KEAMANAN INFORMASI

KEAMANAN CLOUD & SUPPLY CHAIN

Disusun oleh:

Akxel Brian Nirwana

2344390009

Program Studi Sistem Informasi

Fakultas Teknik

UNIVERSITAS PERSADA INDONESIA

2025

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, sebab atas rahmat dan karunia-Nya penulis dapat menyelesaikan penulisan makalah individu dengan judul **"Keamanan Cloud & Supply-Chain: Model Shared Responsibility, Ancaman Khusus Cloud, Mitigasi"** ini dengan baik dan tepat waktu.

Makalah ini disusun sebagai bentuk dari pemenuhan tugas mata kuliah Keamanan Informasi dan secara spesifik membahas mengenai tantangan keamanan siber di era adopsi komputasi awan yang masif. Pembahasan difokuskan pada tiga pilar utama keamanan *cloud* dan rantai pasok modern: **Model Tanggung Jawab Bersama (*Shared Responsibility Model*)** untuk mengklarifikasi batas keamanan antara penyedia dan pelanggan, identifikasi **Ancaman Khusus *Cloud*** yang muncul dari sifat dinamis dan *multi tenant* lingkungan *cloud*, serta perumusan **Strategi Mitigasi** yang berfokus pada pendekatan *Policy as Code* dan *Zero Trust*.

Penulis juga mengucapkan terima kasih yang sebesar-besarnya kepada dosen pengampu mata kuliah Keamanan Informasi, Bapak Jhonny Z.A, Ir., M.M., atas bimbingan dan arahan yang telah diberikan selama proses penyusunan makalah ini. Bimbingan beliau sangat membantu penulis dalam menyajikan pemahaman yang komprehensif mengenai pergeseran paradigma keamanan dari perimeter jaringan ke identitas dan konfigurasi, serta bagaimana perlindungan rantai pasok (*supply chain*) digital menjadi kunci utama dalam menjaga *Triad CIA* (Kerahasiaan, Integritas, dan Ketersediaan) aset digital di lingkungan *cloud*.

Akhir kata, penulis berharap semoga tulisan ini dapat memberikan pemahaman serta wawasan yang lebih baik mengenai arsitektur keamanan *cloud*, pentingnya tata kelola konfigurasi yang ketat, serta urgensi adopsi solusi *DevSecOps* dan *Zero Trust* dalam menghadapi kompleksitas keamanan *cloud* dan rantai pasok di dunia digital yang terus berkembang. Semoga makalah ini bermanfaat bagi para pembaca dan memberikan kontribusi kecil terhadap upaya membangun pertahanan *cloud* yang tangguh.

Akxel Brian Nirwana

Jakarta, 24 Oktober 2025

DAFTAR ISI

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Adopsi komputasi awan (*cloud computing*) telah menjadi strategi inti bagi transformasi digital organisasi di seluruh dunia. Fleksibilitas, skalabilitas, dan efisiensi biaya yang ditawarkan oleh layanan *cloud* publik (IaaS, PaaS, dan SaaS) mendorong migrasi aset digital yang kritikal. Namun, perpindahan ke lingkungan *cloud* juga memperkenalkan tantangan keamanan yang unik dan kompleks, berbeda secara fundamental dengan model keamanan tradisional berbasis perimeter.

Tantangan utama berakar pada tiga area yang saling berkaitan:

1. Ambiguitas Tanggung Jawab: Lingkungan cloud beroperasi di bawah Model Tanggung Jawab Bersama (*Shared Responsibility Model*), yang mendefinisikan batas antara keamanan yang menjadi tugas Penyedia Layanan *Cloud* (CSP) dan keamanan yang harus dikelola oleh Pelanggan. Kesalahpahaman atau misinterpretasi terhadap batas ini menjadi penyebab utama insiden keamanan, di mana *misconfiguration* pada sisi pelanggan menjadi vektor serangan yang dominan.
2. Evolusi Ancaman: Sifat dinamis dan *multi tenant cloud* memperbesar permukaan serangan. Ancaman seperti kelemahan pada Manajemen Identitas dan Akses (IAM), kerentanan pada *Application Programming Interfaces* (APIs), dan risiko yang timbul dari otomatisasi masif memerlukan strategi mitigasi yang lebih canggih daripada alat keamanan konvensional.
3. Ancaman Rantai Pasok (*Supply Chain*): Integrasi cloud dengan *Software Development Life Cycle* (SDLC) modern menjadikan rantai pasok perangkat lunak, termasuk *third party component* dan *pipeline* CI/CD yang di *host* di *cloud*, sebagai target serangan baru yang berpotensi memiliki dampak *cascading* yang luas. Insiden keamanan rantai pasok menunjukkan bahwa keamanan aplikasi tidak lagi hanya bergantung pada kode internal, melainkan juga pada integritas seluruh ekosistem pemasok.

Oleh karena itu, diperlukan analisis yang komprehensif mengenai kerangka kerja keamanan yang relevan, identifikasi ancaman spesifik, dan perumusan strategi mitigasi best practice yang terintegrasi (seperti *Policy as Code*, *Zero Trust*, dan *DevSecOps*) untuk memastikan aset digital terlindungi secara optimal dalam ekosistem *cloud* yang saling terhubung.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, rumusan masalah dalam makalah ini adalah sebagai berikut:

1. Bagaimana Model Tanggung Jawab Bersama (*Shared Responsibility Model*) membagi tugas keamanan antara Penyedia Layanan *Cloud* (CSP) dan Pelanggan, dan bagaimana model ini bervariasi di antara model layanan (IaaS, PaaS, dan SaaS)?
2. Apa saja ancaman keamanan yang bersifat khusus dan dominan di lingkungan komputasi awan, termasuk risiko yang berasal dari rantai pasok perangkat lunak?
3. Bagaimana strategi mitigasi dan *best practice*, seperti *Policy as Code* (PaC), *Zero Trust*, dan integrasi *DevSecOps*/SBOM, dapat diterapkan untuk mengurangi risiko dan memperkuat postur keamanan *cloud* dan rantai pasok?

1.3 Tujuan Penulisan

Tujuan penulisan makalah ini adalah untuk:

1. Menganalisis dan menjelaskan secara mendalam konsep Model Tanggung Jawab Bersama, termasuk variasi implementasinya pada model layanan IaaS, PaaS, dan SaaS, serta implikasinya terhadap kepatuhan hukum dan regulasi.
2. Mengidentifikasi dan menguraikan secara rinci ancaman-ancaman keamanan khas *cloud* yang paling sering dieksploitasi, dengan fokus khusus pada risiko yang ditimbulkan oleh *miskonfigurasi*, kelemahan IAM, *Insecure* API, dan serangan rantai pasok *cloud*.
3. Merumuskan dan mengevaluasi strategi mitigasi dan *best practice modern*, meliputi penerapan tata kelola berbasis kode (*Policy as Code*), arsitektur

Zero Trust, dan teknik DevSecOps yang didukung oleh *Software Bill of Materials* (SBOM), untuk membangun pertahanan keamanan *cloud* yang proaktif dan berkelanjutan.

BAB II

PEMBAHASAN

2.1 Model Tanggung Jawab Bersama (Shared Responsibility Model)

Model Tanggung Jawab Bersama (*Shared Responsibility Model*) adalah landasan tata kelola keamanan dalam layanan cloud, yang secara fundamental membedakan antara tanggung jawab Penyedia Layanan *Cloud* (CSP) dan Pelanggan. Kegagalan dalam memahami pembagian tugas ini merupakan pintu masuk utama bagi banyak pelanggaran keamanan di *cloud*.

2.1.1 Konsep Dasar dan Prinsip Inti

Model ini beroperasi di bawah prinsip dikotomi yang jelas: Keamanan dari *Cloud* dan Keamanan di *Cloud* (AWS, 2024).

1. Tanggung Jawab Penyedia Layanan Cloud (CSP): CSP bertanggung jawab atas Keamanan dari *Cloud*. Area tanggung jawab ini mencakup perlindungan terhadap infrastruktur global yang menjalankan layanan *cloud*, termasuk fasilitas fisik (pusat data), perangkat keras, jaringan, *storage*, dan lapisan virtualisasi (*hypervisor*). Dalam konteks ini, pelanggan melepaskan beban operasional pengelolaan infrastruktur fisik (Davenport Group, 2024).
2. Tanggung Jawab Pelanggan: Pelanggan bertanggung jawab atas Keamanan di *Cloud*. Domain ini mencakup seluruh konfigurasi yang ditempatkan atau dikelola oleh pelanggan, termasuk keamanan data (enkripsi), Manajemen Identitas dan Akses (IAM), konfigurasi *firewall* jaringan virtual, *patching* sistem operasi tamu (pada model tertentu), dan keamanan aplikasi (Orca Security, 2024).

Intinya, CSP mengamankan fondasi, sementara pelanggan mengamankan apa yang dibangun di atas fondasi tersebut.

2.1.2 Variasi Berdasarkan Model Layanan (IaaS, PaaS, SaaS)

Pembagian tanggung jawab keamanan bersifat dinamis dan bervariasi secara signifikan sesuai dengan model layanan *cloud* yang diadopsi (IaaS, PaaS, atau SaaS). Semakin tinggi tingkat abstraksi layanan, semakin besar tanggung

jawab yang diambil alih oleh CSP, dan semakin kecil domain tanggung jawab pelanggan.

- *Infrastructure as a Service* (IaaS): Pelanggan memegang tanggung jawab terluas, mencakup sistem operasi, *middleware*, aplikasi, data, dan IAM. CSP hanya bertanggung jawab atas lapisan di bawah OS (virtualisasi, server fisik, *storage*).
- *Platform as a Service* (PaaS): Tanggung jawab CSP diperluas hingga mencakup sistem operasi dan middleware atau runtime aplikasi. Pelanggan berfokus secara eksklusif pada kode aplikasi, konfigurasi data, dan IAM.
- *Software as a Service* (SaaS): Tanggung jawab pelanggan paling minimal, terbatas pada pengelolaan akses pengguna (otorisasi) dan klasifikasi data sensitif. Sebagian besar lapisan keamanan operasional dikelola oleh CSP (Davenport Group, 2024).

Pemahaman rinci tentang variasi ini adalah prasyarat untuk merancang kontrol keamanan yang efektif.

2.1.3 Implikasi Hukum dan Kepatuhan

Model Tanggung Jawab Bersama memiliki implikasi kritis terhadap kepatuhan regulasi dan potensi pertanggungjawaban hukum.

- Audit Kepatuhan: Sertifikasi kepatuhan CSP (seperti ISO 27001 atau SOC 2) hanya mencakup Keamanan dari *Cloud*. Pelanggan wajib menunjukkan bukti pelaksanaan kontrol keamanan di *cloud* mereka sendiri untuk memenuhi persyaratan regulasi sektoral (misalnya, HIPAA, GDPR, atau regulasi keuangan).
- Pertanggungjawaban (*Liability*): Dalam kasus pelanggaran data yang disebabkan oleh miskonfigurasi (tanggung jawab pelanggan), entitas pelanggan lah yang akan menghadapi sanksi denda dan tuntutan hukum. Kegagalan dalam menerapkan kontrol pelanggan, seperti kegagalan enkripsi atau kelemahan IAM, akan dikenakan pertanggungjawaban sepenuhnya kepada pelanggan, meskipun CSP telah memenuhi semua kewajiban infrastruktur mereka (Orca Security, 2024). Model ini membantu mendefinisikan mitigasi kewajiban (mitigate liability) dengan menetapkan batas akuntabilitas yang jelas.

2.2 Ancaman Khusus dalam Lingkungan *Cloud*

Lingkungan *cloud* memperkenalkan serangkaian vektor serangan yang diperkuat oleh sifat dinamis, multi-tenant, dan interkonektivitas API. Menurut laporan

ancaman terkini (SecPod, 2025; Check Point, 2025), ancaman-ancaman ini terus mendominasi insiden keamanan *cloud*.

2.2.1 *Miskonfigurasi* (Kekeliruan Konfigurasi)

Miskonfigurasi (*misconfiguration*) secara konsisten menjadi ancaman nomor satu di *cloud* dan bertanggung jawab atas sebagian besar pelanggaran data (SecPod, 2025).

- Sifat Ancaman: Kesalahan ini muncul dari pengaturan sumber daya *cloud* yang tidak disengaja terlalu permisif, yang seringkali disebabkan oleh kompleksitas antarmuka manajemen *cloud* dan *human error*.
- Vektor Eksploitasi Umum: Pengaturan *storage bucket* publik (misalnya Amazon S3 atau Azure Blob Storage) tanpa batasan akses yang tepat; kebijakan keamanan jaringan virtual yang terlalu terbuka, dan *instance* komputasi dengan *port* manajemen terekspos ke internet publik (CyCognito, 2025).

2.2.2 Manajemen Identitas dan Akses (IAM) yang Tidak Memadai

Kelemahan IAM adalah ancaman kritis karena identitas adalah perimeter keamanan baru di *cloud*.

- Hak Akses Berlebihan (*Over privileged Access*): Memberikan izin yang jauh melebihi yang diperlukan untuk suatu tugas, melanggar prinsip *Least Privilege*. Jika akun ini dikompromikan, penyerang dapat melakukan eskalasi hak istimewa (*privilege escalation*) dan lateral *movement* dengan mudah (Check Point, 2025).
- Kegagalan Autentikasi: Kurangnya penerapan Autentikasi Multifaktor (MFA) yang kuat pada akun administrator dan akun layanan kritikal, membuat akun tersebut rentan terhadap kompromi melalui *phishing* atau pencurian kredensial.

2.2.3 Ancaman *Supply Chain Cloud*

Serangan terhadap rantai pasok perangkat lunak telah menjadi vektor berprofil tinggi, di mana cloud bertindak sebagai medium penularan dan target akhir.

- Konteks Cloud Native: Ancaman ini berfokus pada eksploitasi dependensi pihak ketiga, container images yang disusupi, atau *pipeline Continuous Integration/Continuous Deployment* (CI/CD) yang di *host* di *cloud*.
- Vektor Kunci: Kompromi terhadap repositori kode atau *build server* yang berjalan di lingkungan *cloud*, memungkinkan penyisipan kode berbahaya langsung ke artefak *deployment*. Dalam pandangan

keamanan, layanan *cloud* itu sendiri merupakan pemasok penting yang memerlukan pemeriksaan risiko rantai pasok yang ketat (ISC2, 2025).

2.2.4 *Insecure Application Programming Interfaces* (APIs)

API adalah mekanisme interaksi utama baik antara layanan *cloud* itu sendiri maupun antara pelanggan dan aplikasi mereka, menjadikannya permukaan serangan yang berkembang pesat.

- Risiko Eksploitasi: Kelemahan pada API disebabkan oleh kurangnya otentikasi, otorisasi yang buruk, atau paparan data yang berlebihan (*excessive data exposure*) (SecPod, 2025).
- Contoh: *Broken Object Level Authorization* (BOLA) yang memungkinkan pengguna berinteraksi dengan sumber daya di luar domain mereka, atau kegagalan penerapan rate limiting yang memfasilitasi serangan *brute force* dan enumerasi.

2.3 Strategi Mitigasi dan *Best Practice*

Mitigasi yang efektif di cloud membutuhkan pergeseran dari pertahanan berbasis perimeter ke pertahanan yang didorong oleh policy dan identitas, yang terintegrasi secara inheren dalam siklus hidup pengembangan.

2.3.1 Tata Kelola dan *Policy as Code* (PaC)

Policy as Code (PaC) adalah mekanisme utama untuk mengatasi akar permasalahan Miskonfigurasi (2.2.1).

- Definisi dan Fungsi: PaC mengekspresikan kebijakan keamanan, tata kelola, dan kepatuhan dalam bentuk kode yang dapat dibaca mesin (misalnya, Rego, JSON, atau YAML). Kebijakan ini kemudian diterapkan secara otomatis dan konsisten melalui alat manajemen konfigurasi (SentinelOne, 2025).
- Penerapan *Shift Left*: PaC terintegrasi ke dalam *pipeline* CI/CD, memungkinkan pemeriksaan kepatuhan dilakukan sebelum sumber daya di deploy (*shift left*). Hal ini mencegah infrastruktur yang tidak aman masuk ke lingkungan produksi, menggantikan proses audit manual yang rentan terhadap kesalahan (Check Point, 2025).

2.3.2 Penguatan *IAM* dan *Zero Trust*

Implementasi arsitektur Zero Trust adalah solusi strategis untuk mengatasi Kelemahan IAM (2.2.2).

- Prinsip *Zero Trust*: Model ini didasarkan pada asumsi bahwa tidak ada pengguna, perangkat, atau layanan yang secara inheren dapat dipercaya, baik di dalam maupun di luar perimeter jaringan tradisional. Verifikasi harus dilakukan secara berkelanjutan (*continuous verification*) (CyberArk, 2025).
- Akses J*ust in Time* (JIT): Untuk memperkuat prinsip Least Privilege, *JIT Access* memberikan hak istimewa tinggi hanya ketika benar-benar diperlukan dan untuk durasi waktu yang sangat terbatas. Setelah tugas selesai atau batas waktu tercapai, izin dicabut secara otomatis. Pendekatan ini secara drastis mengurangi *standing privileges*, yang merupakan target utama penyerang (Cloudanix, 2025).

2.3.3 Keamanan Rantai Pasok Terintegrasi

Mitigasi terhadap Ancaman *Supply Chain Cloud* (2.2.3) memerlukan integrasi keamanan ke dalam siklus pengembangan perangkat lunak secara keseluruhan, dikenal sebagai *DevSecOps*.

- *DevSecOps*: Ini adalah budaya dan praktik yang mengotomatisasi pengujian keamanan di setiap tahap *pipeline* CI/CD. Ini termasuk pemindaian kerentanan *image container* dan pemindaian *dependency* kode aplikasi.
- *Software Bill of Materials* (SBOM): SBOM adalah daftar formal dan rinci dari komponen, lisensi, dan dependensi *open source* maupun komersial yang membentuk suatu perangkat lunak. SBOM (bersama dengan tooling *DevSecOps*) memberikan visibilitas penuh ke dalam rantai pasok, memungkinkan organisasi untuk dengan cepat mengidentifikasi dan menambal kerentanan (misalnya, kasus Log4j) di komponen pihak ketiga (Oteemo, 2025).

2.3.4 Enkripsi dan Kontrol Data

Strategi ini memastikan kerahasiaan data sensitif, bahkan jika terjadi cloud breach yang tidak dapat dicegah.

- Enkripsi Wajib: Penerapan enkripsi harus dilakukan pada data saat diam (*at rest*) (menggunakan AES-256 pada storage dan database) dan data saat bergerak (*in transit*) (menggunakan TLS/SSL wajib) (CloudOptimo, 2025).
- Kontrol Kunci Enkripsi: Pelanggan disarankan untuk menggunakan layanan *Key Management Service* (KMS) milik CSP (misalnya, AWS KMS, Azure Key Vault) atau menerapkan strategi *Bring Your Own Key* (BYOK). Kontrol kunci yang kuat, termasuk rotasi kunci secara teratur dan pemisahan tugas antara pengelola kunci dan pengguna data, adalah fundamental untuk memastikan bahwa bahkan CSP tidak dapat mengakses data sensitif tanpa izin (CrowdStrike, 2025).

BAB III

PENUTUP

3.1 Kesimpulan

Makalah ini menyimpulkan bahwa keamanan dalam lingkungan *cloud* modern dan rantai pasok digital tidak lagi dapat dipertahankan menggunakan model tradisional. Keberhasilan pertahanan bergantung pada pemahaman yang utuh dan pelaksanaan yang ketat terhadap Model Tanggung Jawab Bersama (*Shared Responsibility Model*), yang menempatkan tanggung jawab konfigurasi, data, dan identitas sepenuhnya pada pihak pelanggan. Ancaman utama, yang didominasi oleh *miskonfigurasi*, kelemahan Manajemen Identitas dan Akses (IAM), dan kerentanan pada API, diperburuk oleh risiko *supply chain* yang muncul dari ketergantungan pada komponen pihak ketiga.

Oleh karena itu, mitigasi yang efektif harus didasarkan pada otomatisasi dan verifikasi berkelanjutan. Strategi *Policy as Code* (PaC) terbukti esensial untuk mencegah *miskonfigurasi* sejak fase *deployment*, sementara arsitektur *Zero Trust* dan implementasi akses *Just in Time* (JIT) menjadi kunci untuk mengatasi kelemahan IAM. Lebih lanjut, perlindungan terhadap rantai pasok *(supply chain*) harus diintegrasikan melalui pendekatan DevSecOps yang didukung oleh *Software Bill of Materials* (SBOM), guna menjamin visibilitas penuh dan integritas kode dari pengembangan hingga produksi. Keseluruhan strategi ini menegaskan bahwa keamanan cloud adalah upaya kolaboratif yang memerlukan tata kelola proaktif, bukan hanya solusi reaktif.

3.2 Saran

Berdasarkan temuan dan analisis dalam makalah ini, terdapat beberapa saran yang direkomendasikan untuk memperkuat postur keamanan *cloud* dan rantai pasok:

1. **Penguatan Tata Kelola (*Governance*) melalui Otomatisasi**: Organisasi disarankan untuk berinvestasi secara signifikan dalam *implementasi Policy as Code* (PaC) dan *Cloud Security Posture Management* (CSPM) untuk mengotomatisasi pemantauan dan penegakan kebijakan konfigurasi. Pendekatan ini adalah cara paling efektif untuk memitigasi risiko

miskonfigurasi, yang merupakan ancaman utama yang berada dalam domain tanggung jawab pelanggan.

2. **Transisi Penuh ke *Zero Trust* dan JIT *Access***: Organisasi harus secara bertahap menghapus hak akses permanen (*standing privileges*) dan bertransisi menuju kerangka kerja *Zero Trust* dengan mengimplementasikan akses *Just in Time* (JIT). Strategi ini memastikan bahwa semua identitas (manusia maupun mesin) hanya mendapatkan izin yang paling minim (*least privilege*) dan hanya untuk durasi waktu yang dibutuhkan, sehingga secara drastis mengurangi permukaan serangan yang diakibatkan oleh kompromi kredensial.
3. **Adopsi Wajib *Software Bill of Materials* (SBOM)**: Dalam konteks keamanan rantai pasok, disarankan agar adopsi SBOM menjadi persyaratan wajib dalam *pipeline DevSecOps*. SBOM harus digunakan untuk pemindaian kerentanan yang berkelanjutan dan untuk memverifikasi integritas komponen perangkat lunak pihak ketiga, memungkinkan respons cepat dan tepat sasaran terhadap kerentanan baru yang terungkap di komponen *supply chain* eksternal.

DAFTAR PUSTAKA

Community. (2025, July 15). *Shared Security Responsibility Model*. Retrieved from Alibaba cloud: https://www.alibabacloud.com/help/en/well-architected/latest/security-responsibility-model

Editor. (2025, october 09). *Cloud Supply Chain Attacks: A Comprehensive Security Guide*. Retrieved from Startup defense: https://www.startupdefense.io/cyberattacks/cloud-supply-chain-attack

Editor. (2025, 30 July). *Cloud Supply Chain Security*. Retrieved from isc2: https://www.isc2.org/Insights/2025/07/Cloud-Supply-Chain-Security

Editor. (2025, October 27). *Most Common Cloud Security Threats*. Retrieved from Darktrace: https://www.darktrace.com/cyber-ai-glossary/the-most-common-cloud-security-threats

Editor. (2025, April 28). *Top Threats to Cloud Computing - Deep Dive 2025*. Retrieved from Cloud security alliance: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2025

Editorial. (2024, January 25). *What is the Shared Responsibility Model in the Cloud?* Retrieved from Cloud security alliance: https://cloudsecurityalliance.org/blog/2024/01/25/what-is-the-shared-responsibility-model-in-the-cloud

Editorial. (2025, October 17). *Shared Responsibility Model*. Retrieved from AWS cloud security: https://aws.amazon.com/compliance/shared-responsibility-model/

Katz, E. (2024, December 25). *8 Steps to Mitigate Supply Chain Risk in Cybersecurity*. Retrieved from Spectra lops: https://spectralops.io/blog/steps-to-mitigate-supply-chain-risk-in-cybersecurity/

Shared responsibility in the cloud. (09/29/2024, September 29). Retrieved from Microsoft ignite: https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility