Journal of Research and Public Horizons
Volume:2, Nomor: 1, (2026), Juni: 313 - 330
Link Publish: https://ejournal.lppnusantara.com/index.php/jrph/article/view/898
E-ISSN: 3123-9595; DOI: https://doi.org/10.65244/jrph.v2i1.898

Analisis Risiko Keamanan Data Pribadi Pada Sistem Clound Computing

Beby Fadila [1], Muhammmad Irwan Padli Nasution [2]
Program Studi Manajeman, Universitas Islam Negeri Sumatera Utara, Medan, Indonesia [1,2]
Corresponding Author: bebyfadila575@gmail.com[1], irwannst@uinsu.ac.id[2]*

Info Artikel
Submitted: *21 Mei 2026*
Revised : *08 Juni 2026*
Accepted: *19 Juni 2026*
Published: *27 Juni 2026*

Keywords: *Cloud Computing; Personal Data Security; Risk Analysis; Encryption; Cyber Threat Mitigation*

Abstract
The rapid deveplopment of clound computing technology has driven various sectors to transition from local infrastructure to cloud-based platforms. While this shift provides significant benefits in data management efficiency and scalability, it also introduces complex security risks, particularly concerning the protection of users' personal data. This study aims to identify, classify, and analyze the key personal data security risks in cloud computing systems, and to formulate relevant mitigation recommendations. A systematic literature review method was applied, examining eight scientific articles focusing on cloud security, digital marketing, and information technology transformation. The analysis reveals that major threats include data breaches, unauthorized access, DoS/DDoS attacks, snooping, and multi-tenancy infrastructure exploitation. Effective security mechanisms include advanced encryption (AES-256, TLS 1.3), role-based access management, multi-factor authentication, and real-time threat monitoring. The findings confirm that collaboration between cloud service providers and users is a decisive factor in reducing security incidents by up to 30%. This study offers an analytical framework applicable by organizations in planning cloud-based information security governance.

Kata Kunci*: clound computing, keamanan data pribadi; Analisis risiko;Enkripsi; Mitigasi Ancaman Siber*

Abstrak
Perkembngan pesat teknologi clound computing telah mendorong berbagai sektor untuk beralih dari infrastuktur lokal ke platfrom berbasis awan. Perpindahan ini memberikan kemudahaan pengelolaan data, namun di sisi lain memunculkan risiko keamanan yang kompleks, terutama berkenaan dengan perlindungan data pribadi pengguna. Penelitian ini bertujuan mengidentifikasi, mengklasifikasi, dan menganalisis berbagi risiko keamanan data pribadi pada sistem clound computing, serta meruuskan rekomendasi mitigasi yang relevan. Metode yang digunakan adalah kajian literatur sistematis yang berfokus pada keamanan clound, pemasaran digital, dan transformasi teknologi informasi. Hasil analisis menunjukkan bahwa ancaman utama meliputi kebocoran data, akses tidak sah, serangan Dos/DDoS, snooping, attack, dan penyalahgunaan infrastruktur multi-tenancy. Mekanisme keamanan efektif mencakup enkripsi tingkat lanjut (AES-256, TLS 1.3), manajeman akses berbasis peran, autentikasi multi faktor,serta pemanatauan ancaman secara real-time. Kolaborasi atara penyediaan layanan clound dan pengguna terbukti menjadi faktor kunci dalam menurunkan insiden keamanan hingga 30%. Penelitian ini memberikan kerangka analitis yang dapat diadopsi oleh organisasi dalam merencanakan tata kelola keamanan informasi berbasis clound.

Publisher: Lembaga Penerbit Penelitian Nusantara

Pendahuluan

Transformasi digital yang berlangsung secara masif sejak awal abad ke-21 telah menempatkan clound computing sebagai infrastruktur inti dalam pngelolaan data skala besar. Teknologi ini memungkinkan akses sumber daya komputasi secara on-demand, mulai dari server, penyimpanan, basis data, jaringan, hingga bebagai layanan perangkat lunak, tanpa memerlukan pengelolaan fisik dari pengguna (Rifany,Prakoso, & Laksono,2023). Platfrom digital global seperti netflix, spotify, instagram, WhatsApp, dan tiktok semuanya bertumpu pada arsitektur clound untuk melayani miliaran pengguna di seluruh penjuru dunia.

Di sisi lain, meningkatnya ketergantungan terhadap clound computing turut memperluas permukaan serangan (attack surface) yang dapat dieksploitasi oleh pihak pikah yang tidak bertanggung jawab. Data dari berbagai laporan keamanan menunjukkan trend ancaman siber yang ters meningkat dari tahun ke tahun. Serangan berupa prncurian kredensial, peretasan antarmuka pemograman aplikasi (API), serangan penolakan layanan (DoS), serta kebocoran data merupakan ancaman yang paling umum dan berdampak besar terhadap integritas serta kerahasiaan informasi pengguna (Pandu,widodo,& Muttaqin,2024).

Isu keamanan data pribadi menjadi semakin krusial seiring berlakunya regulasi perlindungan data di berbagai negara, seperti General Data Protection Regulation (GDPR) di Eropa dan Undang-Undang Perlindungan Data Pribadi (UU PDP) di indonesia. Pelanggan terhadap regulasi tersebut tidak hanya berakibat pada sanski hukum yang berat, tetapi juga merusak kepercayaan publik terhadap layanan digital. Iiyasa (2021) menegaskan bahwa tata kelola keamanan informasi yang terstruktur menjadi persyaratak mutlak dalm penerapan clond computing yang bertanggung jawab.

Meskipun litaratur tentang keamanan cloud cukup berkembang, kajian yang secara khusus memetakan dan menganalisis risiko keamanan data pribadi dengan perpektif holistik mencakup jenis ancaman, mekanisme mitigasi, hingga perbandingan efektivitas solusi masih relatif terbatas. Penelitian ini bertujuan untuk mengisi celah tersebut melalui analisis sistematis berbasis kajian pustaka terhadap sumbr sumber ilmiah terkini.

Secara spesifik, penelitian ini berupaya menjawab tiga pertanyaan : (1) apa saja jenis risiko utama terhadap data pribadi pada sistem cloud computing, (2) mekanisme keamanan apa yang terbukti efektif dalam menghadapi risiko tersebut dan, (3) bagaimana peta perbandingan efektivitas berbagai solusi keamanan yang ada saat ini. Temuan penelitian diharapkan dapat memberikan panduan praktis bagi organisasi maupun pengembangan sistem dalam merancang strategi keamanan

data berbasis cloud komprehensif.

Tinjauan Pustaka

1. Konsep cloud computing dan arsitekturnya

Cloud computing sebagaimana didefinisikan oleh National Institute of Standards and Technology (NIST), adalah model komputasi yang memungkinkan akses jaringan yang nyaman, on-demand, dan dapat di konfigurasi terhadap sekumpulan sumber daya komputasi bersama termasuk jaringan, server, penyimpanan, aplikasi, dan layanan yang dapat disediakan serta dilepaskan dengan upaya manajeman minimal (llyasa, 2021). Secara arsitektural, cloud computing dibagi berdasarkan dua dimensi utama: lokasi dan model layanan.

Berdasarkan lokasinya, cloud diklasifikasikan ke dalam empat tipe : public cloud (infrastruktur dikelola penyedia cloud dan dapat di akses siapa saja), private cloud (infrastruktur ekslusif satu organisasi), hybrid cloud (kombinasi keduanya), serta community cloud (infrastruktur bersama oleh komuitas dengan kepentingan yang sama). Dari sisi model layanan, terdapata tiga kategori utama : Infrastructure as a service (IaaS) yang menyediakan sumber komputasi dasar, Platform as a Service (PaaS) yang menyedikan lingkungan aplikasi, dan Sofware as a Service (SaaS) yang menyediakan palikasi siap pakai berbasis internet (Rifany et.al,.2023).

Karakteristik fundamental cloud computing mencakup lima aspek : on-demand self service (layanan dapat dikonfigurasi tanpa intervensi manual penyediaan), broad network access (dapat di akses dari berbagai prangkat dan platrfrom), resource pooling (sumber daya dikumpulkan dan dibagikan secara multi-tenancy), rapid elasticity (kapasitas dapat ditingkatkan atau diturunkan secara dinamis), dan measured service (pengguna sumber daya dapat dipantau dan dikontrol secara transparan) (llyasa,2021). Karakteristik multi-tenancy dan elastisitas inilah yang sekaligus menjasi sumber kompleksitas keamanan yang paling signifikan dalam ekosistem cloud.

2. Data pribadi dan urgensi perlindungannya

Data pribadi merujuk pada segala informasi yang dapat digunakan untuk mengidentifikasi seorang individu, baik secara langsung maupun tidak langsung, termasuk nama, alamat, nomor identitas, data biometrik, riwayat transaksi keuangan, hingga perilaku daring pengguna. Dalam konteks layanan cloud yang digunakan oleh platfrom digital berskala besar, volume dan variasi data pribadi yang di proses mencapai tingkat yang sangat masif-mencakup miliaran rekaman dari pengguna di berbagai negara.

Keamanan informasi menjadi tiga prinsip fundamental yang dikenal sebagai triad CIA:

Confidentiality (kerahasiaan), Integrity (integritas), dan Availability (ketersediaan) data. Pelanggaran terhadap salah satu dimensi ini dapat menimbulkan kerugian material dan immaterian yang signifikan, baik bagi individu pengguna maupun bagi organisasi pengelola data. Di tengah konteks regulasi yang semakin ketat, kegagalan dalam melindungi data pribadi berisiko mengakibatkan denda besar, gugatan hukum, hingga pencabutan izin oprasional (pandu et al.,2024)

3. Keangka regulasi perlindungan data

Perlindungan data pribadi di era digital saat ini dilandasi oleh sejumlah regulasi internasional dan nasional. GDPR yang berlaku sejak 2018 di Uni Eropa menetapkan standar tinggi dalam pengumpulan, pemrosesan, dan penyimpanan data pribadi, dengan sanksi mencapai 4% dari omset global tahunann perusahaan yang melanggar. Di indonesia, UU No 27 Tahun 2022 tentang perlindungan data pribadi (UU PDP) mewajibkan setiap pengendali dan prosesor data untuk menerapkan langkah-langkah keamanan yang propesional terhadap risiko yang di hadapi.

Regulasi-regulasi ini mendorong penerapan prinsip privacy by design, yakni mengintegrasikan mekanisme perlindungan data sejak tahap perancangan sistem, bukan sekedar sebagai tambahan setelah sistem berjalan. Platrom digital besar seperti Netflix dan WhatsApp telah menunjukkan tingkat kepatuhan yan tinggi terhadap regulasi ini, sementara beberapa platfrom lain khususnya TikTok masih menghadapi tantangan dalam memenuhi persyaratan regulasi yang beragam di setiap yurisdiks (Pandu et al., 2024)

Dalam konteks indonesia, kerangka regulasi perlindungan data juga bersinggungan dengan peraturan pemerintah No. 71 Tahun 2019 tetntang penyelenggaraan sistem dan transaksi elektronik (PP PSTE) yang mewajibkan penyelenggara sistem elektronik unuk menyimpan, mengelola, dan memproses data di pusat data yang berlokasi di wilayah indonesia bagi data strategis. Ketentuan ini memiliki impikasi langsung bagi penyedia layanan cloud yang beroprasi bagi lintas batas, karena mereka harus memastikan bahwa data warga negara indonesia yang bersiat strategis tidak di proses semata-mata untuk infrastruktur luar negeri. Kebijakan lokasi data (data localization) semacam ini menjadi isu yang semakin kompleks dalam tata kelola keamanan cloud di era globalisasi digital.

4. Model Layanan Cloud dan Implikasi Keamanannya

Setiap layanan cloud memiliki karakteristik keamanan yang berbeda dan menentukan pembagian tanggung jawab antara penyediaan dan pengguna. Pada model LaaS, pengguna memiliki kendali penuh atas sistem informasi,aplikasi,dan data, sehingga tanggung jawab keamanan lapisan atas sepenuhnya berada di tangan pengguna. Penyedian hanya bertanggung jawab atas keamana fisik infrastruktur dan jaringan. Model ini memberikan fleksibilitas maksmial namun menuntut kapabilitas

keamanan yang tinggi dari sisi pengguna.

Model PaaS menggeser sebagian tanggung jawab keamanan kepada penyedia, yang kini menanggung keamanan runtime,middleware, dan sistem oprasi. Pengguna hanya perlu fokus pada keamanan data dan aplikasi yang mereka kembangkan di atas platfrom tersebut. Sementara itu pada model SaaS, penyedian menanggung hampir seluruh aspek keamanan teknis,dan pengguna hanya bertanggung jawabatas manajeman akun serta kebijakan penggunaan data. Implikasi dari pembagian ini adalah bahwa organisasi yang mengadopsi SaaS harus sangat selektif dalam memilih penyedia, karena merek menyerahkan sebagian besar kontrol kepada pihak eksternal (Rifany et al., 2023).

Pemahaman tentang model tanggung jawab bersama (shared responsibility model) ini menjadi fondasi penting dalam perencanaan keamanan cloud. Banyak insiden kebocoran data terjadi bukan karena kelemahan infrastruktur penyedia,melainkan karena kesalahpahaman pengguna tentang batas tanggung jawab mereka-misalnya mengira bahwa enkripsi data telah ditangani sepenuhnya oleh penyedia padahal konfigurasi enkripsi harus di aktifkan secr manual oleh penguna pada lapisan aplikasi.

5. Transformasi digital dan perluasan permukaan serangan.

Akselerasi transformasi digital yang di percepat oleh berbagai faktor- termasuk pandemi global,ekspansi eccommers,dan meningkatnya adopsi layanan streamin) g-telah secara dramatismemperluas permukaan serangan(ettack surface) pada ekosistem cloude.Sumerdana et al.(2024) mencatat bahwa hingga tahun 2022,pengguna internet di Indonesia mencapai 204,7 Juta jiwa atau sekitar 73,7% dari total populasi.Volume oengguna yang masuk ini menciotakan target yang sangat menggiur bagi para pelaku kejahatab siber.

Disi bisnis,adopsi ecommerce dan pemasarnan digital oleh UMKM indonesia turut memperluas permukaan serangan ini ke sekmen yang justru paling retan dari ss kapabilitas keamanan.Platfrom media sosial seperti instagram,tiktok dan facebook yang di gunakan secara masif untuk keperluan bisnis menyimpan data transaksi,preferensi konsumen,dan informasi kontak yang bernilai tinggi bagi pelaku kejahatn siber siastra dan adam,2017.Ketika data”ini di proses melalui infrastruktur cloud pihak ketiga tanpa pengamanan yang memadai,resiko kebocroan pribadi meninhgkat secara eksponensial

Metode Penelitian

Pemilihan ini menggunakam pendekatan kajian literatur sistematis (systematic literature rivew) untuk meng indentifikasi,meng evaluasi,dan mensintesis temuan dari berbagai sumber ilmiah yang

relavan.Pendektan ini di pilih karena memungkinkan pemetaan komprensif terhadap lanskap resiko keamanan data pada cloud computing dengan meng integrasikan presfektif dari berbagai bidang yang saling berkaitan-mulai dari keamanan sistem informasi,teknologi cloud,hingga transformasi digital.

Sumber data penelitia ini terdiri dari 8 artikel ilmiah yang di proleh dari jurnal jurnal bereputasi dalam bidang informatika,manajemen informasi,dan keamanan siber. Proses seleksi literatur mengikuti kriteria PICO (Population, Intervention, Comparison, Outcome): literatur yang berfokus pada sistem cloud computing (P), menjelaskan mekanisme atau insiden keamanan data (I), membandingkan berbagai pendekatan keamanan (C), dan menyajikan temuan terkait efektivitas perlindungan data pribadi (O). Artikel yang di terbitkan dalam rentan 2017-2024 di prioritaskan untuk memastikan relavansi remuan terhadap kondisi teknologi terkini.

Analisis data dilakukan melalui tiga tahapan. Pertama, ektrasi data : setiap literatur di baca secara mendalam untuk mengidentifikasi jenis ancaman, mekanisme mitigasi, dan bukti, empiris yang disajikan. Kedua, kategorisasi: temuan dikelompokkan berdasarkan dimensi risiko (ancaman teknis, ancaman administratif,dan ancaman regulasi) dan berdasarkan lapisan arsitektur cloud (IaaS,PaaS,SaaS). Ketiga, sintesis komparatif: efektivitas berbagai solusi keamanan dibandingkan secara kualitatif berdasarkan bukti yang tersedia dari masing masing sumber.

Validasi hasil dilakukan melalui triangulasi sumber, yakni memastikan bahwa setiap temuan utama didukung oleh minimal dua sumber literatur yang indivenden. Pendekatan ini bertujuan meminimalkan bias interpretasi dan meningkatkan realibilitas kesimpulan yang di hasilkan.

Batasan penelitian ini perlu diakui secara eksplisif. Kajian literatur sistematis sebagai metode penelitian memiliki keterbatasan dalam hal refresentasi empiris, karna tidak melakukan pengujian langsung terhadap sistem cloud yang ada. Selain itu, perkembangan ancaman siber yang sangat dinamis mengakibatkan temyan dari literatur yang diterbitkan beberapa tahun lalu mungkin sudah mengalami pergeseran relevansi. Oleh karena itu, temuan penelitian ini sebaiknya di validasi lebih lanjut melalui studi empiris di lapangan.

Kerangka analisis yang digunakan dalam peneltian ini mengacu pada standar internasional ISO-IEC 27001: 2013 tentang sistem menajema keamanan informasi (SMKI) dan NIST Cybersecurity Frameworrk sebagai referensi salam mengklasifikasikan dan mengevaluasi praktik kemananan yang ditemukan dalam literatur. Penggunaan kerangka strandar internasional ini memungkinkan komparasi yang lebih terstruktur antara berbagai pendekatan keamanan yang dibahas dalam berbagai sumber yang di kaji.

Hasil dan Pembahasan

Identifikasi dan Klasifikasi Risiko Keamanan Data Pribadi

Hasil kajian literatur mengidentifikasi enam kategori risiko utama yang secara langsung mengancam keamanan data pribadi pada sistem cloud computing. Setiap kategori memiliki vektor serangan, tingkat dampak, dan peendekatan mitigasi yang berbeda beda sebagaimana dirangkum dalam Tabel 1 berikut

Tabel 1. Klasifikasi Risiko Keamanan Data Pribadi pada Cloud Computing

No.	Jenis Risiko	Vektor Serangan	Tingkat Dampak	Mitigasi Utama
1	Kebocoran Data Pribadi	MITM, API tidak terautentikasi	Sangat Tinggi	Enkripsi end-to-end, TLS 1.3
2	Akses Tidak Sah (Unauthorized Access)	Credential stuffing, phishing	Tinggi	MFA, role-based access control
3	Denial of Service (DoS/DDoS)	Flooding, botnet	Tinggi	PoC, PoP, auto-scaling
4	Snooping & Traffic Analysis	Passive eavesdropping	Sedang	Enkripsi ICING, Onion Routing
5	Penyalahgunaan Sumber Daya	Multi-tenancy exploitation	Sedang	Isolasi VM, monitoring real-time
6	Kehilangan Data Permanen	Penghapusan berbahaya, bencana	Sangat Tinggi	Backup berlapis, SLA ketat

Sumber : Hasil analisis literatur (2024)

Dari enam kategori, yang teridentifikasi, kebocoran data pribadi dan kehilangan data permanen merupakan risiko dengan dampak paling tinggi. Kebocoran dat kerap terjadi melalui serangan Man-in-the-middle (MITM), dimana penyerang memposisikan dirinya diantara pengguna dan server cloud untuk menyadap atau memanipulasi arus data yang sedang di komunikasikan. Ilyasa (2021) mencatat bahwa serangan MITM merupakan salah satu penyebab utama insiden kebocoran data pada lingkungan cloud, pertama pada sistem yang belum mengimplementasikan enkripsi komunikasi secara menyeluruh.

Ancaman akses tidak sah (unauthorized acces) menjadi perhatian berikutnya. Sifat multi-tenacy cloud, dimana infrastruktur fisik digunakan bersama oleh banyak penyewa, menciptakan celah, yang potensial apabila mekanisme isolasi virtual machine tidak dikelola dengan ketat.

Rifanny et al., (2023) menegaskan bahwa kelemahan pada lapisan virtualisasi dapat memungkinkan seorang penyewa yang berniat jahat untuk mengakses data milik penyewa lain dalam lingkungan cloud yang sama.

Serangan denial of service (DoS-DDoS) meski tidak secar langsung mencuri data tetapi berdampak serius terhadap ketersediaan layanan dan secara tidak langsung dapat memicu celah keamanan lainnya. Berdasarkan data dari Pandu et al. (2024), trend insiden keamanan siber pada platrfom digital terus meningkat sepanjang periode 2019-2023, dengan netflix mencatat jumlah insiden tertinggi dibandingkan platfrom lain yang diteliti. Hal ini sebanding dengan sekala bayaran netflix yang melayani ratusan juta pengguna secara simultan.

Kaetegori risiko snooping attack dan traffic analysis, meskipun bersifat pasif dan tidak momodifikasi data target, memiliki implikasi serius terhadap privasi. Snooping attack terjadi ketika penyerang memposisikan dirinya untuk mengamati arus paket data yang melintas di jaringan tanpa terdeteksi. Dengan menganalisis pola trafik secara konsisten, penyerang dapat menyimpulkan informasi sensitef secara jadwal aktivitas pengguna, lawan bicara, atau bahkana isi komunikasi yang tidak terenkripsi, Ilyasa (2021) mencatat bahwa serangan jenis ini khususnya berbahaya dalam lingkungan multi-tenant cloud, dimana beberapa organisasi berbagai imfrastruktur fisik yang sama.

Penyalahgunan layanan cloud (service abuse) merupakan kategori risiko yang sering kali luput dari perhatian. Pemudahan dalam membuat akun cloud secara anonim atau menggunakan data identitas palsu memugkinkan pelaku kejahatan memanfaatkan infrastruktur cloud yang bertenaga tinggi untuk aktivitas ilegal mulai dari penambangan cryptocurrency secara tidak sah (cryptojacking), pengiriman spam masal, hingga penyelenggaraan infrastruktur untuk serangan siber terhadap pihak ketiga. Rifanny et al., (2023) menekankan bahwa karakteristik elastisitas dan

skalibilitas cloud yang menjadi daya tarik utamanya justru menjadi faktor yang memperparah dampak penyalahgunaan jenis ini, karena pelaku dapat dengan mudah meningkatkan kapasitas secara instan

Mekanisme Mitigasi dan Efektivitasnya

Berbagai mekanisme keamanan telah dikembangkan dan diimplementasikan untuk menghadapi risiko-risiko tersebut. Tabel 2 menyajikan perbandingan efektivitas beberapa mekanisme keamanan utama berdasarkan data dari literatur yang dikaji.

Tabel 2. Perbandingan Efektivitas Mekanisme Keamanan Cloud

Mekanisme Keamanan	Efektivitas	Biaya Implementasi	Platform Pengguna
Enkripsi Data (AES-256)	Tinggi (97%)	Rendah	Netflix, Spotify, WhatsApp
Role-Based Access Control	Tinggi (90%)	Sedang	Semua Platform Besar
Pemantauan Real-Time	Sedang (85%)	Sedang	TikTok, Instagram, Netflix
SSL/TLS 1.3	Sangat Tinggi	Rendah	Semua Platform
Multi-Factor Authentication	Sangat Tinggi	Sedang	Instagram, WhatsApp
Quantum Encryption (Eksperimental)	Sangat Tinggi (99%)	Tinggi	Riset Google & AWS

Sumber: Diadaptasi dari Pandu et al. (2024) dan Rifany et al. (2023)

Enkripsi data menggunakan algoritma AES-256 terbukti menjadi lini pertahanan paling andal dalam melindungi data pribadi pengguna. Pandu et al. (2024) melaporkan bahwa platform seperti Netflix, Spotify, dan WhatsApp yang menerapkan enkripsi tingkat lanjut mencatat efektivitas perlindungan data hingga 97%. Enkripsi bekerja dengan mengubah data menjadi format yang tidak

terbaca tanpa kunci dekripsi yang tepat, sehingga meskipun data berhasil dicuri, pelaku tidak dapat memanfaatkannya.

Mekanisme Onion Routing yang terinspirasi dari arsitektur NEBULA, rancangan jaringan cloud masa depanmenawarkan pendekatan inovatif dalam mengatasi ancaman traffic analysis. Mekanisme ini menyembunyikan identitas asli pengguna dengan merutekan paket data melalui beberapa lapisan enkripsi dan node antara. Sementara itu, mekanisme Proof of Path (PoP) dan Proof of Consent (PoC) dalam NEBULA dirancang untuk memastikan bahwa setiap paket data hanya melewati jalur yang telah terautentikasi d an disetujui oleh semua pihak yang terlibat, sehingga serangan DoS dan MITM dapat dicegah secara sistemik (Ilyasa, 2021).

Autentikasi multi-faktor (MFA) merupakan salah satu kontrol keamanan yang paling cost-effective mengingat kemampuannya mencegah akses tidak sah tanpa memerlukan perubahan infrastruktur yang signifikan. Rifany et al. (2023) merekomendasikan kombinasi beberapa faktor autentikasi, meliputi biometrik (sidik jari, pengenalan wajah), token one-time password (OTP), kartu identitas berbasis chip, serta kata sandi konvensional. Kombinasi faktor-faktor ini secara dramatis meningkatkan kesulitan bagi penyerang untuk melewati lapisan autentikasi, bahkan ketika satu faktor berhasil dikompromikan.

Dari sisi pemantauan, implementasi sistem monitoring real-time yang mengintegrasikan machine learning terbukti memiliki kemampuan deteksi anomali yang jauh lebih unggul dibandingkan sistem pemantauan berbasis aturan statis. Platform seperti Spotify memanfaatkan Google Cloud BigQuery dan Dataflow untuk menganalisis pola perilaku pengguna secara real-time, sehingga aktivitas mencurigakan dapat terdeteksi dan direspons dalam hitungan detik (Pandu et al., 2024).

Service Level Agreement (SLA) merupakan instrumen non-teknis yang memiliki peran penting dalam kerangka keamanan cloud. SLA mendefinisikan secara hukum standar layanan minimum yang harus dipenuhi penyedia, termasuk parameter ketersediaan (uptime), waktu respons insiden, prosedur pemulihan bencana, dan mekanisme kompensasi apabila terjadi pelanggaran. Ilyasa (2021) menekankan bahwa SLA yang dirancang dengan baik tidak hanya melindungi kepentingan pengguna secara hukum, tetapi juga mendorong penyedia untuk secara aktif memelihara standar keamanan yang tinggi demi menghindari penalti kontraktual.

Kontrol akses berbasis peran (Role-Based Access Control/RBAC) bekerja dengan prinsip least privilege, yakni memberikan setiap pengguna atau sistem hanya izin minimum yang diperlukan untuk menjalankan fungsinya. Dalam implementasi cloud enterprise, RBAC dikombinasikan

dengan manajemen identitas terpusat (Identity and Access Management/IAM) yang memungkinkan administrator untuk mendefinisikan, memantau, dan mencabut hak akses secara granular dari satu antarmuka terpadu. AWS IAM, Azure Active Directory, dan Google Cloud IAM adalah implementasi IAM paling banyak digunakan, masing-masing menawarkan fitur-fitur canggih seperti just-in-time access, conditional access policies, dan integrasi dengan sistem SIEM (Security Information and Event Management) (Rifany et al., 2023).

SSL/TLS (Secure Socket Layer/Transport Layer Security) menjadi protokol dasar yang mengamankan komunikasi data antara klien dan server cloud. Transisi dari TLS 1.2 ke TLS 1.3 membawa peningkatan signifikan dalam keamanan dan performa: TLS 1.3 menghapus algoritma kriptografi usang yang rentan (seperti RC4 dan MD5), mempersingkat proses handshake dari dua kali round-trip menjadi satu, dan memperkenalkan fitur forward secrecy yang memastikan bahwa kompromi kunci sesi di masa depan tidak dapat digunakan untuk mendekripsi komunikasi masa lalu. Pandu et al. (2024) mencatat bahwa WhatsApp mengimplementasikan enkripsi end-to-end yang dibangun di atas protokol Signal, lebih kuat dari TLS standar, untuk memastikan bahwa bahkan penyedia layanan sendiri pun tidak dapat membaca pesan pengguna.

Analisis Kesenjangan Perlindungan Data pada UMKM

Kontras yang mencolok terlihat antara kapabilitas keamanan platform digital berskala besar dengan realitas yang dihadapi oleh organisasi skala menengah ke bawah. Penelitian terkait strategi digital marketing pada UMKM Indonesia mengungkap bahwa sebagian besar pelaku usaha belum memiliki kesadaran yang memadai tentang risiko keamanan data dalam operasional digital mereka (Sumardana, Sussanti, & Damayanti, 2024). Padahal, UMKM yang mengadopsi platform e-commerce dan media sosial untuk keperluan pemasaran secara tidak langsung turut memproses data pribadi pelanggan mereka.

Ketergantungan UMKM terhadap layanan cloud pihak ketiga, seperti platform marketplace dan media social, menempatkan mereka dalam posisi yang rentan, karena keamanan data pelanggan mereka bergantung pada kebijakan keamanan platform yang digunakan, di luar kendali langsung pelaku usaha. Utami dan Fauzi (2023) menyoroti bahwa transformasi digital yang tidak diimbangi dengan peningkatan kapabilitas keamanan informasi dapat menciptakan risiko yang justru kontraproduktif bagi pertumbuhan usaha.

Kesenjangan ini mengindikasikan perlunya program literasi keamanan digital yang terarah bagi pelaku UMKM, mencakup pemahaman tentang risiko dasar keamanan data, tata cara memilih platform cloud yang aman, pengelolaan kata sandi yang baik, serta prosedur penanganan insiden

ketika data pelanggan mengalami kebocoran.

Data dari Rizky et al. (2020) menunjukkan bahwa strategi pemasaran digital berpengaruh terhadap keunggulan bersaing UMKM sebesar 78%, dengan variabel komunikasi online, ketersediaan transaksi digital, dan dukungan layanan pelanggan menjadi sub-indikator paling berpengaruh. Temuan ini menggarisbawahi betapa sentralnya infrastruktur digital—dan dengan demikian, keamanan cloud, terhadap keberlanjutan kompetitif UMKM. Ketika data pelanggan yang menjadi fondasi strategi digital marketing ini bocor atau disalahgunakan, dampaknya tidak hanya berupa kerugian finansial jangka pendek, tetapi juga kehilangan kepercayaan pelanggan yang sulit dipulihkan.

Syastra dan Adam (2017) dalam penelitian mereka tentang penggunaan media sosial berbasis Model AIDA untuk UKM menekankan pentingnya pendekatan strategis dalam pengelolaan platform digital. Ironisnya, aspek keamanan data tidak mendapat porsi perhatian yang memadai dalam sebagian besar panduan adopsi digital yang ditujukan bagi UMKM, menciptakan blind spot yang berbahaya. Pengembang kebijakan dan ekosistem pendukung UMKM perlu mengintegrasikan komponen keamanan siber dasar ke dalam setiap program pelatihan dan pendampingan digitalisasi usaha.

Peran Kolaborasi dalam Ekosistem Keamanan Cloud

Salah satu temuan paling signifikan dari penelitian ini adalah bahwa keamanan data pada cloud computing tidak dapat dicapai secara unilateral. Pandu et al. (2024) mendokumentasikan bahwa kemitraan strategis antara Netflix dan AWS, dua entitas yang memiliki kepentingan selaras dalam menjaga keamanan data pengguna, berhasil menurunkan jumlah insiden keamanan sebesar 30% dalam satu tahun. Keberhasilan ini dicapai melalui pemantauan bersama, berbagi informasi ancaman (threat intelligence sharing), dan respons insiden yang terkoordinasi.

Model kolaborasi semacam ini mencerminkan paradigma keamanan yang lebih matang, di mana keamanan dipandang sebagai tanggung jawab bersama seluruh ekosistem, bukan semata-mata beban yang ditanggung oleh satu pihak. Regulasi seperti GDPR secara eksplisit mengakui konsep shared responsibility ini dengan membedakan tanggung jawab antara pengendali data (data controller) dan prosesor data (data processor), masing-masing dengan kewajiban keamanan spesifik yang harus dipenuhi.

Perspektif kolaboratif ini juga relevan dalam konteks domestik Indonesia. Ilyasa (2021) mengusulkan sinergi antara pengguna layanan cloud, penyedia infrastruktur, dan regulator untuk menciptakan ekosistem penyimpanan data yang aman dan dapat dipercaya. Dalam kerangka ini,

regulator berperan menetapkan standar minimum keamanan, penyedia layanan bertanggung jawab atas keamanan infrastruktur, sementara pengguna berkewajiban mengelola akses dan kebijakan keamanan di sisi aplikasi.

Model kolaborasi lintas sektor ini juga dapat diperluas untuk mencakup komunitas riset dan akademisi. Inisiatif bug bounty, program yang memberikan penghargaan finansial kepada peneliti keamanan yang menemukan dan melaporkan kerentanan secara bertanggung jawab, telah diadopsi oleh AWS, Google Cloud, dan Microsoft Azure sebagai mekanisme crowdsourcing untuk pengujian keamanan. Pendekatan ini secara efektif memperluas kapabilitas pengujian keamanan jauh melebihi apa yang dapat dicapai oleh tim internal yang terbatas, sekaligus membangun hubungan positif dengan komunitas peneliti keamanan independen.

Prospek Teknologi Keamanan Masa Depan

Perkembangan teknologi membuka sejumlah inovasi keamanan yang menjanjikan untuk masa depan. Quantum encryption, yang memanfaatkan prinsip mekanika kuantum untuk menghasilkan kunci enkripsi yang secara teoritis tidak dapat dipecahkan oleh komputasi konvensional, tengah diuji coba oleh Google dan AWS dengan efektivitas yang diklaim mencapai 99% (Pandu et al., 2024). Meskipun teknologi ini masih dalam fase eksperimental, potensinya untuk merevolusi keamanan data sangat besar.

Integrasi kecerdasan buatan (AI) dalam sistem deteksi ancaman juga membuka dimensi baru dalam keamanan cloud. Sistem berbasis AI mampu mengenali pola serangan yang belum pernah terlihat sebelumnya (zero-day threats), menganalisis jutaan log keamanan secara simultan, dan merespons ancaman jauh lebih cepat dari yang mungkin dilakukan oleh analis manusia. Rifany et al. (2023) merekomendasikan investasi berkelanjutan dalam teknologi keamanan berbasis AI sebagai bagian dari strategi keamanan cloud yang berpandangan jauh ke depan.

Teknologi Zero Trust Architecture (ZTA) semakin mendapat perhatian sebagai pendekatan keamanan yang lebih relevan untuk lingkungan cloud modern. Berbeda dengan model keamanan perimeter tradisional yang mengasumsikan semua aktivitas di dalam jaringan internal bersifat tepercaya, ZTA menerapkan prinsip 'never trust, always verify', setiap permintaan akses, tanpa memandang asalnya, harus diautentikasi dan diotorisasi secara eksplisit. Implementasi ZTA pada infrastruktur cloud secara signifikan mengurangi risiko lateral movement oleh penyerang yang telah berhasil menembus lapisan pertahanan pertama, karena mereka tidak dapat bergerak bebas di dalam jaringan tanpa terus-menerus membuktikan identitas dan otorisasi mereka.

Analisis Perbandingan Penyedia Layanan Cloud dari Sisi Keamanan

Tiga penyedia layanan cloud dominan, Amazon Web Services (AWS), Google Cloud Platform (GCP), dan Microsoft Azure, memiliki pendekatan keamanan yang berbeda namun sama-sama komprehensif. AWS, sebagai pemimpin pasar, menawarkan ekosistem keamanan terlengkap dengan layanan seperti AWS Identity and Access Management (IAM), AWS Key Management Service (KMS) untuk enkripsi data, AWS GuardDuty untuk deteksi ancaman berbasis machine learning, serta AWS Shield untuk perlindungan DDoS. Netflix, sebagai salah satu pengguna terbesar AWS, memanfaatkan AWS CloudWatch untuk pemantauan real-time yang memungkinkan deteksi dan respons terhadap anomali keamanan dalam hitungan menit (Rifany et al., 2023).

Google Cloud Platform menonjol dalam kemampuan analitik data skala besar yang dapat dimanfaatkan untuk keperluan keamanan. Layanan BigQuery dan Dataflow memungkinkan pemrosesan log keamanan dalam volume sangat besar secara efisien, sementara Google Cloud Security Command Center menyediakan visibilitas terpusat terhadap postur keamanan seluruh infrastruktur cloud. Spotify, sebagai pengguna intensif GCP, memanfaatkan kemampuan machine learning Google untuk mengembangkan sistem deteksi anomali yang secara proaktif mengidentifikasi pola perilaku mencurigakan sebelum berkembang menjadi insiden keamanan (Pandu et al., 2024).

Microsoft Azure menonjolkan integrasi yang mulus dengan ekosistem Microsoft yang sudah digunakan secara luas di lingkungan enterprise, termasuk Active Directory, Office 365, dan berbagai solusi kepatuhan regulasi. Azure Sentinel sebagai platform SIEM cloud-native memungkinkan korelasi data dari berbagai sumber, termasuk sumber pihak ketiga—untuk memberikan gambaran ancaman yang komprehensif. Bagi organisasi yang telah menginvestasikan infrastruktur TI berbasis Microsoft, migrasi ke Azure menawarkan kurva pembelajaran yang lebih landai dengan tetap mempertahankan postur keamanan yang kuat.

Pemilihan penyedia layanan cloud tidak semata-mata ditentukan oleh fitur keamanan teknis, tetapi juga oleh pertimbangan kepatuhan regulasi, lokasi geografis pusat data, dan rekam jejak keandalan layanan. TikTok, misalnya, telah bermitra dengan Oracle Cloud untuk pengelolaan data pengguna di Amerika Serikat sebagai respons terhadap kekhawatiran keamanan nasional, sebuah keputusan yang mencerminkan bagaimana faktor geopolitik semakin mempengaruhi lanskap keamanan cloud global (Pandu et al., 2024). Organisasi Indonesia perlu mempertimbangkan faktor serupa, termasuk kesesuaian dengan persyaratan UU PDP, ketika mengevaluasi dan memilih penyedia layanan cloud.

Kerangka Manajemen Risiko Keamanan Cloud yang Terintegrasi

Berdasarkan sintesis temuan dari seluruh literatur yang dikaji, penelitian ini mengusulkan sebuah kerangka manajemen risiko keamanan cloud yang terintegrasi dengan lima komponen utama. Komponen pertama adalah identifikasi dan penilaian risiko (risk identification and assessment), yang mencakup inventarisasi aset data, pemetaan aliran data (data flow mapping), dan penilaian risiko berbasis ancaman (threat-based risk assessment). Tahap ini menjadi fondasi dari seluruh program keamanan, karena organisasi tidak dapat melindungi apa yang tidak mereka ketahui keberadaannya.

Komponen kedua adalah implementasi kontrol teknis berlapis (layered technical controls), yang mencakup enkripsi data at-rest dan in-transit, kontrol akses berbasis identitas dan peran, segmentasi jaringan, serta pemantauan ancaman secara real-time. Prinsip defense in depth mengajarkan bahwa tidak ada kontrol keamanan tunggal yang sempurna, sehingga implementasi berlapis memastikan bahwa kegagalan satu lapisan tidak serta-merta mengakibatkan kompromi total terhadap sistem (Ilyasa, 2021).

Komponen ketiga adalah tata kelola dan kepatuhan (governance and compliance), yang mencakup kebijakan keamanan informasi yang terdokumentasi, program kesadaran keamanan bagi seluruh personel, audit keamanan berkala, dan mekanisme pelaporan insiden yang jelas. Aspek tata kelola ini seringkali mendapat perhatian yang kurang memadai dibandingkan kontrol teknis, padahal banyak insiden keamanan yang berakar pada kegagalan proses dan manusia, bukan pada kelemahan teknologi semata.

Komponen keempat adalah kesiapsiagaan dan pemulihan insiden (incident readiness and recovery), yang meliputi rencana respons insiden yang telah diuji secara rutin, prosedur backup dan pemulihan data yang terverifikasi, serta mekanisme komunikasi krisis yang jelas. Rifany et al. (2023) menekankan bahwa waktu respons terhadap insiden keamanan merupakan faktor kritis dalam membatasi dampak kebocoran data, setiap jam keterlambatan deteksi dan respons berpotensi meningkatkan jumlah data yang terekspos secara eksponensial.

Komponen kelima adalah peningkatan berkelanjutan (continuous improvement), yang mencakup pemantauan tren ancaman terkini, evaluasi efektivitas kontrol yang telah diimplementasikan, dan adaptasi terhadap perubahan lingkungan teknologi dan regulasi. Keamanan cloud bukan merupakan destinasi akhir, melainkan sebuah perjalanan berkelanjutan yang menuntut komitmen jangka panjang dari seluruh organisasi. Dalam kerangka ini, kolaborasi antara tim keamanan internal, penyedia layanan cloud, dan komunitas riset keamanan menjadi instrumen

esensial yang memungkinkan organisasi tetap selangkah di depan para pelaku ancaman yang terus berinovasi (Pandu et al., 2024).

SIMPULAN

Kesimpulan

Penelitian ini berhasil memetakan enam kategori risiko utama keamanan data pribadi pada sistem cloud computing: kebocoran data, akses tidak sah, serangan DoS/DDoS, snooping dan analisis trafik, penyalahgunaan sumber daya multi-tenancy, serta kehilangan data permanen. Masing-masing risiko memiliki karakteristik, vektor serangan, dan dampak yang berbeda, sehingga memerlukan pendekatan mitigasi yang spesifik dan berlapis.

Analisis mekanisme keamanan menunjukkan bahwa enkripsi data tingkat lanjut (AES-256, TLS 1.3) merupakan kontrol keamanan paling efektif dengan tingkat keberhasilan hingga 97% dalam mencegah eksploitasi data. Dikombinasikan dengan role-based access control, autentikasi multi-faktor, dan pemantauan real-time berbasis AI, implementasi berlapis ini membentuk arsitektur pertahanan yang kokoh terhadap berbagai vektor ancaman.

Temuan penting lainnya adalah bahwa kolaborasi antara penyedia layanan cloud dan pengguna terbukti menurunkan insiden keamanan hingga 30%. Hal ini menegaskan bahwa keamanan cloud bukan semata-mata persoalan teknis, melainkan juga persoalan tata kelola, kebijakan, dan kemitraan yang terstruktur. Di sisi lain, kesenjangan yang signifikan ditemukan antara kapabilitas keamanan platform besar dengan UMKM yang adopsi digitalnya tidak diimbangi dengan peningkatan kesadaran dan kapabilitas keamanan informasi.

Saran

Berdasarkan temuan penelitian, beberapa rekomendasi diajukan sebagai berikut. Pertama, organisasi yang mengadopsi cloud computing hendaknya menerapkan prinsip defense in depth dengan mengintegrasikan setidaknya tiga lapisan keamanan: enkripsi, kontrol akses berbasis peran, dan pemantauan real-time. Implementasi berlapis ini memastikan bahwa kegagalan satu mekanisme tidak mengakibatkan kompromi total terhadap keamanan data.

Kedua, pemerintah perlu mendorong program literasi keamanan digital yang menyasar pelaku UMKM, mengingat besarnya populasi usaha ini dan keterbatasan kapabilitas keamanan yang mereka miliki. Program ini idealnya diintegrasikan ke dalam ekosistem pembinaan UMKM yang sudah ada, seperti program digitalisasi UMKM yang diselenggarakan oleh Kementerian Koperasi

dan UKM, dengan menambahkan modul keamanan siber dasar yang praktis dan mudah diterapkan.

Ketiga, penelitian lanjutan disarankan untuk mengembangkan model penilaian risiko keamanan cloud yang terstandarisasi dan dapat diadaptasi oleh organisasi dari berbagai skala. Model tersebut idealnya mempertimbangkan konteks spesifik Indonesia, termasuk infrastruktur internet yang heterogen, tingkat literasi digital yang bervariasi, dan kerangka regulasi UU PDP yang masih dalam tahap implementasi awal.

Keempat, eksplorasi implementasi Zero Trust Architecture dan quantum encryption dalam konteks keamanan cloud Indonesia perlu segera dimulai. Meskipun kedua teknologi ini masih relatif baru, keterlambatan dalam adopsi akan semakin memperlebar kesenjangan kapabilitas keamanan antara Indonesia dengan negara-negara yang lebih maju secara digital. Kolaborasi antara lembaga riset, perguruan tinggi, dan industri TI dalam mengkaji dan mengujicobakan teknologi-teknologi ini di lingkungan yang terkontrol merupakan langkah awal yang strategis.

Kelima, pengembangan standar keamanan cloud nasional yang selaras dengan kerangka internasional (ISO 27001, NIST CSF) namun mempertimbangkan konteks dan kapabilitas lokal menjadi kebutuhan mendesak. Standar semacam ini akan menjadi referensi bersama bagi penyedia layanan, pengguna korporat, dan regulator dalam membangun ekosistem cloud yang aman, terpercaya, dan sejalan dengan kepentingan nasional dalam tata kelola data digital.

DAFTAR PUSTAKA

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in Cloud Computing: Opportunities and Challenges. *Information Sciences*, 305, 357–383.

Almorsy, M., Grundy, J., & Müller, I. (2016). An Analysis of the Cloud Computing Security Problem. *arXiv preprint arXiv:1609.01107*.

Anggraini, D., & Bisma, R. (2021). Perencanaan Tata Kelola Keamanan Informasi dalam Penerapan Cloud Computing Menggunakan ISO 27001:2013 pada PT. SPINDO, Tbk. *Journal of Informatics and Computer Science*, 3.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., & Zaharia, M. (2010). A View of Cloud Computing. *Communications of the ACM*, 53(4), 50–58.

Aulia, R., & Batubara, C. (2023). Penerapan Strategi Syariah dalam Meningkatkan Digital Marketing pada Usaha Kecil Menengah di Indonesia. *Ekonomi Bisnis Manajemen dan Akuntansi (EBMA)*, 4(1), 1759–1766.

Fauziah, Y. (2014). Tinjauan Keamanan Sistem pada Teknologi Cloud Computing. *Jurnal*

Informatika, Universitas Ahmad Dahlan.

Gartner. (2023). Top Trends in Cloud Security. *Gartner Research Reports*.

Herlawati, et al. (2018). Security Issues in Cloud Computing Systems. *Jurnal Informatika UBHARA Jaya*.

Ilyasa, N. D. (2021). Keamanan dan Privasi pada Cloud Computing sebagai Tempat Penyimpanan Data Masa Kini. Program Studi Teknik Informatika, Universitas Komputer Indonesia Bandung.

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity. *U.S. Department of Commerce*.

Pandu, R. M., Widodo, D. S. A., & Muttaqin, H. A. (2024). Manajemen Keamanan Data dalam Era Transformasi Digital dan Cloud Computing. *Journal of Information and Information Security (JIFORTY)*, 5(2), 145–154.

Rifany, R., Prakoso, M. D., & Laksono, P. D. (2023). Analisis Dampak Cloud Computing terhadap Keamanan Sistem dan Data. *Seminar Nasional TEKNOKA*, 8, 152–158.

Rittinghouse, J. W., & Ransome, J. F. (2016). *Cloud Computing: Implementation, Management, and Security*. CRC Press.

Rizky, D. M., Hakim, I., Fauzi, A., Setyawati, I., & Ristanto, A. (2020). Implementasi Digital Marketing pada UKM. *Jurnal Teknologi dan Manajemen Industri*, 1(2), 1–5.

Sengupta, S., Kaulgud, V., & Sharma, V. S. (2011). Cloud Computing Security: Trends and Research Directions. *Proceedings of IEEE World Congress on Services*, 524–531.

Setiawan, W. (2022). Analisa Layanan Cloud Computing di Era Digital. *Jurnal Informatika*, 1.

Sumardana, K., Sussanti, & Damayanti, V. K. (2024). Penerapan E-Commerce bagi UMKM sebagai Pemasaran Digital dalam Menghadapi Revolusi Industri 4.0. *CEMERLANG: Jurnal Manajemen dan Ekonomi Bisnis*, 4(4), 279–287.

Syastra, M. T., & Adam, S. (2017). Penggunaan Media Sosial dengan Pendekatan Model AIDA bagi Usaha Kecil dan Menengah. *Jurnal Sistem Informasi Bisnis*, 7(2), 114–119.

Ula, M. (2019). Analisis Metode Pengamanan Data pada Layanan Cloud Computing. *TECHSI – Jurnal Teknik Informatika*, 11(1), 116–125.

Utami, R., & Fauzi, A. (2023). Strategi Pemasaran Usaha Mikro, Kecil dan Menengah (UMKM) di Era Revolusi Industri 4.0. *Jurnal JAMAN*, 3(1), 90–94.