfaat (*Cost-Benefit Analysis*) pada implementasi *Private Cloud*, pengembangan model integrasi *Blockchain* untuk transparansi audit SLA, serta studi longitudinal mengenai efektivitas program edukasi keamanan siber dalam memitigasi risiko *human error* di lingkungan organisasi.

Acknowledgment

Daftar Pustaka

- Ali, O., Shrestha, A., Soar, J., & Wamba, S. F. (2021). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. *International Journal of Information Management*, 60, 102363. <https://doi.org/10.1016/j.ijinfomgt.2021.102363>
- Alkadrie, S. A., & Fitroh. (2024). Keamanan cloud computing di era Industri 4.0: Systematic literature review. *KONSTELASI: Konvergensi Teknologi dan Sistem Informasi*, 4(2). <https://doi.org/10.24002/konstelasi.v4i2.10277>
- Alshamrani, A. (2021). Cloud computing adoption: A review of challenges and solutions. *Computers*, 10(10), 123. <https://doi.org/10.3390/computers10100123>

- Ang'udi, J. J. (2023). Security challenges in cloud computing: A comprehensive analysis. *World Journal of Advanced Engineering Technology and Sciences*, 10(2), 155–181. <https://doi.org/10.30574/wjaets.2023.10.2.0304>
- Apriliani, N., Pratama, A. R. I., & Irawan, A. S. Y. (2022). Perbandingan antara teknologi dan performa pada komputasi awan (cloud computing). *Infotek: Jurnal Informatika dan Teknologi*, 5(2), 219–229. <https://doi.org/10.29408/jit.v5i2.5672>
- Barus, E., Pardede, K. M., & Manjorang, J. A. P. B. (2024). Transformasi digital: teknologi cloud computing dalam efisiensi akuntansi. *Jurnal Sains Dan Teknologi*, 5(3), 904–911. <https://doi.org/10.55338/saintek.v5i1.2862>
- Candra, A., Maghfira, M., & Anisa, A. (2025). Pemanfaatan Teknologi Cloud Computing Untuk Efisiensi Proses Pengolahan Data Informasi Di Institut Teknologi Dan Bisnis Bina Adinata Bulukumba. *RIGGS: Journal of Artificial Intelligence and Digital Business*, 4(2), 4172–4177. <https://doi.org/10.31004/riggs.v4i2.1192>
- Darmawan, D. (2024). Nextcloud: Keamanan Data Terbaik Dengan Manajemen File Dan Pengguna Yang Cerdas.
- Duha, T., Setiawan, W., & Fajriyah, N. (2022). Analisis layanan cloud computing di era digital. *Jurnal Informatika*, 1(1), 32–39. <https://doi.org/10.57094/ji.v1i1.355>
- Febrianti, S. (2024). Sustainability finance dan green investment: Literature review dengan metode PRISMA. *Manajemen: Jurnal Ekonomi*, 6(1), 95–106. <https://doi.org/10.36985/pmyj1709>
- Ilahi, E. N., Saripudin, M., Nughraha, M. A., Cardinsyah, G. D. A., Hikmatulloh, M. F., & Encep, M. (2024). Mengungkap potensi luar biasa dan tantangan menantang cloud computing di era digital. *Karimah Tauhid*, 3(2), 2197–2206. <https://doi.org/10.30997/karimahtauhid.v3i2.12300>
- Istiqomah, I., & Nasution, M. I. P. (2024). Implementasi sistem informasi manajemen berbasis cloud computing untuk meningkatkan daya saing organisasi. *Jurnal Ilmiah Ekonomi dan Manajemen*, 3(1). <https://doi.org/10.61722/jiem.v3i1.3396>
- Khan, N., Al-Yasiri, A., & Al-Mashhadi, S. (2022). Cloud computing security challenges and future directions: A systematic review. *Computers & Security*, 113, 102537. <https://doi.org/10.1016/j.cose.2021.102537>
- Kurniawan, S., Ruseno, N., & Irfansyah, D. (2025). Analisis tren teknologi cloud computing dalam e-business dan e-commerce untuk optimalisasi operasional. *Jurnal PASTI*, 1(1), 23–29. <https://doi.org/10.9001/jurnalpasti.v1i1.917>
- Liga, M., Oktaviani, T. W., Khaliq, I., Jayanti, N. T., Sakinah, N., Sampe, A., & Revassy, R. N. (2025). Transformasi digital: Implementasi sistem penyimpanan berkas (SiMAS) melalui platform Nextcloud (studi kasus: Fakultas Ekonomi dan Bisnis Universitas Cenderawasih). *Prosiding Seminar Nasional Teknik Elektro (SEMNASTEK)*, 2, 9–13.
- Mehrtak, M., Seyedalinaghi, S., Mohssenipour, M., Noori, T., Karimi, A., Shamsabadi, A., Heydari, M., Barzegary, A., Mirzapour, P., Soleymanzadeh, M., Vahedi, F., Mehraeen, E., & Dadras, O. (2021). Security challenges and solutions using healthcare cloud computing. *Journal of Medicine and Life*, 14(4), 448–461. <https://doi.org/10.25122/jml-2021-0100>

- Pakkaja, R. A., Wafda, A., & Ishak, M. (2026). Transformasi Administrasi Surat: Perancangan Konseptual Sistem Berbasis Odoo ERP pada Armbian Linux untuk Lingkungan Perkantoran. *Journal Artificial: Informatika Dan Sistem Informasi*, 4(1), 78–88. <https://doi.org/10.54065/artificial.1130>
- Prasetya, A., Arganata, M. D., & Sutabri, T. (2024). Analisis perbandingan antara teknologi cloud computing dan infrastruktur komputer tradisional dalam konteks bisnis. *Scientica: Jurnal Ilmiah Sains dan Teknologi*, 2(7), 143–147. <https://doi.org/10.572349/scientica.v2i7.1725>
- Pratama, W. A., & Prasetyo, K. W. (2024). Leveraging cloud computing for network infrastructure disaster mitigation and recovery. *Jurnal Komputasi*, 13(1). <https://doi.org/10.23960/komputasi.v13i1.278>
- Purba, A. A. E., & Nasution, M. I. P. (2025). Business Intelligence dalam Era Ekonomi Digital: Kajian Sistematis atas Strategi dan Implementasi. *Journal Artificial: Informatika Dan Sistem Informasi*, 3(2), 161–171. <https://doi.org/10.54065/artificial.753>
- Putri, N. I., Iswanto, I., Widhiantoro, D., Munawar, Z., & Soerjono, H. (2022). Penerapan manajemen risiko pada komputasi awan. *TEMATIK*, 9(2), 144–151. <https://doi.org/10.38204/tematik.v9i2.1074>
- Rakhmat, E., Dwiyatno, S., Irawan, A., & Setiawan, F. (2021). Pemanfaatan aplikasi ownCloud pada sistem keamanan cloud computing. *Jurnal Sistem Informasi dan Informatika (SIMIKA)*, 4(2). <https://doi.org/10.47080/simika.v4i2.1097>
- Rozi, F., Ibrahim, A. M., & Pujiastuti, E. (2023). Analisis ancaman keamanan dalam penggunaan teknologi cloud computing. *Jurnal Sistem Informasi, Teknologi Informatika dan Komputer*, 14(3), 209–219. <https://doi.org/10.24853/justit.14.3.209-219>
- Sijabat, H. H., & Widjaja, G. (2025). Privasi dan keamanan data dalam layanan cloud: Perspektif hukum dan regulasi. *SIBATIK Journal*, 4(4). <https://doi.org/10.54443/sibatik.v4i4.2649>
- Simamora, S. C., Gaffar, V., & Arief, M. (2024). Systematic literature review dengan metode PRISMA: Dampak teknologi blockchain terhadap periklanan digital. *Jurnal Ilmiah M-Progress*, 14(1). <https://doi.org/10.35968/m-pu.v14i1.1182>
- Suryawijaya, M. R., & Praptodiyono, S. (2024). Pemanfaatan komputasi awan untuk pengarsipan digital di Indonesia. *Jurnal Ilmu Komputer dan Teknologi (IKOMTI)*, 5(3), 1–7. <https://doi.org/10.35960/ikomti.v5i3.1479>
- Tantowi, L., & Wijayanti. (2023). Peluang dan tantangan penyimpanan cloud storage pada dokumen digital. *Shaut Al-Maktabah: Jurnal Perpustakaan, Arsip dan Dokumentasi*, 15(1). <https://doi.org/10.37108/shaut.v15i1.803>
- Tu, Z., An Wang, X., Du, W., Wang, Z., & Lv, M. (2023). An improved multi-copy cloud data auditing scheme and its application. *Journal of King Saud University - Computer and Information Sciences*, 35(3), 120–130. <https://doi.org/10.1016/j.jksuci.2023.01.021>
- Widarma, A., Siregar, H. F., & Sitorus, I. R. (2023). Implementasi cloud computing menggunakan Nextcloud berbasis infrastruktur as a service (IaaS). *CESS (Journal*

of Computer Engineering, System and Science), 9(1).

<https://doi.org/10.24114/cess.v9i1.55993>

Wulan, W., Hadita, H., Fauzi, A., Putri, A. M., Fitriyani, F., Astriyani, R., Arisana, V., & Cahyani, Y. I. (2024). Tinjauan ancaman dan risiko pada sistem keamanan Internet of Things berbasis cloud computing dalam penggunaan e-commerce dan rencana strategis. *Jurnal Kewirausahaan dan Multi Talenta*, 2(2), 126–137.

<https://doi.org/10.38035/jkmt.v2i2.164>

Zaki, A., Damanik, A. P., Syahnur, E. A., Yahya, H., Naufal, M., Hibrizi, F., & Nugraha, R. K. (2023). Implementasi cloud computing berbasis software as a service (SaaS) menggunakan ownCloud untuk pengolahan data mahasiswa sistem informasi UINSU. *Jurnal Informatika*, 1(3).

Zhang, Q., Chen, M., Li, L., & Chen, J. (2022). . *IEEE Access*, 10, 103545–103567.

<https://doi.org/10.1109/ACCESS.2022.3201234>