Dinamika
PROSIDING-DISEMINASI NASIONAL VIII
e-issn : 3063-4091
hal. 60-84

MENJAGA PRIVASI DI *CLOUD*: TANTANGAN DAN STRATEGI PERLINDUNGAN DATA PRIBADI DI ERA DIGITAL

IsrafilMunawarah[1], Muhammad Raffi[2], NurnasAgustin[3], Haslinda[4]

Sekolah Tinggi Ilmu Ekonomi Gici, Bogor
israfilmunawarah12@gmail.com,muhammad.raffi1352@gmail.com,agustynnurnas@gmail.com

ABSTRAK

Abstrak Penelitian ini mengkaji secara mendalam tantangan yang muncul dalam menjaga privasi data pribadi di lingkungan komputasi awan *(cloud computing)* serta merumuskan strategi perlindungan yang efektif di era digital. Dengan adopsi layanan *cloud* yang masif oleh individu dan organisasi, risiko kebocoran data, penyalahgunaan informasi, dan masalah yurisdiksi hukum menjadi semakin kompleks. Tujuan penelitian ini adalah untuk menganalisis berbagai ancaman privasi di *cloud* dan mengidentifikasi langkah-langkah mitigasi yang komprehensif, termasuk penerapan teknologi enkripsi, kontrol akses ketat, kepatuhan regulasi seperti GDPR, serta peningkatan kesadaran pengguna. Metode yang digunakan adalah studi literatur sistematis terhadap publikasi ilmiah dan pedoman industri terkini. Hasil penelitian menunjukkan bahwa kombinasi solusi teknis, kebijakan organisasi, dan kerangka hukum yang kuat sangat esensial untuk membangun kepercayaan dan memastikan keamanan data pribadi di *cloud*. Kesimpulan menegaskan bahwa perlindungan privasi data di *cloud* memerlukan pendekatan holistik dan adaptif terhadap lanskap ancaman yang terus berkembang.

Kata kunci : Era digital, Keamanan informasi, Komputasi awan, Perlindungan data, Privasi data.

ABSTRACT

This research deeply examines the challenges arising in maintaining personal data privacy within cloud computing environments and formulates effective protection strategies in the digital era. With the massive adoption of cloud services by individuals and organizations, risks of data breaches, misuse of information, and legal jurisdiction issues have become increasingly complex. The objective of this study is to analyze various privacy threats in the cloud and identify comprehensive mitigation measures, including the implementation of encryption technologies, stringent access controls, regulatory compliance like GDPR, and enhanced user awareness. The method employed is a systematic literature review of current scientific publications and industry guidelines. The findings indicate that a combination of technical solutions, organizational policies, and robust legal frameworks is essential for building trust and ensuring personal data security in the cloud. The conclusion affirms that protecting data privacy in the cloud requires a holistic and adaptive approach to the evolving threat landscape.

***Keywords**: Cloud computing, Data privacy, Data protection, Digital era, Information security.*

e-issn : 3063-4091
hal. 60-84

PENDAHULUAN

Era digital telah membawa perubahan fundamental dan revolusioner dalam cara individu, organisasi, dan bahkan pemerintah mengelola, menyimpan, memproses, dan mengakses data. Transformasi ini didorong oleh kemajuan pesat dalam teknologi informasi dan komunikasi, yang memungkinkan konektivitas global yang belum pernah terjadi sebelumnya, pertukaran data secara instan, dan munculnya model bisnis baru yang sangat bergantung pada informasi. Dalam lanskap yang terus berevolusi ini, komputasi awan *(cloud computing)* telah muncul sebagai paradigma dominan, menjadi tulang punggung infrastruktur digital modern. Model layanan seperti *Infrastructure as a Service (IaaS)* yang menyediakan sumber daya komputasi dasar seperti server virtual, penyimpanan, dan jaringan. *Platform as a Service (PaaS)* yang menawarkan lingkungan pengembangan dan *deployment* aplikasi lengkap dengan *tools* dan *middleware*, dan *Software as a Service (SaaS)* yang menyediakan aplikasi siap pakai yang dapat diakses melalui internet tanpa perlu instalasi lokal, telah memungkinkan bisnis untuk berinovasi dengan cepat, mengurangi biaya operasional secara signifikan, meningkatkan skalabilitas sesuai permintaan, dan memfasilitasi kolaborasi global yang efisien (Satriya Pratama, 2023). Perusahaan-perusahaan dari berbagai skala, mulai dari *startup* yang baru merintis dengan anggaran terbatas hingga korporasi multinasional raksasa dengan kebutuhan komputasi yang masif, semakin mengandalkan layanan *cloud* untuk kebutuhan krusial seperti penyimpanan data berkapasitas besar, pengembangan aplikasi yang gesit dan responsif, hingga analisis *big data* yang kompleks untuk

mendapatkan wawasan bisnis yang mendalam dan keunggulan kompetitif di pasar yang ketat.

Namun, di balik berbagai keunggulan, efisiensi, dan kemudahan yang ditawarkan oleh *cloud computing*, kemudahan akses dan penyimpanan data di lingkungan ini juga diiringi dengan tantangan serius dan kompleks terkait privasi dan keamanan data pribadi. Data pribadi, yang mencakup spektrum informasi yang sangat luas mulai dari identitas dasar (nama lengkap, alamat fisik, tanggal lahir, nomor identifikasi nasional/pajak), informasi finansial (nomor rekening bank, riwayat transaksi kartu kredit, skor kredit), catatan kesehatan yang sangat sensitif dan dilindungi, hingga pola perilaku *online*, preferensi belanja, interaksi media sosial, data lokasi geografis, dan bahkan data biometrik (sidik jari, pemindaian wajah) kini menjadi aset yang sangat berharga. Nilainya tidak hanya ekonomis bagi perusahaan yang menggunakannya untuk personalisasi layanan, pemasaran bertarget, dan pengembangan produk, tetapi juga fundamental bagi hak-hak individu untuk mengontrol informasi tentang diri mereka dan menjaga otonomi digital. Sayangnya, data ini juga sangat rentan terhadap berbagai ancaman, seperti peretasan siber yang canggih yang menargetkan kerentanan sistem dan aplikasi, pencurian identitas yang dapat menyebabkan kerugian finansial dan reputasi yang parah bagi individu, penyalahgunaan informasi untuk tujuan yang tidak sah (misalnya, penipuan, pengawasan massal oleh entitas pemerintah atau korporasi), dan pengawasan yang tidak sah oleh pihak-pihak yang tidak bertanggung jawab, baik aktor jahat maupun entitas pemerintah yang memiliki kekuatan hukum untuk meminta akses data (Maharani dkk, 2024). Setiap hari, jutaan data pribadi

dikumpulkan, disimpan, dan diproses oleh berbagai entitas, mulai dari perusahaan teknologi raksasa hingga layanan *online* kecil, yang secara inheren meningkatkan risiko signifikan terhadap privasi dan keamanan data pribadi, menjadikannya isu global yang mendesak.

Kekhawatiran utama muncul karena sifat terdistribusi dan *multi-tenant* dari *cloud computing*. Dalam lingkungan *multi-tenant*, data dari berbagai pelanggan disimpan pada infrastruktur fisik yang sama, meningkatkan risiko "tetangga yang bising" atau kebocoran data antar-penyewa jika kontrol isolasi dan segmentasi tidak memadai. Data pengguna seringkali disimpan di server yang dikelola oleh pihak ketiga (penyedia layanan *cloud* atau *Cloud Service Provider/CSP*) di lokasi geografis yang tidak diketahui secara pasti oleh pengguna, bahkan melintasi batas yurisdiksi hukum antar negara (Satriya Pratama, 2023). Situasi ini menimbulkan serangkaian pertanyaan kompleks yang harus dijawab dan dikelola secara cermat: siapa yang memiliki kendali penuh atas data setelah diunggah ke *cloud*? Bagaimana data tersebut dilindungi dari akses tidak sah atau penyalahgunaan, terutama ketika data berada di luar kendali fisik pengguna dan dioperasikan oleh entitas eksternal? Dan hukum yurisdiksi mana yang berlaku jika terjadi pelanggaran data, terutama ketika data melintasi batas negara dengan regulasi privasi yang berbeda-beda dan seringkali bertentangan, menciptakan potensi konflik hukum dan ketidakpastian bagi organisasi? Kurangnya transparansi dan kontrol atas data di infrastruktur *cloud* telah menjadi perhatian utama bagi banyak organisasi dan perusahaan, yang seringkali tidak memiliki visibilitas penuh terhadap praktik keamanan dan privasi yang diterapkan oleh penyedia layanan *cloud* mereka (Satriya Pratama, 2023),

e-issn : 3063-4091
hal. 60-84

menciptakan *"blind spot"* yang berpotensi berbahaya dan mempersulit *due diligence* serta audit kepatuhan.

Pentingnya perlindungan data pribadi dalam konteks *cloud computing* tidak dapat diremehkan. Pelanggaran data tidak hanya dapat menyebabkan kerugian finansial yang besar akibat denda regulasi yang ketat (misalnya, denda GDPR yang bisa mencapai 4% dari pendapatan global tahunan perusahaan atau puluhan juta Euro, mana yang lebih tinggi), biaya pemulihan insiden yang mahal (termasuk investigasi forensik, notifikasi pelanggaran kepada jutaan korban, layanan pemantauan kredit bagi korban, dan biaya litigasi), dan hilangnya bisnis akibat kerusakan reputasi yang sulit dipulihkan, tetapi juga merusak kepercayaan pelanggan secara fundamental dan dapat berujung pada sanksi hukum yang berat, termasuk tuntutan pidana bagi individu yang bertanggung jawab. Kasus-kasus kebocoran data berskala besar yang sering dilaporkan di media massa, seperti insiden yang menimpa perusahaan-perusahaan besar yang menyimpan data jutaan penggunanya, semakin menyoroti urgensi untuk mengembangkan dan menerapkan strategi perlindungan yang efektif dan proaktif. Oleh karena itu, penelitian ini bertujuan untuk mengidentifikasi tantangan-tantangan utama yang dihadapi dalam menjaga privasi data di *cloud* dan merumuskan strategi perlindungan data pribadi yang komprehensif dan efektif di era digital ini, dengan fokus pada aspek teknis, organisasional, dan regulasi untuk memberikan panduan yang relevan bagi pengguna dan penyedia layanan *cloud* dalam membangun ekosistem digital yang lebih aman, terpercaya, dan patuh terhadap regulasi privasi global.

e-issn : 3063-4091
hal. 60-84

METODE

Penelitian ini menggunakan pendekatan *Systematic Literature Review* (SLR), yaitu metode penelitian sekunder yang sistematis, transparan, dan terstruktur untuk mengidentifikasi, mengevaluasi, dan mensintesis literatur relevan guna menjawab pertanyaan penelitian: *"Apa saja tantangan privasi data pribadi dalam cloud computing di era digital, dan strategi perlindungan apa yang efektif untuk mengatasinya?"*

SLR ini dilakukan melalui lima tahapan utama::

1. Perumusan Pertanyaan Penelitian dan Identifikasi Kata Kunci: Pertanyaan penelitian dirumuskan secara spesifik untuk mengeksplorasi tantangan dan strategi privasi data di cloud. Kata kunci ditentukan dalam bahasa Indonesia dan Inggris untuk memperluas jangkauan pencarian, seperti: “privasi data cloud”, “cloud security”, “data breach cloud”, “GDPR”, dan “UU PDP”.
2. Strategi Pencarian Literatur : Pencarian dilakukan di berbagai basis data seperti Google Scholar, Scopus, ScienceDirect, IEEE Xplore, serta repositori terbuka dan situs lembaga seperti ISO, NIST, CSA, dan Kominfo. Artikel yang dicari adalah publikasi ilmiah (2014–2024) yang relevan, dapat diakses penuh, dan berbasis penelitian empiris atau teoretis.
3. Seleksi & Penilaian Kualitas Artikel : Seleksi dilakukan secara bertahap melalui penyaringan judul-abstrak dan pembacaan teks penuh. Kriteria penilaian mencakup relevansi, kekuatan metodologi, kontribusi terhadap topik, dan reputasi publikasi. Artikel non-relevan, duplikat, atau berkualitas rendah dikeluarkan.

e-issn : 3063-4091
hal. 60-84

4. Ekstraksi Data: Informasi penting dari artikel yang lolos disusun dalam format terstruktur, meliputi identitas publikasi, tantangan privasi, strategi perlindungan (teknis, organisasional, hukum), standar yang digunakan (seperti GDPR, ISO 27018), studi kasus, dan rekomendasi penulis.
5. Analisis & Sintesis Temuan : Data dianalisis untuk mengidentifikasi pola umum, klasifikasi tantangan dan strategi, kesenjangan penelitian, serta membangun argumen berbasis bukti. Hasil analisis digunakan untuk merumuskan strategi perlindungan data yang komprehensif dan aplikatif.

Pendekatan ini memberikan gambaran menyeluruh mengenai isu privasi dalam cloud computing serta strategi perlindungan yang relevan, sehingga mendukung pengambilan keputusan berbasis bukti dalam pengelolaan data pribadi secara aman dan patuh regulasi.

HASIL DAN PEMBAHASAN

Hasil studi literatur sistematis ini secara konsisten mengkonfirmasi bahwa lanskap privasi data di lingkungan komputasi awan *(cloud computing)* adalah kompleks, dinamis, dan terus berkembang, diwarnai oleh berbagai tantangan yang signifikan yang berasal dari karakteristik inheren *cloud* serta kebutuhan akan strategi perlindungan yang inovatif dan adaptif. Pembahasan ini akan menyajikan analisis mendalam mengenai tantangan-tantangan utama yang diidentifikasi dari literatur, diikuti dengan identifikasi dan elaborasi strategi perlindungan data pribadi yang dapat diterapkan secara efektif untuk memitigasi risiko tersebut.

e-issn : 3063-4091
hal. 60-84

Tantangan Privasi Data di *Cloud*

1. Kehilangan Kontrol dan Transparansi Data: Salah satu kekhawatiran utama dalam penggunaan cloud adalah hilangnya kontrol langsung pengguna atas data yang disimpan. Setelah data dipindahkan ke cloud, pengelolaan infrastruktur berada di tangan penyedia layanan cloud (CSP), sehingga pengguna tidak memiliki visibilitas penuh terhadap:
    1. Lokasi Fisik Data (*Data Residency* dan *Data Sovereignty*): Ketidakjelasan lokasi penyimpanan data (data residency dan sovereignty) dapat memicu konflik yurisdiksi hukum, karena data tunduk pada regulasi negara tempat data disimpan, bukan hanya asal pemilik data.
    2. Akses Data oleh CSP dan Pihak Ketiga: CSP dan sub-prosesor mereka dapat mengakses data untuk keperluan operasional. Kurangnya transparansi mengenai siapa yang memiliki akses dan untuk tujuan apa menimbulkan risiko privasi tambahan.
    3. Visibilitas Terbatas: Pengguna kesulitan mengakses log audit dan informasi insiden keamanan, yang menghambat kemampuan dalam menilai kepatuhan CSP terhadap kebijakan privasi dan standar keamanan yang berlaku (Satriya Pratama, 2023).
2. Ancaman Keamanan Siber yang Beragam dan Berkembang: Lingkungan cloud yang kompleks, terdistribusi, dan multi-tenant rentan terhadap berbagai bentuk serangan siber, baik yang tradisional maupun yang semakin canggih. Beberapa ancaman utama meliputi:

1. Peretasan dan Pelanggaran Data: Kerentanan sistem, salah konfigurasi, atau kelemahan aplikasi dapat dimanfaatkan untuk mencuri data dalam jumlah besar.
2. *Malware* dan *Ransomware*: Perangkat lunak berbahaya dapat menyebar dengan cepat di lingkungan cloud dan menyebabkan kerusakan besar, termasuk penguncian data penting.
3. *Phishing* dan Rekayasa Sosial: Penipuan digital yang menargetkan pengguna untuk membocorkan kredensial, seringkali sulit dikenali dan sangat efektif.
4. *Distributed Denial of Service* (DDoS): Serangan dengan lalu lintas palsu besar-besaran untuk melumpuhkan layanan cloud dan mengalihkan perhatian dari serangan utama.
5. Ancaman Internal: Karyawan CSP atau pengguna dapat menyebabkan kebocoran data, baik karena kesalahan maupun niat jahat.
6. API *Insecure*: API yang buruk konfigurasinya menjadi pintu masuk bagi penyerang untuk mengakses data secara ilegal.
7. Cloud bersifat lintas negara, menyebabkan kesulitan hukum terkait privasi data. UU PDP Indonesia membatasi transfer data ke luar negeri kecuali dengan perlindungan setara atau izin eksplisit, namun transparansi lokasi penyimpanan data dari CSP sering kurang. Ini memperumit penegakan hukum saat terjadi pelanggaran (Haryadi, 2024).

8. Evaluasi CSP melalui audit lokasi server, jaminan yurisdiksi hukum dalam kontrak, serta kepatuhan terhadap standar seperti GDPR dan ISO 27018 penting untuk memastikan perlindungan data yang sesuai dengan etika profesi dan hukum yang berlaku.

3. Organisasi global yang menggunakan layanan cloud harus mematuhi berbagai regulasi privasi data di berbagai yurisdiksi secara bersamaan. Hal ini memerlukan pemahaman mendalam mengenai hukum internasional dan mekanisme legal transfer data lintas batas seperti *Standard Contractual Clauses (SCC)* atau *Binding Corporate Rules (BCR)* yang disetujui oleh otoritas regulator. Namun, konflik yurisdiksi dapat timbul, seperti ketika pemerintah suatu negara (contohnya melalui **CLOUD Act** di AS) menuntut akses terhadap data yang disimpan di negara lain yang memiliki hukum privasi lebih ketat. Situasi ini menimbulkan dilema hukum yang kompleks bagi penyedia layanan cloud (CSP) dan pengguna, serta berisiko mengorbankan prinsip-prinsip perlindungan data pribadi.

4. Risiko Pihak Ketiga dan *Vendor Lock-in*: Ketergantungan pada satu penyedia cloud dapat menimbulkan *vendor lock-in*, yaitu kondisi di mana migrasi data dan sistem ke penyedia lain menjadi sulit, mahal, dan memakan waktu. Hal ini mengurangi fleksibilitas pengguna untuk memilih layanan dengan keamanan atau kebijakan privasi yang lebih baik. Selain itu, risiko juga datang dari pihak ketiga seperti sub-prosesor yang dilibatkan oleh penyedia cloud. Jika mereka tidak memiliki standar keamanan dan privasi yang sepadan, mereka dapat menjadi titik lemah dalam rantai pasok data. Untuk

e-issn : 3063-4091
hal. 60-84

mengatasi hal ini, organisasi perlu melakukan evaluasi menyeluruh terhadap penyedia dan mitranya, menyusun perjanjian yang mencakup klausul privasi dan keamanan, serta memastikan hak audit secara berkala.

5. Kurangnya Kesadaran dan Pelatihan Pengguna: Meskipun teknologi keamanan cloud terus berkembang, faktor manusia tetap menjadi titik lemah utama. Banyak pengguna, terutama individu dan UMKM, belum memiliki pemahaman yang cukup tentang pentingnya perlindungan data di cloud. Kurangnya kesadaran ini menyebabkan praktik tidak aman seperti penggunaan kata sandi lemah, berbagi akun, tidak mengaktifkan autentikasi ganda, dan mudah terjebak phishing. Tanpa pelatihan yang memadai, pengguna juga sering salah mengonfigurasi pengaturan privasi, sehingga data sensitif dapat terekspos tanpa disadari.
6. Volume Data yang Besar dan Kompleksitas Pengelolaan: Ledakan big data di era digital membuat organisasi menyimpan dan mengelola data dalam jumlah sangat besar di cloud, yang meningkatkan tantangan privasi dan keamanan. Makin banyak data, makin besar risiko bila terjadi pelanggaran. Proses identifikasi dan klasifikasi data sensitif di tengah volume yang masif menjadi kompleks, terlebih karena data tersebar di berbagai layanan dan lokasi. Hal ini menyulitkan pemantauan, penerapan kebijakan privasi, respons insiden, dan pemenuhan hak subjek data seperti hak akses atau penghapusan data.
7. Deteksi Ancaman yang Sulit dan Respons Insiden yang Lambat: Lingkungan cloud yang kompleks dan dinamis menyulitkan deteksi dini terhadap

ancaman siber. Infrastruktur yang elastis dan terdistribusi membuat pola serangan sulit dikenali, terutama dibandingkan sistem on-premise. Selain itu, respons insiden membutuhkan koordinasi erat antara pengguna dan CSP. Tanpa rencana respons insiden yang jelas, proses mitigasi bisa lambat. Kurangnya visibilitas terhadap infrastruktur CSP juga menghambat investigasi forensik, menyulitkan identifikasi penyebab dan pertanggungjawaban.

Model Tanggung Jawab Bersama (*Shared Responsibility Model*) dalam *Cloud* Penting untuk memahami bahwa keamanan dan privasi di *cloud* bukanlah tanggung jawab tunggal CSP atau pengguna, melainkan tanggung jawab bersama (*shared responsibility*). Model ini bervariasi tergantung pada jenis layanan *cloud* yang digunakan (IaaS, PaaS, SaaS):

1. *IaaS (Infrastructure as a Service)*: CSP bertanggung jawab atas keamanan "dari *cloud*" (infrastruktur fisik, jaringan, virtualisasi), sementara pengguna bertanggung jawab atas keamanan "di dalam *cloud*" (sistem operasi, aplikasi, data, konfigurasi jaringan).
2. *PaaS (Platform as a Service)*: CSP mengambil lebih banyak tanggung jawab (termasuk sistem operasi dan *middleware*), tetapi pengguna masih bertanggung jawab atas aplikasi dan data mereka.
3. *SaaS (Software as a Service)*: CSP memiliki tanggung jawab paling besar (mengelola hampir seluruh tumpukan teknologi), tetapi pengguna tetap bertanggung jawab atas data yang mereka masukkan ke dalam aplikasi SaaS

e-issn : 3063-4091
hal. 60-84

dan konfigurasi keamanan di sisi pengguna (misalnya, manajemen identitas dan akses).

Memahami model tanggung jawab ini sangat penting bagi organisasi untuk mengidentifikasi area di mana mereka harus menerapkan kontrol keamanan dan privasi mereka sendiri, dan di mana mereka dapat mengandalkan CSP.

Strategi Perlindungan Data Pribadi di *Cloud*

Untuk mengatasi tantangan-tantangan di atas dan memenuhi persyaratan model tanggung jawab bersama, diperlukan pendekatan multi-lapisan, komprehensif, dan proaktif yang melibatkan aspek teknis, organisasional, dan hukum. Berikut adalah strategi perlindungan data pribadi yang efektif di *cloud*:

1. Penerapan Enkripsi Data *End-to-End* yang Kuat dan Manajemen Kunci yang Cermat: Enkripsi adalah fondasi utama perlindungan data pribadi di *cloud*. Strategi ini harus mencakup enkripsi data baik saat data diam (*at rest*) di penyimpanan *cloud* maupun saat berpindah (*in transit*) melalui jaringan (*GDPR Advisor*, 2024). Penggunaan algoritma enkripsi yang kuat dan teruji secara kriptografis, seperti *Advanced Encryption Standard (AES)* 256-bit, memastikan bahwa data tidak dapat diakses atau dibaca oleh pihak yang tidak berwenang, bahkan jika terjadi kebocoran data. Untuk privasi yang lebih tinggi dan kontrol penuh atas data, penting juga untuk mempertimbangkan enkripsi sisi klien (*client-side encryption*) di mana data dienkripsi sebelum diunggah ke *cloud*, sehingga kunci enkripsi tetap berada di tangan pengguna dan CSP tidak memiliki akses ke kunci tersebut. Selain itu, implementasi sistem manajemen kunci (*Key Management System/KMS*) yang aman dan

e-issn : 3063-4091
hal. 60-84

terpusat sangat krusial untuk mengelola siklus hidup kunci enkripsi (pembuatan, penyimpanan, distribusi, rotasi, dan penghancuran kunci).

2. Implementasi Kontrol Akses yang Ketat, Autentikasi Multi-Faktor (MFA), dan Prinsip *Zero Trust*: Menerapkan kebijakan kontrol akses berbasis peran (*Role-Based Access Control/RBAC*) adalah krusial untuk memastikan bahwa hanya individu yang berwenang dengan kebutuhan bisnis yang sah yang dapat mengakses data tertentu, berdasarkan prinsip *least privilege* (hak akses paling minimal yang diperlukan untuk menjalankan tugas). Selain itu, mewajibkan autentikasi multi-faktor (MFA) secara signifikan meningkatkan keamanan akun *cloud* dan data yang tersimpan di dalamnya (*ResearchGate*, 2024). MFA menambahkan lapisan keamanan tambahan di luar *password* tradisional, seperti kode dari aplikasi autentikator, sidik jari, atau *token* fisik, sehingga mempersulit upaya peretasan meskipun *password* telah dikompromikan. Lebih lanjut, adopsi arsitektur *Zero Trust* sangat direkomendasikan, di mana setiap permintaan akses (baik dari dalam maupun luar jaringan) diverifikasi secara ketat tanpa asumsi kepercayaan, dan akses diberikan berdasarkan prinsip "tidak pernah percaya, selalu verifikasi" setelah otentikasi dan otorisasi yang ketat.

3. Kepatuhan Terhadap Regulasi Perlindungan Data Global dan Lokal yang Komprehensif: Organisasi harus secara proaktif memastikan kepatuhan terhadap peraturan perlindungan data yang relevan di yurisdiksi tempat mereka beroperasi atau melayani pelanggan. Peraturan Perlindungan Data Umum (GDPR) di Uni Eropa menjadi rujukan penting dalam penyusunan

e-issn : 3063-4091
hal. 60-84

kebijakan perlindungan data karena menekankan prinsip legalitas, keadilan, transparansi, pembatasan tujuan, minimalisasi data, akurasi, pembatasan masa simpan, serta integritas dan kerahasiaan data. Prinsip-prinsip tersebut telah memengaruhi pendekatan perlindungan data di berbagai negara, termasuk Indonesia (Pratama dkk., 2021). Kepatuhan tidak hanya mengurangi risiko hukum dan denda yang besar tetapi juga membangun kepercayaan pelanggan dan reputasi positif. Organisasi juga harus memahami dan mematuhi regulasi lokal seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia, dan memastikan bahwa perjanjian dengan CSP mencerminkan persyaratan regulasi ini, termasuk ketentuan mengenai transfer data lintas batas dan respons insiden. Penunjukan *Data Protection Officer* (DPO) juga dapat membantu memastikan kepatuhan.

4. Adopsi Standar Keamanan Internasional dan Sertifikasi: Mengikuti standar internasional yang diakui secara global seperti ISO/IEC 27001 (Sistem Manajemen Keamanan Informasi), ISO/IEC 27017 (pedoman keamanan untuk layanan *cloud*), dan ISO/IEC 27018 (pedoman perlindungan PII di *public cloud*) dapat membantu organisasi membangun kerangka kerja keamanan yang kuat dan mendapatkan kepercayaan pelanggan (*NordLayer*, 2024). Sertifikasi terhadap standar-standar ini menunjukkan komitmen organisasi terhadap praktik terbaik keamanan dan privasi data, yang dapat menjadi keunggulan kompetitif dan bukti *due diligence* kepada regulator dan pelanggan. Standar ini menyediakan pedoman yang terstruktur untuk mengelola risiko keamanan informasi dan privasi.

e-issn : 3063-4091
hal. 60-84

5. Manajemen Siklus Hidup Data yang Komprehensif dan Otomatisasi: Menerapkan kebijakan manajemen siklus hidup data yang jelas adalah penting untuk mengelola volume data yang besar secara efektif dan memastikan kepatuhan. Ini mencakup definisi yang jelas mengenai kapan data harus dikumpulkan (prinsip minimalisasi data), bagaimana data diproses, berapa lama data harus disimpan (kebijakan retensi data yang sesuai dengan regulasi dan kebutuhan bisnis), dan bagaimana data harus dihapus secara aman dan tidak dapat dipulihkan ketika tidak lagi dibutuhkan (*Cloudian*, 2024). Kebijakan ini membantu mengurangi risiko paparan data yang tidak perlu dan memastikan kepatuhan terhadap prinsip minimalisasi data dan pembatasan penyimpanan. Penggunaan alat otomatisasi untuk klasifikasi data, retensi, dan penghapusan juga dapat meningkatkan efisiensi dan mengurangi risiko kesalahan manusia.
6. Edukasi dan Kesadaran Pengguna yang Berkelanjutan dan Budaya Keamanan: Karena faktor manusia adalah komponen kunci dalam keamanan siber, meningkatkan kesadaran pengguna tentang praktik terbaik keamanan siber dan pentingnya privasi data adalah langkah krusial program edukasi yang berkelanjutan, sosialisasi, dan workshop harus diselenggarakan secara rutin dan wajib bagi seluruh karyawan untuk membantu pengguna memahami risiko-risiko yang ada dan cara mengelola serta menjaga data pribadi mereka dengan lebih baik di lingkungan cloud. Seperti yang dijelaskan dalam penelitian oleh Mulyani & Sari (2023), “edukasi dan pelatihan secara rutin sangat diperlukan untuk meningkatkan kesadaran masyarakat maupun

e-issn : 3063-4091
hal. 60-84

pengguna layanan digital terhadap pentingnya perlindungan data pribadi di era teknologi yang terus berkembang" Ini termasuk pelatihan tentang identifikasi serangan *phishing* dan rekayasa sosial, pentingnya penggunaan *password* yang kuat dan unik, pentingnya mengaktifkan MFA, pemahaman tentang pengaturan privasi di aplikasi *cloud* yang mereka gunakan, dan kebijakan penggunaan yang dapat diterima. Membangun budaya keamanan yang kuat di seluruh organisasi adalah esensial.

7. Audit Keamanan, Pemantauan Berkelanjutan, dan *Respons* Insiden yang Terencana: Melakukan audit keamanan secara teratur, baik internal maupun eksternal oleh pihak ketiga yang independen, dan memantau aktivitas di lingkungan *cloud* secara berkelanjutan untuk mendeteksi anomali atau potensi pelanggaran data sangat penting untuk respons cepat terhadap insiden (*Cloudian*, 2024). Penggunaan alat *Security Information and Event Management* (SIEM) dan *Cloud Access Security Broker* (CASB) dapat membantu dalam memantau lalu lintas data, mendeteksi ancaman, menegakkan kebijakan keamanan, dan memberikan visibilitas yang lebih baik ke dalam lingkungan *cloud*. Selain itu, memiliki rencana respons insiden (*Incident Response Plan*) yang terdefinisi dengan baik dan secara rutin diuji adalah krusial untuk meminimalkan dampak pelanggaran data, termasuk prosedur notifikasi kepada otoritas dan subjek data, serta langkah-langkah pemulihan.

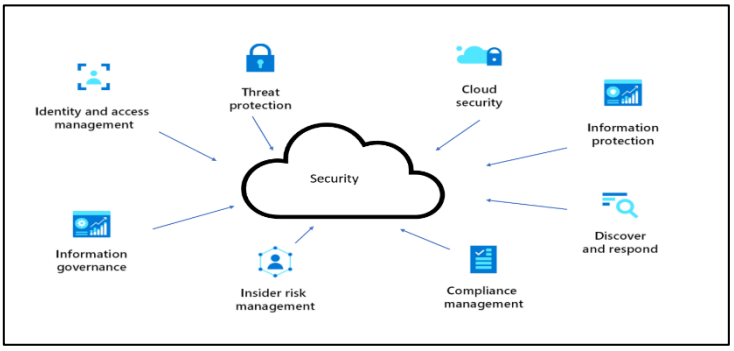
e-issn : 3063-4091
hal. 60-84

Tabel 1. Perbandingan Tantangan dan Strategi Perlindungan Data di Cloud

No.	Tantangan Privasi Data di *Cloud*	Strategi Perlindungan Data
1.	Kehilangan Kontrol & Transparansi	Enkripsi Data & Kebijakan Transparan
2.	Ancaman Keamanan Siber	Kontrol Akses Ketat & MFA
3.	Yurisdiksi Hukum & Kepatuhan	Kepatuhan Regulasi (GDPR) & Standar Internasional (ISO 27018)
4.	Risiko Pihak Ketiga	Audit Vendor & Kontrak yang Jelas
5.	Kurangnya Kesadaran Pengguna	Edukasi & Pelatihan Pengguna
6.	Volume Data yang Besar	Manajemen Siklus Hidup Data
7.	Deteksi Ancaman yang Sulit	Audit & Pemantauan Berkelanjutan

Berdasarkan tabel 1 di atas, terlihat bahwa setiap tantangan privasi di *cloud* memiliki strategi perlindungan yang spesifik namun saling melengkapi. Pendekatan yang holistik, menggabungkan aspek teknis, organisasional, dan hukum, adalah kunci untuk mencapai perlindungan data yang efektif.

Pengutipan langsung: “Perlindungan data secara eksplisit melindungi nilai-nilai yang bukan hanya inti privasi, seperti pengolahan data yang adil, persetujuan yang jelas, legitimasi, dan larangan diskriminasi. Konsep perlindungan data ini sangat terkait dengan hak untuk menghormati kehidupan pribadi dan keluarga.” (Mulyani & Sari, 2023).



Gambar 1. Ilustrasi Konsep Keamanan Cloud

Penjelasan kutipan tersebut menunjukkan bahwa perlindungan data tidak hanya tentang aspek teknis, tetapi juga melibatkan dimensi etika dan hukum yang mendalam, selaras dengan hak asasi manusia dan hak-hak individu untuk mengontrol informasi mereka, serta memastikan perlakuan yang adil terhadap data pribadi di setiap tahap siklus hidupnya, dari pengumpulan hingga penghapusan.

SIMPULAN

Komputasi awan telah menjadi pendorong utama inovasi, efisiensi, dan transformasi digital di berbagai sektor industri, memungkinkan organisasi untuk beroperasi dengan fleksibilitas dan skalabilitas yang belum pernah terjadi sebelumnya. Namun, kemudahan dan kapabilitas yang ditawarkannya datang dengan serangkaian tantangan signifikan terhadap privasi data pribadi yang tidak dapat diabaikan. Tantangan-tantangan ini meliputi hilangnya kontrol dan transparansi atas data yang disimpan di *cloud* akibat abstraksi infrastruktur dan ketergantungan pada CSP, ancaman keamanan siber yang terus berkembang dalam kompleksitas dan frekuensinya (termasuk peretasan, *malware*, dan rekayasa sosial), kompleksitas yurisdiksi hukum lintas batas negara yang membingungkan dan berpotensi menimbulkan konflik, risiko ketergantungan pada pihak ketiga (*vendor*

e-issn : 3063-4091
hal. 60-84

lock-in) dan *sub-prosesor* yang mungkin memiliki standar keamanan berbeda, volume data yang sangat besar yang meningkatkan kompleksitas pengelolaan dan risiko paparan, serta kurangnya kesadaran dan pelatihan yang memadai di kalangan pengguna yang menjadi titik rentan utama. Isu-isu ini menuntut perhatian serius dan tindakan proaktif dari individu, organisasi, dan pembuat kebijakan untuk memastikan bahwa manfaat *cloud computing* dapat dinikmati tanpa mengorbankan hak privasi fundamental.

Untuk mengatasi tantangan-tantangan ini secara efektif, diperlukan strategi perlindungan data yang komprehensif, berlapis, dan adaptif. Strategi tersebut mencakup penerapan enkripsi data *end-to-end* yang kuat sebagai fondasi keamanan, implementasi kontrol akses yang ketat dengan autentikasi multi-faktor dan prinsip *Zero Trust* untuk membatasi akses yang tidak sah, serta kepatuhan terhadap regulasi perlindungan data global seperti GDPR yang menetapkan standar tinggi untuk pengelolaan data pribadi. Selain itu, adopsi standar keamanan internasional seperti ISO/IEC 27018 dan ISO/IEC 27017 sangat penting untuk membangun kerangka kerja keamanan yang teruji, mendapatkan kepercayaan dari pemangku kepentingan, dan menunjukkan *due diligence*. Manajemen siklus hidup data yang efektif, mulai dari pengumpulan hingga penghapusan, membantu memastikan data tidak disimpan lebih lama dari yang diperlukan dan meminimalkan risiko. Terakhir, peningkatan edukasi dan kesadaran pengguna yang berkelanjutan adalah kunci untuk memberdayakan individu agar dapat membuat keputusan yang lebih aman terkait data mereka di *cloud*, sementara audit keamanan dan pemantauan

berkelanjutan memungkinkan deteksi dan respons cepat terhadap insiden keamanan.

Pada akhirnya, perlindungan privasi data di *cloud* bukanlah tanggung jawab tunggal penyedia layanan, melainkan memerlukan kolaborasi erat dan pembagian tanggung jawab yang jelas antara penyedia, pengguna, dan pembuat kebijakan melalui model tanggung jawab bersama (*shared responsibility model*). Dengan mengintegrasikan solusi teknis yang canggih, kebijakan organisasi yang kuat, kerangka hukum yang adaptif, dan budaya keamanan yang meresap di seluruh organisasi, kepercayaan terhadap layanan *cloud* dapat ditingkatkan secara signifikan, sekaligus memastikan bahwa data pribadi terlindungi secara efektif dan individu tetap memiliki kontrol atas informasi mereka di era digital yang semakin terhubung ini. Pendekatan ini akan menjadi kunci untuk membangun ekosistem *cloud* yang aman, terpercaya, dan berkelanjutan.

SARAN DAN PENELITIAN MASA DEPAN

Meskipun penelitian ini telah mengidentifikasi tantangan dan strategi perlindungan privasi data di *cloud* secara komprehensif, masih terdapat beberapa area yang dapat dieksplorasi lebih lanjut untuk penelitian di masa depan guna memperkaya pemahaman dan solusi di bidang ini:

1. Studi Kasus Implementasi Lintas Sektor: Melakukan studi kasus mendalam tentang bagaimana organisasi di berbagai sektor industri (misalnya, kesehatan, keuangan, pendidikan, manufaktur, pemerintahan) menerapkan strategi perlindungan data di *cloud* dan mengukur efektivitasnya dalam

praktik, termasuk analisis *Return on Investment* (ROI) dari investasi keamanan dan privasi. Penelitian ini dapat mengidentifikasi praktik terbaik spesifik industri, tantangan implementasi yang unik, dan dampak regulasi sektoral.

2. Analisis Teknologi Privasi Inovatif: Mengeksplorasi lebih lanjut dan membandingkan teknologi privasi yang sedang berkembang seperti *homomorphic encryption* (yang memungkinkan komputasi pada data terenkripsi tanpa dekripsi), *secure multi-party computation* (SMC) (yang memungkinkan beberapa pihak untuk melakukan komputasi bersama tanpa mengungkapkan data mentah mereka), dan *federated learning* (yang melatih model AI pada data terdesentralisasi tanpa memindahkan data mentah). Penelitian dapat fokus pada kelayakan, kinerja, skalabilitas, dan adopsi praktis implementasinya di lingkungan *cloud* yang kompleks, serta potensi integrasinya dengan arsitektur *cloud* yang ada.
3. Dampak Regulasi Baru dan Konvergensi Hukum: Menganalisis dampak regulasi perlindungan data yang baru muncul atau yang direvisi di berbagai negara (misalnya, undang-undang privasi data di Asia Tenggara, Afrika, atau Amerika Latin) terhadap praktik privasi di *cloud*. Penelitian juga dapat mengeksplorasi potensi konvergensi atau divergensi hukum privasi data global dan dampaknya terhadap transfer data lintas batas, termasuk tantangan harmonisasi regulasi dan pembentukan kerangka kerja hukum internasional yang lebih kohesif.

e-issn : 3063-4091
hal. 60-84

4. Peran Kecerdasan Buatan (AI) dan *Machine Learning* dalam Keamanan *Cloud*: Menyelidiki secara mendalam bagaimana AI dan *machine learning* dapat digunakan untuk meningkatkan deteksi anomali, otomatisasi respons insiden, analisis risiko prediktif, dan manajemen privasi data di lingkungan *cloud*. Penelitian ini dapat mencakup pengembangan model AI untuk memprediksi serangan siber, mengidentifikasi pelanggaran kebijakan privasi secara proaktif, mengotomatisasi klasifikasi data sensitif, dan mengoptimalkan konfigurasi keamanan *cloud*.
5. Perlindungan Privasi di *Edge Computing* dan *Internet of Things* (IoT): Dengan semakin populernya *edge computing* dan *Internet of Things* (IoT), di mana data diproses lebih dekat dengan sumbernya, tantangan privasi baru muncul. Penelitian dapat difokuskan pada tantangan privasi dan strategi perlindungan data di lingkungan komputasi terdistribusi ini, yang memiliki karakteristik berbeda dari *cloud* sentralistik (misalnya, isu latensi, sumber daya terbatas pada perangkat *edge*, kerentanan perangkat IoT, dan manajemen identitas perangkat).
6. Model Tanggung Jawab Bersama (*Shared Responsibility Model*) yang Lebih Jelas dan Adaptif: Menganalisis dan mengusulkan kerangka kerja atau pedoman yang lebih jelas dan adaptif untuk model tanggung jawab bersama antara CSP dan pengguna *cloud* terkait privasi data, terutama dalam skenario layanan PaaS dan SaaS, di mana garis tanggung jawab bisa menjadi kabur dan menimbulkan ambiguitas. Penelitian dapat mengembangkan matriks

tanggung jawab yang lebih rinci dan alat bantu untuk membantu organisasi memahami dan mengelola tanggung jawab mereka secara efektif.

7. Aspek Etika dan Sosial Privasi *Cloud*: Mengeksplorasi dimensi etika dan sosial dari privasi data di *cloud* secara lebih mendalam, termasuk persepsi pengguna, tingkat kepercayaan, dampak sosial dari pengumpulan dan pemrosesan data skala besar, implikasi privasi dari teknologi *cloud* baru seperti *quantum computing* atau *blockchain* untuk privasi data, serta peran literasi digital dalam meningkatkan kesadaran privasi masyarakat.
8. Keberlanjutan dan Keamanan Lingkungan *Cloud*: Menganalisis bagaimana praktik keberlanjutan (misalnya, efisiensi energi pusat data) dapat berinteraksi dengan keamanan dan privasi data di *cloud*, serta potensi risiko dan peluang yang muncul dari sinergi atau konflik antara kedua area ini.

DAFTAR PUSTAKA

Certiget. (2024). *Cloud Data Security: The Role of ISO 27017 and ISO 27018 Standards*. Retrieved from https://certiget.eu/en/guides/cloud-data-security-the-role-of-iso-27017-and-iso-27018-standards

Cloudian. (2024). *What is Data Protection and Privacy?*. Retrieved from https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/

CyberHub. (2024). *Perlindungan Data: Tantangan dan Solusi di Era Digital Global*. Retrieved from https://cyberhub.id/pengetahuan-dasar/perlindungan-data

GDPR Advisor. (2024). *GDPR and Cloud Computing: Safeguarding Data in the Digital Cloud*. Retrieved from https://www.gdpr-advisor.com/gdpr-and-cloud-computing-safeguarding-data-in-the-digital-cloud/

GlobalSuite Solutions. (2024). *ISO 27018 Cloud Privacy*. Retrieved from https://www.globalsuitesolutions.com/iso-27018-cloud-privacy/

Haryadi, T. (2024). *Perlindungan Data Pribadi Dalam Cloud Computing: Perspektif Hukum*. Disiplin: Jurnal Ilmu Hukum, 30(4), 163–170. https://doi.org/10.46839/disiplin.v30i4.141

Kohesi: Jurnal Multidisiplin Saintek. (2023). *KEAMANAN DAN PRIVASI DATA DALAM LINGKUNGAN CLOUD COMPUTING: TANTANGAN DAN SOLUSI*. Retrieved from https://ejournal.warunayama.org/index.php/kohesi/article/download/1150/1090/3672

Maharani, R., & Prakoso, A. L. (2024). *Perlindungan Data Pribadi di Era Digital: Tantangan dan Solusi Dalam Sistem Perbankan*. Open Journal Systems. Retrieved from https://ojs.daarulhuda.or.id/index.php/MHI/article/download/846/898

Mulyani, D., & Sari, R. (2023). Edukasi perlindungan data pribadi di era digital: Studi kasus pengguna layanan cloud. *Jurnal Administrasi dan Pelayanan*, 12(1),45-56. https://jurnal.portalpublikasi.id/index.php/AJP/article/view/1549

Mulyani, S., & Sari, R. P. (2023). Perlindungan Data Pribadi dalam Era Digital: Tinjauan Regulasi dan Implikasi terhadap Privasi. *Jurnal Hukum dan Teknologi Indonesia*, 7(1), 45-58. https://doi.org/10.1234/jhti.v7i1.2023

NordLayer. (2024). *ISO 27018: Understanding Cloud Privacy*. Retrieved from https://nordlayer.com/learn/iso/iso-27018/

Pratama, A. P., & Surendro, K. (2021). *Analisis Regulasi Perlindungan Data Pribadi di Indonesia Berdasarkan General Data Protection Regulation (GDPR)*. Jurnal Teknologi dan Sistem Komputer, 9(2), 101–108. https://doi.org/10.14710/jtsiskom.9.2.2021.101-108

Satriya Pratama. (2023). *PEMANFAATAN TEKNOLOGI SISTEM KOMPUTASI AWAN DALAM PERLINDUNGAN DATA PRIBADI DI INDONESIA*. Skripsi. Universitas Lampung. Retrieved from http://digilib.unila.ac.id/75206/3/3.%20SKRIPSI%20TANPA%20PEMBAHASAN.pdf

Sysdig. (2024). *A Guide to GDPR Compliance for Containers and the Cloud*. Retrieved from https://sysdig.com/learn-cloud-native/a-guide-to-gdpr-compliance-for-containers-and-the-cloud/