

# Dasar Dasar **CLOUD COMPUTING & SISTEM INFORMASI**

Mila Jumarlis, Indah Purnama Sari, Heru Saputra, Suhardi Aras  
Sitti Suhada, Andi Ikmal Rachman, Adam M Tanniewa  
Defiariany, Bayu Waseso, Mirfan  
Muharman Lubis, Janner Simarmata



Dasar Dasar  
**CLOUD COMPUTING  
& SISTEM INFORMASI**

## UU 28 tahun 2014 tentang Hak Cipta

### Fungsi dan sifat hak cipta Pasal 4

Hak Cipta sebagaimana dimaksud dalam Pasal 3 huruf a merupakan hak eksklusif yang terdiri atas hak moral dan hak ekonomi.

### Pembatasan Perlindungan Pasal 26

Ketentuan sebagaimana dimaksud dalam Pasal 23, Pasal 24, dan Pasal 25 tidak berlaku terhadap:

- a. penggunaan kutipan singkat Ciptaan dan/atau produk Hak Terkait untuk pelaporan peristiwa aktual yang ditujukan hanya untuk keperluan penyediaan informasi aktual;
- b. Penggandaan Ciptaan dan/atau produk Hak Terkait hanya untuk kepentingan penelitian ilmu pengetahuan;
- c. Penggandaan Ciptaan dan/atau produk Hak Terkait hanya untuk keperluan pengajaran, kecuali pertunjukan dan Fonogram yang telah dilakukan Pengumuman sebagai bahan ajar; dan
- d. penggunaan untuk kepentingan pendidikan dan pengembangan ilmu pengetahuan yang memungkinkan suatu Ciptaan dan/atau produk Hak Terkait dapat digunakan tanpa izin Pelaku Pertunjukan, Produser Fonogram, atau Lembaga Penyiaran.

### Sanksi Pelanggaran Pasal 113

1. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah).
2. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf a, huruf b, huruf e, dan/atau huruf g untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

# **Dasar-dasar Cloud Computing dan Sistem Informasi**

Mila Jumarlis, Indah Purnama Sari, Heru Saputra, Suhardi Aras  
Sitti Suhada, Andi Ikmal Rachman, Adam M Tanniewa  
Defiariany, Bayu Waseso, Mirfan  
Muharman Lubis, Janner Simarmata



Penerbit Yayasan Kita Menulis

# Dasar-dasar Cloud Computing dan Sistem Informasi

Copyright © Yayasan Kita Menulis, 2025

Penulis:

Mila Jumarlis, Indah Purnama Sari, Heru Saputra, Suhardi Aras  
Sitti Suhada, Andi Ikmal Rachman, Adam M Tanniewa  
Defiariany, Bayu Waseso, Mirfan  
Muharman Lubis, Janner Simarmata

Editor: Iko Mart Nadeak

Desain Sampul: Devy Dian Pratama, S.Kom.

Penerbit

Yayasan Kita Menulis

Web: [kitamenulis.id](http://kitamenulis.id)

e-mail: [press@kitamenulis.id](mailto:press@kitamenulis.id)

WA: 0813-9680-7167

IKAPI: 044/SUT/2021

Mila Jumarlis., dkk.

Dasar-dasar Cloud Computing dan Sistem Informasi

Yayasan Kita Menulis, 2025

xvi; 222 hlm; 16 x 23 cm

ISBN: 978-623-113-819-4

Cetakan 1, April 2025

- I. Dasar-dasar Cloud Computing dan Sistem Informasi
- II. Yayasan Kita Menulis

## Katalog Dalam Terbitan

Hak cipta dilindungi undang-undang

Dilarang memperbanyak maupun mengedarkan buku tanpa izin tertulis dari penerbit maupun penulis

# Kata Pengantar

Puji syukur kita panjatkan ke hadirat Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya, sehingga buku yang berjudul “Dasar-dasar Cloud Computing dan Sistem Informasi” ini dapat disusun dan diselesaikan dengan baik. Buku ini hadir sebagai bentuk kontribusi dalam memperkaya literatur di bidang teknologi informasi, khususnya mengenai konsep dasar dan penerapan cloud computing serta keterkaitannya dengan sistem informasi modern.

Seiring dengan perkembangan teknologi yang begitu pesat, kebutuhan akan layanan komputasi awan (cloud computing) menjadi semakin mendesak, baik di sektor bisnis, pemerintahan, maupun pendidikan. Melalui buku ini, pembaca akan dibimbing untuk memahami fondasi dasar cloud computing, mulai dari karakteristik, model layanan, jenis-jenis cloud, hingga arsitektur dan isu-isu keamanan yang melekat di dalamnya. Tak hanya itu, buku ini juga mengulas berbagai aspek penting seperti virtualisasi, manajemen sumber daya, serta penerapannya dalam sistem informasi dan dunia pendidikan.

Buku ini membahas:

- Bab 1 Dasar-Dasar Cloud Computing
- Bab 2 Karakteristik Cloud Computing
- Bab 3 Model Layanan Cloud Computing
- Bab 4 Jenis – Jenis Cloud Computing
- Bab 5 Arsitektur Cloud Computing
- Bab 6 Keamanan dalam Cloud Computing
- Bab 7 Keuntungan dan Kerugian Cloud Computing
- Bab 8 Virtualisasi dan Penggunaan Cloud
- Bab 9 Manajemen Proyek Sistem Informasi Berbasis Cloud
- Bab 10 Cloud Computing Dalam Pendidikan
- Bab 11 Tantangan dalam Penggunaan Cloud Computing
- Bab 12 Tren Masa Depan Cloud Computing

Kami menyadari bahwa buku ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang membangun sangat kami harapkan untuk penyempurnaan di edisi selanjutnya. Akhir kata, semoga buku ini bermanfaat dan menjadi referensi yang berguna dalam pengembangan ilmu pengetahuan di bidang teknologi informasi.

Selamat membaca!

Penulis,  
April 2025

# Daftar Isi

Kata Pengantar .....	v
Daftar Isi .....	vii
Daftar Gambar .....	xiii
Daftar Tabel .....	xv

## **Bab 1 Dasar-Dasar Cloud Computing**

1.1 Pengertian Cloud Computing .....	1
1.2 Karakteristik Cloud Computing .....	3
1.3 Model Layanan Cloud Computing .....	5
1.4 Manfaat Cloud Computing .....	6

## **Bab 2 Karakteristik Cloud Computing**

2.1 Cloud Computing .....	9
2.2 Karakteristik Cloud Computing .....	11
2.3 Jenis Layanan Cloud Computing .....	18
2.4 Deployment Model Layanan Cloud Computing .....	20

## **Bab 3 Model Layanan Cloud Computing**

3.1 Model Layanan Cloud Computing .....	23
3.1.1 Infrastructure as a Service (IaaS) .....	24
3.1.2 Platform as a Service (PaaS) .....	27
3.1.3 Software as a Service (SaaS) .....	30
3.2 Keamanan dalam Cloud Computing .....	34
3.2.1 Ancaman Keamanan pada Cloud Computing .....	34
3.2.2 Strategi dan Solusi Keamanan Cloud .....	35
3.2.3 Regulasi dan Kepatuhan Cloud Computing .....	36
3.4 Masa Depan Cloud Computing .....	37
3.4.1 Teknologi Baru dalam Cloud Computing .....	37
3.4.2 Masa Depan Cloud Computing .....	37
3.4.3 Cloud Computing dan Transformasi Digital .....	38

**Bab 4 Jenis – Jenis Cloud Computing**

4.1 Public Cloud .....	41
4.1.1 Karakteristik Public Cloud.....	42
4.1.2 Keuntungan Penggunaan Public Cloud .....	43
4.1.3 Tantangan Penggunaan Public Cloud .....	44
4.1.4 Infrastruktur Perangkat Keras .....	44
4.2 Private Cloud .....	49
4.2.1 Keuntungan dan Kelemahan .....	51
4.2.2 Infrastruktur Perangkat Keras dan Software .....	52
4.2.3 Contoh Penggunaan Private Cloud .....	54
4.3 Hybrid Cloud .....	56
4.3.1 Contoh Penerapan Hybrid Cloud .....	57
4.3.2 Keuntungan yang Diperoleh.....	58
4.3.3 Tantangan Penggunaan Private Cloud dalam Hybrid Cloud .....	58
4.4 Community Cloud.....	59
4.4.1 Karakteristik Community Cloud .....	59
4.4.2 Alasan Pemilihan Penggunaan Community Cloud .....	60
4.4.3 Keuntungan Penggunaan Community Cloud.....	61
4.4.4 Tantangan dalam Penggunaan Community Cloud .....	62

**Bab 5 Arsitektur Cloud Computing**

5.1 Pendahuluan .....	63
5.2 Infrastruktur Konvensional .....	64
5.3 Lapisan Arsitektur Cloud .....	65
5.4 Cara Kerja Arsitektur Cloud .....	68
5.5 Fungsi Arsitektur Cloud Computing.....	70
5.6 Prinsip Desain Arsitektur Cloud .....	72
5.7 Cloud Computing Life Cycle .....	73
5.8 Referensi Arsitektur Cloud Computing .....	75
5.9 Load Balancing .....	76

**Bab 6 Keamanan dalam Cloud Computing**

6.1 Pendahuluan.....	79
6.2 Konsep Dasar Cloud Computing .....	81
6.2.1 Definisi Cloud Computing.....	81
6.2.2 Karakteristik Utama Cloud Computing .....	82
6.2.3 Model Layanan Cloud Computing.....	83
6.3 Jenis Ancaman Keamanan dalam Cloud Computing .....	84
6.4 Jenis-Jenis Keamanan dalam Cloud Computing.....	86

6.5 Teknologi Keamanan Cloud.....	88
6.6 Strategi Implementasi Keamanan dalam Cloud Computing.....	89
6.7 Tren dan Perkembangan Teknologi Keamanan Cloud Computing .....	92

## **Bab 7 Keuntungan dan Kerugian Cloud Computing**

7.1 Pendahuluan.....	95
7.2 Keuntungan Cloud Computing .....	96
7.2.1 Efisiensi Biaya .....	96
7.2.2 Skalabilitas dan Fleksibilitas.....	97
7.2.3 Aksesibilitas Global.....	98
7.2.4 Pemulihan Bencana dan Backup Otomatis .....	99
7.2.5 Infrastruktur yang Dikelola Pihak Ketiga .....	100
7.3 Kerugian Cloud Computing .....	101
7.3.1 Ketergantungan pada Koneksi Internet.....	101
7.3.2 Risiko Keamanan dan Privasi.....	102
7.3.3 Downtime dan Ketergantungan pada Vendor .....	104
7.3.4 Biaya Jangka Panjang Bisa Membengkak.....	105
7.3.5 Isu Kepatuhan dan Lokasi Data.....	106
7.4 Analisis Singkat .....	107
7.4.1 Kapan Cocok Menggunakan Cloud.....	110
7.4.2 Namun, Cloud Belum Ideal Digunakan Jika.....	112

## **Bab 8 Virtualisasi dan Penggunaan Cloud**

8.1 Definisi Virtualisasi.....	113
8.2 Virtualisasi di Cloud Computing.....	114
8.3 Konsep Virtualisasi .....	115
8.4 Jenis-jenis Virtualisasi didalam Cloud Computing.....	116
8.5 Perbedaan antara Virtualisasi dan Cloud Computing .....	118
8.6 Cara Kerja Virtualisasi di Cloud Computing .....	118
8.7 Karakteristik Virtualisasi di Cloud Computing .....	119
8.8 Tipe Virtualisasi .....	120
8.9 Manfaat Virtualisasi dan Cloud Computing.....	121
8.10 Sumber Daya Yang Dapat Divirtualisasi .....	123
8.11 Keuntungan dari Virtualisasi .....	126
8.12 Kerugian dari Virtualisasi .....	128
8.13 Dari Virtualisasi Ke Cloud Computing .....	130

**Bab 9 Manajemen Proyek Sistem Informasi Berbasis Cloud**

9.1 Pengantar Manajemen Proyek Sistem Informasi .....	133
9.1.1 Definisi Manajemen Proyek dalam Konteks Sistem Informasi.....	133
9.1.2 Peran Penting Manajemen Proyek dalam Keberhasilan Sistem Informasi .....	134
9.1.3 Perbedaan Manajemen Proyek Tradisional vs Berbasis Cloud .....	135
9.2 Ruang Lingkup Proyek Sistem Informasi Berbasis Cloud.....	136
9.2.1 Jenis-jenis Proyek SI yang Umum Berbasis Cloud .....	136
9.2.2 Kebutuhan dan Tantangan Unik dalam Proyek Cloud.....	138
9.3 Siklus Hidup Proyek Cloud .....	139
9.4 Metodologi dan Kerangka Kerja dalam Proyek Cloud .....	143
9.4.1 Agile dalam Proyek Cloud.....	143
9.4.2 DevOps dalam Proyek Cloud.....	144
9.4.3 Pendekatan Hybrid dalam Proyek Cloud.....	144
9.5 Perencanaan Proyek Sistem Informasi Cloud .....	145
9.5.1 Identifikasi Kebutuhan Cloud dan Pemilihan Vendor.....	146
9.5.2 Estimasi Biaya, Waktu, dan Sumber Daya.....	147
9.5.3 Penentuan Parameter Keberhasilan Proyek Cloud .....	147
9.6 Pengelolaan Risiko dalam Proyek Cloud .....	148
9.6.1 Risiko Umum dalam Proyek Cloud.....	149
9.6.2 Strategi Mitigasi Risiko.....	150
9.7 Pemantauan dan Evaluasi Proyek Cloud .....	151
9.7.1 Indikator Kinerja Utama (KPI) dan Service Level Agreement (SLA)	152
9.7.2 Tools Monitoring dan Pengelolaan Proyek Berbasis Cloud .....	153

**Bab 10 Cloud Computing Dalam Pendidikan**

9.1 Manfaat Cloud Computing dalam Dunia Pendidikan .....	155
9.2 Implementasi Cloud Computing dalam Pendidikan di Indonesia .....	162

**Bab 11 Tantangan dalam Penggunaan Cloud Computing**

11.1 Ketergantungan pada Penyedia Layanan Cloud .....	165
11.2 Latensi Jaringan dan Keandalan.....	167
11.3 Pengelolaan Identitas dan Akses .....	169
11.4 Migrasi Data .....	172
11.5 Skalabilitas dan Kapasitas.....	174
11.6 Manajemen Versi Layanan.....	178

---

**Bab 12 Tren Masa Depan Cloud Computing**

12.1 Edge Computing dan Cloud Hybrid .....	181
12.2 Kecerdasan Buatan (AI) dan Pembelajaran Mesin (Machine Learning) di Cloud.....	183
12.3 Keamanan dan Privasi Data yang Lebih Baik.....	184
12.4 Cloud-Native dan Microservices.....	186
12.5 5G dan Cloud.....	187
12.6 Cloud untuk Industri Spesifik.....	190
12.7 Sustainability dan Green Cloud.....	191
Daftar Pustaka .....	195
Biodata Penulis .....	215



# Daftar Gambar

Gambar 1.1: Konsep Dasar Cloud Computing.....	2
Gambar 1.2: Layanan Cloud.....	4
Gambar 1.3: Manfaat Utama Cloud Computing.....	7
Gambar 2.1: Konseptual Komputasi Awan.....	10
Gambar 2.2: Konseptual Karakteristik Komputasi Awan.....	18
Gambar 6.1: Karakteristik Utama Cloud Computing .....	82
Gambar 6.2: Model Layanan Cloud Computing.....	83
Gambar 7.1: Grafik perbandingan keuntungan vs kerugian Cloud Computing.....	110
Gambar 9.1: Triple Constraint .....	135
Gambar 9.2: Tahapan Proyek .....	140
Gambar 10.1: Kelas Online Berbasis Cloud Computing.....	158
Gambar 10.2: Metode Pembelajaran Modern .....	160
Gambar 11.1: Metode Horse Red Runge Kutta .....	166
Gambar 11.2: Pay-As-You-Go Model .....	175



# Daftar Tabel

Tabel 7.1: Tabel perbandingan keuntungan vs kerugian Cloud Computing .....	109
Tabel 9.1: Proyek Tradisional vs Proyek Berbasis Cloud .....	135
Tabel 9.2: Kesesuaian Metodologi dengan Jenis Layanan Cloud .....	145
Tabel 9.3: Parameter Keberhasilan Proyek Cloud .....	147
Tabel 9.4: Kategori KPI .....	152



# Bab 1

## Dasar-Dasar Cloud Computing

### 1.1 Pengertian Cloud Computing

Cloud Computing atau komputasi awan adalah teknologi yang memungkinkan pengguna untuk mengakses dan menyimpan data serta aplikasi melalui internet, tanpa memerlukan infrastruktur fisik secara langsung. Dengan kata lain, data dan aplikasi disimpan di server virtual yang dapat diakses kapan saja dan dari mana saja selama terhubung ke internet. Hal ini memberikan fleksibilitas dan efisiensi dalam pengelolaan sumber daya komputasi.

Dalam penerapannya, data dan aplikasi disimpan pada server virtual yang tersebar di berbagai lokasi pusat data. Server ini dikelola oleh penyedia layanan cloud yang bertanggung jawab atas operasional, pemeliharaan, dan keamanannya. Pengguna cukup terhubung dengan internet untuk dapat mengakses berbagai layanan tersebut, baik melalui komputer, laptop, maupun perangkat mobile.

Konsep dasar dari cloud computing adalah mengubah infrastruktur IT menjadi layanan berbasis permintaan (on-demand), di mana pengguna hanya menggunakan sumber daya sesuai kebutuhan. Model ini serupa dengan penggunaan listrik, air, atau layanan publik lainnya yang dibayar berdasarkan konsumsi. Pendekatan ini membuat perusahaan lebih hemat biaya, karena tidak perlu lagi berinvestasi besar untuk membangun dan memelihara sistem IT sendiri.

Keunggulan utama dari cloud computing adalah fleksibilitas, skalabilitas, dan efisiensi yang diberikannya. Organisasi dapat dengan mudah meningkatkan atau menurunkan kapasitas sumber daya sesuai permintaan bisnis tanpa harus melakukan perubahan besar pada infrastruktur. Oleh karena itu, cloud computing telah menjadi pilihan strategis dalam transformasi digital, baik untuk skala individu, startup, hingga perusahaan besar.



**Gambar 1.1:** Konsep Dasar Cloud Computing

Gambar di atas merupakan infografis bergaya flat design yang menggambarkan konsep dasar Cloud Computing. Di tengah gambar terdapat ikon awan berwarna biru bertuliskan "CLOUD COMPUTING". Awan tersebut terhubung dengan beberapa perangkat digital seperti laptop, smartphone, tablet, dan desktop komputer melalui garis-garis titik, yang melambangkan konektivitas melalui internet. Di atas awan, terdapat ikon

panah naik dan turun yang menunjukkan proses upload dan download data dari dan ke cloud.

## 1.2 Karakteristik Cloud Computing

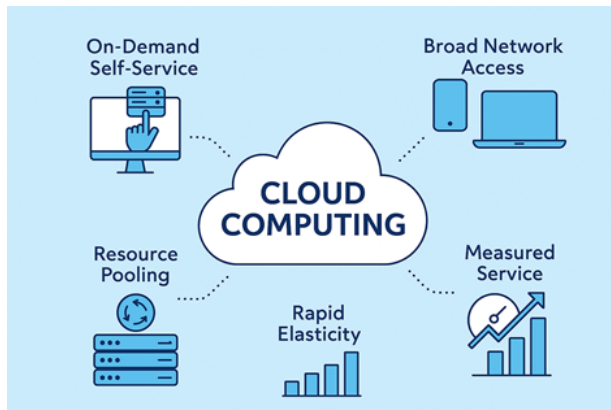
Cloud Computing memiliki sejumlah karakteristik utama yang menjadi fondasi dari fleksibilitas dan efisiensi teknologi ini. Salah satu yang paling menonjol adalah on-demand self-service, yaitu kemampuan pengguna untuk secara mandiri mengakses dan mengelola sumber daya komputasi sesuai kebutuhan. Pengguna dapat mengatur layanan seperti server, penyimpanan data, atau kapasitas jaringan tanpa harus berinteraksi langsung dengan penyedia layanan. Hal ini mempercepat proses penyediaan layanan dan mengurangi ketergantungan pada tim teknis penyedia.

Karakteristik berikutnya adalah broad network access, yang memungkinkan akses layanan cloud melalui jaringan internet dari berbagai jenis perangkat, seperti smartphone, tablet, laptop, hingga komputer desktop. Aksesibilitas yang luas ini mendukung mobilitas kerja dan kolaborasi secara daring, sehingga pengguna dapat terhubung dengan data atau aplikasi dari mana saja dan kapan saja. Ini menjadi sangat penting dalam era kerja jarak jauh dan mobilitas tinggi seperti saat ini.

Selain itu, cloud computing menerapkan konsep resource pooling, di mana penyedia layanan menggabungkan sumber daya komputasi dan mendistribusikannya secara dinamis kepada banyak pengguna. Model ini dikenal dengan sistem multi-tenant, di mana pengguna berbagi infrastruktur fisik namun tetap memperoleh layanan yang bersifat pribadi dan aman. Mekanisme ini meningkatkan efisiensi penggunaan sumber daya serta memberikan fleksibilitas dalam pengalokasian kapasitas sesuai permintaan masing-masing pengguna.

Dua karakteristik penting lainnya adalah rapid elasticity dan measured service. Rapid elasticity memungkinkan pengguna untuk dengan cepat

menambah atau mengurangi kapasitas sumber daya sesuai kebutuhan bisnis yang berubah-ubah, sehingga tampak seperti tidak ada batasan kapasitas. Sementara itu, *measured service* merujuk pada kemampuan sistem cloud dalam mengukur dan memantau penggunaan layanan secara otomatis dan transparan. Pengguna hanya membayar sesuai dengan jumlah layanan yang digunakan, yang menjadikan cloud sebagai solusi hemat biaya dan efisien dalam jangka panjang.



**Gambar 1.2:** Layanan Cloud

Infografis ini menyajikan visualisasi tentang bagaimana layanan cloud memiliki lima karakteristik utama yang saling terhubung dan mendukung keunggulan teknologi ini. Ikon-ikon tersebut membantu mempermudah pemahaman konsep bagi pembaca, terutama dalam konteks pembelajaran visual atau presentasi.

Di tengah, awan bertuliskan "CLOUD COMPUTING" menjadi pusat perhatian, yang menunjukkan bahwa semua karakteristik tersebut merupakan bagian integral dari sistem cloud. Akses luas melalui berbagai perangkat (*Broad Network Access*) dan pengelolaan mandiri (*On-Demand Self-Service*) mempermudah pengguna dalam menjalankan aktivitas komputasi tanpa batasan teknis. Sistem pembagian sumber daya (*Resource Pooling*) dan kemampuan elastisitas tinggi (*Rapid Elasticity*) menciptakan fleksibilitas penggunaan, sementara pengukuran otomatis (*Measured*

Service) memastikan transparansi dan efisiensi biaya.(Afzaal and Ul Haq, 2025)

## 1.3 Model Layanan Cloud Computing

Cloud Computing menyediakan berbagai model layanan yang dapat disesuaikan dengan kebutuhan pengguna, baik untuk individu, pengembang, hingga perusahaan skala besar. Tiga model layanan utama yang menjadi fondasi dari cloud computing adalah Infrastructure as a Service (IaaS), Platform as a Service (PaaS), dan Software as a Service (SaaS). Ketiga model ini memiliki tingkat kontrol dan tanggung jawab yang berbeda-beda antara pengguna dan penyedia layanan (Zhou et al., 2024).

Infrastructure as a Service (IaaS) merupakan model layanan cloud yang paling dasar. Layanan ini menyediakan infrastruktur IT seperti server virtual, penyimpanan data, dan jaringan secara virtual. Pengguna memiliki kontrol penuh terhadap sistem operasi, middleware, dan aplikasi yang dijalankan di atas infrastruktur tersebut. IaaS cocok digunakan oleh perusahaan yang membutuhkan fleksibilitas tinggi dalam membangun dan mengelola lingkungan TI mereka sendiri, tanpa harus membeli dan memelihara perangkat keras secara fisik (Kusuma, Pawening and Dijaya, 2017).

Platform as a Service (PaaS) menawarkan platform pengembangan aplikasi lengkap yang mencakup sistem operasi, basis data, dan alat pengembangan, tanpa pengguna harus mengelola infrastruktur di bawahnya. PaaS dirancang untuk mendukung siklus hidup pengembangan aplikasi mulai dari perancangan, pengujian, hingga penerapan (deployment). Dengan model ini, pengembang dapat lebih fokus pada penulisan kode dan fungsionalitas aplikasi tanpa terbebani oleh aspek teknis infrastruktur (Barus, Pardede and Putri Br. Manjorang, 2024).

Sementara itu, Software as a Service (SaaS) adalah model layanan di mana aplikasi perangkat lunak disediakan dan dikelola sepenuhnya oleh penyedia

cloud. Pengguna cukup mengakses aplikasi tersebut melalui internet menggunakan browser, tanpa perlu menginstal atau memeliharanya secara lokal. Contoh populer dari SaaS antara lain Google Workspace, Microsoft 365, dan Dropbox. Model ini sangat efisien karena memudahkan pengguna untuk langsung menggunakan aplikasi tanpa proses instalasi, update, atau konfigurasi teknis.

## 1.4 Manfaat Cloud Computing

Adopsi Cloud Computing telah membawa berbagai manfaat signifikan bagi individu, organisasi, dan dunia bisnis secara umum. Salah satu manfaat utama adalah skalabilitas, yaitu kemampuan untuk menyesuaikan kapasitas sumber daya komputasi sesuai kebutuhan. Dengan cloud, perusahaan dapat menangani lonjakan permintaan sistem secara fleksibel tanpa harus berinvestasi besar dalam perangkat keras fisik. Hal ini sangat membantu, terutama dalam situasi yang memerlukan respon cepat terhadap peningkatan beban kerja, seperti saat peluncuran produk atau musim puncak penjualan (Jumarlis and Mirfan, 2022).

Selain skalabilitas, efisiensi biaya menjadi alasan kuat lainnya bagi banyak organisasi untuk beralih ke cloud. Dengan menggunakan model sewa atau pay-as-you-go, pengguna hanya membayar sumber daya yang mereka gunakan. Hal ini mengurangi kebutuhan akan investasi awal yang besar untuk pembelian perangkat keras dan perangkat lunak, serta biaya pemeliharaan sistem secara berkelanjutan. Efisiensi ini memberikan keuntungan finansial terutama bagi usaha kecil dan menengah yang memiliki keterbatasan anggaran TI (Suryawijaya and Praptodiyono, 2024).

Manfaat berikutnya adalah aksesibilitas. Dengan sistem berbasis internet, data dan aplikasi dapat diakses kapan saja dan dari mana saja selama tersedia koneksi internet. Hal ini mendukung mobilitas kerja dan fleksibilitas yang lebih tinggi bagi pengguna, baik dalam konteks kerja jarak jauh, kerja tim lintas lokasi, maupun kolaborasi global. Aksesibilitas ini juga meningkatkan

produktivitas karena pengguna tidak lagi terbatas pada perangkat atau lokasi tertentu.

Terakhir, keamanan merupakan aspek penting yang ditawarkan oleh penyedia layanan cloud. Umumnya, mereka menyediakan fitur keamanan tingkat lanjut seperti enkripsi data, autentikasi multi-faktor, serta sistem pemantauan dan pemulihan bencana (disaster recovery). Meskipun masih ada kekhawatiran terkait privasi data, banyak penyedia cloud terkemuka telah memenuhi standar dan regulasi keamanan internasional, sehingga pengguna dapat merasa lebih tenang dalam menyimpan dan mengelola data mereka di lingkungan cloud.



**Gambar 1.3:** Manfaat Utama Cloud Computing

Gambar di atas memberikan representasi visual dari empat manfaat utama cloud computing dalam bentuk infografis yang mudah dicerna. Awan besar di tengah menunjukkan pusat layanan cloud yang menjadi sumber utama dari semua manfaat. Masing-masing ikon yang mengelilinginya memperjelas bagaimana teknologi ini memberikan solusi terhadap berbagai tantangan tradisional dalam pengelolaan data dan sistem TI.

Ilustrasi panah pada grafik menunjukkan fleksibilitas dalam menyesuaikan kapasitas (skalabilitas), sedangkan ikon dompet atau koin menyimbolkan

efisiensi pengeluaran karena cloud tidak menuntut investasi awal besar. Sementara itu, koneksi antar perangkat menunjukkan bahwa cloud dapat diakses dari mana saja (aksesibilitas), dan ikon gembok melambangkan jaminan keamanan data yang disediakan oleh penyedia cloud. Dengan pendekatan visual ini, pembaca dapat lebih mudah memahami inti manfaat Cloud Computing secara komprehensif.

## Bab 2

# Karakteristik Cloud Computing

## 2.1 Cloud Computing

Cloud computing adalah suatu model komputasi, dimana sumber daya seperti processor, storage, network, dan software menjadi abstrak dan diberikan sebagai layanan di jaringan/internet dengan menggunakan pola akses remote. Ketersediaan on-demand sesuai kebutuhan, mudah untuk dikontrol, dinamik dan skalabilitas yang hampir tanpa batas adalah beberapa atribut penting dari cloud computing.

Komputasi awan (cloud computing) adalah teknologi yang menjadikan internet sebagai pusat pengelolaan data dan aplikasi, dengan pengguna komputer diberikan hak akses (login). Awan (cloud) adalah metafora dari internet, sebagaimana awan yang sering digambarkan di diagram jaringan komputer. Sebagaimana awan dalam diagram jaringan komputer, awan (cloud) dalam cloud computing, juga merupakan abstraksi dari infrastruktur kompleks yang disembunyikannya.

Ia adalah suatu metode komputasi, yang kapabilitas terkait teknologi informasinya disajikan sebagai suatu layanan (as a service), sehingga pengguna dapat mengaksesnya melalui internet ("di dalam awan") tanpa mengetahui apa yang ada di dalamnya, ahli dengannya, atau memiliki kendali terhadap infrastruktur teknologi yang membantunya.

Makalah tahun 2008 yang di publikasi dengan judul Institute of Electrical and Engineers, IEEE, mendefenisikan internet computing sebagai berikut:

"Cloud Computing adalah paradigma di mana informasi secara permanen tersimpan di server di internet dan tersimpan secara sementara di komputer pengguna (client) termasuk di dalamnya adalah desktop, komputer tablet, notebook, komputer tembok, handheld, sensor-sensor, monitor dan lain-lain."

....



**Gambar 2.1:** Konseptual Komputasi Awan

Komputasi awan adalah konsep umum mencakup SaaS, Web 2.0, dan tren teknologi terbaru lain, yang dikenal luas, dengan tema umum berupa ketergantungan terhadap internet untuk memberikan kebutuhan komputasi pengguna. Sebagai contoh, Google Apps menyediakan aplikasi bisnis umum secara daring yang diakses melalui penjelajah web dengan

perangkat lunak dan data yang tersimpan di server. Komputasi awan saat ini merupakan tren teknologi terbaru, contoh bentuk pengembangan dari teknologi cloud computing ini adalah iCloud.

Cloud computing adalah evolusi selanjutnya dari internet. Cloud computing merupakan penyedia atau hal-hal yang berkaitan dari tenaga komputasi, hingga infrastruktur komputasi, aplikasi-aplikasi, proses bisnis hingga kolaborasi yang muncul sebagai layanan yang dapat diakses pada saat dibutuhkan kapan pun di mana pun (Muttaqin *et al.*, 2024).

## 2.2 Karakteristik Cloud Computing

Agar sebuah layanan bisa dikategorikan sebagai layanan Cloud Computing maka layanan tersebut harus memenuhi lima karakteristik dasar sesuai dengan panduan karakteristik dari NIST.

Kelima karakteristik tersebut adalah sebagai berikut:

### 1. On-demand Self Service

Pengguna layanan harus bisa mengelola sumber daya komputasi secara mandiri dan memiliki kontrol dalam hal pengadaan dan pengelolaan sumber daya komputasi tanpa memerlukan persetujuan atau bantuan dari pihak penyedia layanan.

Beberapa hal penting yang harus diperhatikan agar memenuhi kriteria ini antara lain adalah sebagai berikut:

- a. Akses Mandiri: Pengguna mempunyai kemampuan untuk dapat memilih, mengkonfigurasi dan mengelola sumber daya komputasi sesuai kebutuhan mereka sendiri tanpa perlu melibatkan pihak penyedia layanan.
- b. Kemudahan Pengguna: Tersedianya antarmuka pengguna yang dirancang untuk memastikan pengguna dapat dengan mudah

mengelola sumber daya komputasi tersebut tanpa memerlukan keahlian ataupun kemampuan teknis yang mendalam.

- c. **Pengadaan Cepat:** Pengadaan sumber daya komputasi dapat dilakukan secara cepat dan efisien. Pengadaan tersebut harus bisa dilakukan dalam hitungan menit atau bahkan detik sehingga mempunyai skalabilitas yang baik untuk memenuhi kebutuhan bisnis ataupun beban komputasi yang dibutuhkan.
  - d. **Otomatisasi:** Proses otomatisasi adalah kunci dari on-demand self service ini. Pengadaan sumber daya komputasi, konfigurasi dan pengelolaannya harus dapat dilakukan secara otomatis berdasarkan kebutuhan pengguna.
  - e. **Kontrol Penuh:** Pengguna harus memiliki kendali penuh atas sumber daya komputasi yang digunakan. Mereka dapat memonitor, mengelola dan menghentikan penggunaan sumber daya komputasi sesuai dengan kebutuhan tanpa campur tangan penyedia layanan.
2. **Broad Network Access**

Sumber daya komputasi harus dapat diakses melalui berbagai jenis perangkat. Pengguna dapat terhubung dengan sumber daya komputasi melalui berbagai jenis perangkat dan berbagai jenis konektivitas jaringan.

Beberapa hal penting yang harus diperhatikan terkait hal ini adalah sebagai berikut:

- a. **Akses Melalui Internet:** Sumber daya komputasi dapat diakses melalui internet, sehingga memungkinkan pengguna untuk terhubung dengan sumber daya tersebut dari lokasi manapun selama tersedia koneksi jaringan internet.
- b. **Kemampuan Akses dari Berbagai Perangkat:** Sumber daya komputasi tersebut harus dapat diakses dari berbagai

perangkat, misalnya seperti: laptop, komputer desktop, ponsel pintar dan tablet. Hal ini akan memberikan kemudahan dan fleksibilitas bagi pengguna untuk mengakses layanannya dari berbagai perangkat, kapan saja dan dimana saja saat dibutuhkan.

- c. Platform Independen: Layanan cloud computing tersebut harus bisa diakses dari berbagai platform dan sistem operasi tanpa hambatan yang signifikan. Hal ini akan mempermudah pengguna untuk bisa menggunakan layanan tersebut tanpa tergantung oleh platform atau sistem operasi tertentu.
  - d. Antarmuka Pengguna Yang Mudah: Pengguna layanan cloud computing harus diberikan kemudahan akses tanpa memerlukan instalasi perangkat tambahan khusus. Untuk itu biasanya layanan cloud computing akan menyediakan antar muka berbasis web sehingga pengguna bisa mengelola layanan yang ada dengan cukup menggunakan web browser.
  - e. Protokol Komunikasi Data: Komunikasi antara pengguna dan sumber daya komputasi menggunakan protokol komunikasi data yang standar, seperti HTTP, HTTPS, ataupun protokol komunikasi data lainnya yang mendukung interoperabilitas dan kompatibilitas dari berbagai perangkat yang ada.
3. Resource Pooling

Layanan cloud computing akan bermuara pada data center atau pusat data. Pada pusat data merupakan bangunan fisik dimana sumber daya komputasi dikumpulkan, dikelola dan dikonfigurasi sehingga bisa menjadi pondasi dari layanan cloud computing yang diberikan.

Beberapa hal penting terkait resource pooling ini antara lain adalah sebagai berikut:

- a. Penggabungan Sumber Daya: Pada pusat data tersedia berbagai sumber daya pendukung komputasi yang digabungkan sehingga mempunyai kemampuan komputasi yang sangat besar. Kemampuan komputasi ini kemudian bisa dibagipakaikan kepada para pelanggannya untuk memenuhi berbagai kebutuhan pelanggan.
- b. Pemisahan Logis: Pada pusat data dan perangkat pendukung layanan cloud computing dilakukan implementasi pemisahan secara logis dengan menggunakan bantuan perangkat lunak dan perangkat keras sehingga masing-masing pelanggan tetap memiliki kontrol penuh dan eksklusif atas sumber daya komputasi yang mereka gunakan.
- c. Penggunaan Yang Efisien: Implementasi resource pooling akan mengoptimalkan penggunaan sumber daya secara lebih efisien. Sumber daya yang tidak digunakan bisa dialokasikan untuk beban kerja lainnya sehingga resource komputasi bisa digunakan secara lebih optimal.
- d. Skalabilitas Layanan: Besarnya sumber daya komputasi yang dikonfigurasi pada pusat data akan memengaruhi tingkat skalabilitas layanan. Semakin besar sumber daya komputasi yang ada pada pusat data akan membuat skalabilitas semakin baik. Hal ini diperlukan agar dapat memenuhi kebutuhan pelanggan yang bisa berubah-ubah sesuai dengan fluktuasi beban komputasi yang dibutuhkan.
- e. Pengelolaan Sumber Daya Komputasi Terpusat: Penyedia layanan cloud computing akan melakukan pengawasan secara terpusat untuk mengetahui perangkat komputasi yang

dibutuhkan berjalan dengan baik sesuai tugas dan fungsinya. Pengawasan ini mencakup alokasi dan perubahan kapasitas sumber daya sesuai dengan kebutuhan seluruh pelanggannya.

#### 4. Rapid Elasticity

Kemampuan sumber daya komputasi untuk secara cepat dan otomatis menyesuaikan kapasitasnya sesuai dengan perubahan permintaan dari pengguna. Dengan kemampuan ini maka akan memungkinkan pelanggan untuk dengan mudah meningkatkan atau mengurangi kapasitas sumber daya komputasi secara instan, sesuai dengan fluktuasi kebutuhan beban komputasi.

Beberapa hal penting terkait dengan rapid elasticity ini adalah sebagai berikut:

- a. Skalabilitas Yang Dinamis: Memungkinkan sumber daya komputasi untuk dapat ditingkatkan kemampuannya (scale up) atau diturunkan (scale down) secara cepat dan mudah.
- b. Respon Yang Cepat: Saat terjadi lonjakan permintaan atau beban kerja komputasi yang tinggi, layanan cloud computing harus mampu memberikan respon yang cepat. Respon tersebut misalnya secara otomatis dapat menambah kapasitas sumber daya untuk menjaga kinerja dan ketersediaan layanan komputasi. Sebaliknya apabila beban kerja komputasi menurun secara otomatis kapasitas sumber daya komputasi juga dapat diturunkan sehingga akan mengurangi dan menghindari pengeluaran biaya yang tidak diperlukan.
- c. Otomatisasi Proses Skalabilitas: Skalabilitas pada layanan cloud computing bisa dilakukan secara otomatis tanpa campur tangan manusia sehingga memungkinkan tanggapan yang cepat terhadap perubahan beban kerja komputasi.

- d. **Fleksibilitas dan Efisiensi Biaya:** Pengguna layanan cloud computing dapat menghindari investasi awal yang besar karena dapat menyesuaikan kapasitas sumber daya komputasi secara fleksibel sesuai dengan beban kerja komputasi yang dibutuhkan dan hanya membayar berdasarkan penggunaan aktual dari sumber daya komputasi yang digunakan.
- e. **Penggunaan Yang Dinamis:** Karakteristik rapid elasticity ini memungkinkan pengguna/organisasi untuk menanggapi dinamika bisnis yang cepat dan perubahan yang tiba-tiba dalam kebutuhan kapasitas sumber daya komputasi tanpa perlu mengalami penurunan kinerja ataupun gangguan layanan.

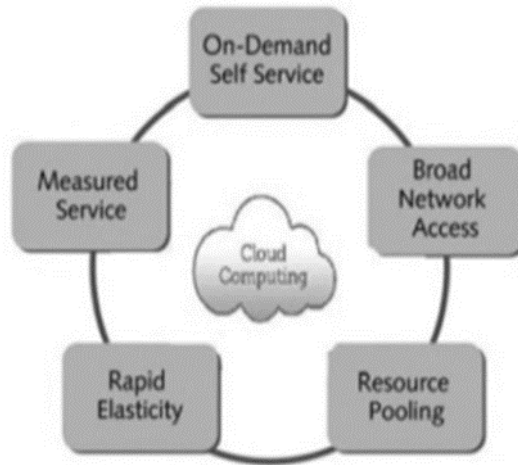
#### 5. Measured Service

Kemampuan untuk mengukur dan memantau penggunaan sumber daya komputasi secara menyeluruh. Proses ini melibatkan fungsi pemantauan, kontrol dan juga pelaporan penggunaan sumber daya komputasi. Pengguna bisa mengakses fungsi tersebut setiap saat sehingga bisa mengetahui biaya penggunaan dan prediksi biaya layanan dari sumber daya komputasi yang digunakan. Pengguna layanan cloud computing bisa melakukan hal tersebut melalui dashboard/antar muka berbasis web yang disediakan oleh penyedia layanan cloud computing.

Beberapa hal penting terkait dengan measured service ini adalah sebagai berikut:

- a. **Pengukuran Otomatis:** Layanan cloud computing akan secara otomatis dan terus menerus mengukur penggunaan sumber daya komputasi. Pengukuran ini mencakup berbagai parameter yang penting sehingga penggunaan layanan cloud computing bisa transparan.

- b. Pemantauan Realtime: Informasi penggunaan sumber daya komputasi tersedia secara realtime, sehingga pengguna layanan bisa memantau performa dan juga penggunaan sumber daya komputasi setiap diperlukan.
- c. Pelaporan dan Analisis: Data pengukuran dikumpulkan dan disajikan dalam bentuk laporan yang dapat dipahami, memberikan visibilitas terhadap bagaimana sumber daya digunakan. Analisis data ini dapat membantu organisasi membuat keputusan yang lebih baik terkait alokasi sumber daya, perencanaan kapasitas, dan efisiensi operasional.
- d. Pembayaran Berdasarkan Penggunaan Aktual: Biaya yang perlu dibayarkan berdasarkan pada penggunaan aktual sumber daya komputasi. Pengguna hanya akan membayar untuk sumber daya yang benar-benar digunakan, menghindari pembayaran yang berlebihan atau biaya tetap yang tidak efisien.
- e. Efisiensi Biaya: Dengan memiliki pemahaman yang jelas tentang penggunaan sumber daya, pengguna dapat melakukan efisiensi dengan mengelola sumber daya komputasi dengan baik untuk mengoptimalkan biaya. Berdasarkan informasi tersebut pengguna dapat membuat keputusan tentang kapan dan seberapa banyak sumber daya komputasi yang diperlukan.
- f. Audit dan Kepatuhan: Data pengukuran tersebut dapat juga dapat digunakan untuk tujuan audit dan kepatuhan. Organisasi dapat melacak dan melaporkan penggunaan sumber daya untuk memastikan bahwa mereka mematuhi kebijakan dan aturan dari organisasi terkait penggunaan sumber daya komputasi.



**Gambar 2.2:** Konseptual Karakteristik Komputasi Awan

## 2.3 Jenis Layanan Cloud Computing

Menurut NIST terdapat tiga jenis layanan cloud computing. Jenis layanan ini menentukan kontrol dan tingkat keterlibatan pengguna dalam pengelolaan sumber daya komputasi.

Ketiga jenis layanan cloud computing tersebut adalah sebagai berikut:

1. Infrastructure as a Service (IaaS):

Adalah layanan cloud computing yang menyediakan akses kepada infrastruktur sumber daya komputasi yang mendasar, seperti server, storage, jaringan, dan mesin virtual (virtual machine). Pengguna memiliki kontrol penuh atas lingkungan infrastruktur, termasuk pilihan instalasi sistem operasi, dan bisa melakukan apa saja diatas sistem operasi tersebut, misalnya menginstal aplikasi, middleware, database server dsbnya. Contoh layanan IaaS ini

antara lain: Amazon Web Services (AWS) EC2, Microsoft Azure Virtual Machines, Google Compute Engine, dsbnya.

2. Platform as a Service (PaaS):

Adalah layanan cloud computing yang telah dikonfigurasi secara khusus sebagai lingkungan untuk menjalankan aplikasi yang dibuat oleh para pengembang perangkat lunak. Umumnya lingkungan tersebut akan mendukung aplikasi berbasis web (web application). Keuntungan dalam menggunakan layanan ini adalah organisasi/pengembang perangkat lunak bisa fokus dalam mengembangkan perangkat lunaknya tidak perlu lagi memikirkan bagaimana kompleksitas pengelolaan lingkungan pendukung aplikasi tersebut (infrastruktur, sistem operasi, database, middleware, dsbnya). Contoh layanan PaaS ini antara lain: Google App Engine, Microsoft Azure App Service, Heroku, dsbnya.

3. Software as a Service (SaaS):

Adalah layanan cloud computing yang menyediakan aplikasi perangkat lunak yang lengkap dan siap pakai sebagai sebuah layanan. Pengguna dapat mengakses dan menggunakan aplikasi ini melalui internet tanpa perlu menginstal atau menjalankan perangkat lunak di perangkat lokal mereka. Pengguna membayar berlangganan untuk menggunakan aplikasi ini, biasanya berdasarkan pemakaian atau jumlah pengguna. Contoh layanan SaaS ini antara lain: Microsoft Office 365, Google Workspace, Salesforce, dsbnya.

## 2.4 Deployment Model Layanan Cloud Computing

NIST menyampaikan ada empat deployment model dari layanan cloud computing. Deployment model ini mengacu pada dimana layanan cloud computing tersebut dibangun dan dioperasikan. Setiap deployment model cloud memiliki karakteristik, manfaat, dan pertimbangan keamanan yang berbeda, dan pemilihan model yang tepat tergantung pada kebutuhan dan strategi bisnis masing-masing organisasi.

Keempat deployment model tersebut adalah:

1. Public Cloud

Merupakan layanan cloud computing yang dibangun dan ditujukan untuk melayani masyarakat umum. Semua orang bisa mendaftar dan menggunakannya selama mereka terhubung dengan internet. Contoh layanan public cloud ini antara lain: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) dan berbagai cloud provider yang ada di Indonesia.

2. Private Cloud

Merupakan layanan cloud computing yang dibangun dan ditujukan untuk melayani secara eksklusif suatu organisasi tertentu. Sumber daya komputasi ini hanya bisa diakses dan digunakan oleh orang-orang dalam organisasi tersebut. Organisasi tersebut bisa membangun layanan cloud computing secara mandiri atau bisa juga menggunakan penyedia layanan cloud computing dari pihak lain namun sumber daya yang diperlukan dikonfigurasi secara khusus hanya melayani organisasi tersebut. Private cloud ini memberikan kontrol dan keamanan

yang lebih besar karena sumber daya tidak dibagi dengan entitas/organisasi lainnya.

### 3. Community Cloud

Community cloud merupakan model di mana infrastruktur cloud dibagi dan digunakan oleh beberapa organisasi yang memiliki kepentingan, kebijakan, atau keamanan yang serupa atau berbagi kebutuhan bisnis tertentu. Sumber daya cloud ini dapat dikelola bersama oleh organisasi-organisasi dalam komunitas yang sama atau oleh penyedia layanan cloud khusus yang melayani komunitas tertentu.

### 4. Hybrid Cloud

Hybrid cloud adalah model yang menggabungkan dua atau lebih deployment model cloud yang berbeda, seperti public cloud, private cloud, atau community cloud, menjadi satu lingkungan yang terintegrasi. Penggunaan hybrid cloud memungkinkan organisasi untuk memanfaatkan kelebihan dari masing-masing model, seperti keamanan dan kontrol dari private cloud serta skalabilitas dan elastisitas dari public cloud. Hybrid cloud juga memungkinkan untuk fleksibilitas dalam memindahkan beban kerja antara berbagai lingkungan cloud.



# Bab 3

## Model Layanan Cloud Computing

### 3.1 Model Layanan Cloud Computing

Cloud computing merupakan cara baru dalam memberikan layanan teknologi informasi yang memungkinkan pengguna mengakses sumber daya komputer dengan mudah, seperti penyimpanan data atau perangkat lunak, melalui Internet. Komputasi awan menawarkan beragam model layanan yang dirancang untuk memenuhi berbagai kebutuhan pengguna, mulai dari penyediaan infrastruktur hingga aplikasi siap pakai. Secara umum, layanan ini dibagi menjadi tiga jenis utama: Infrastruktur sebagai Layanan (IaaS), Platform sebagai Layanan (PaaS), dan Perangkat Lunak sebagai Layanan (SaaS).

Salah satu model utamanya adalah Infrastruktur sebagai Layanan (IaaS), yang menyediakan sumber daya komputasi dasar seperti server, penyimpanan, dan jaringan melalui Internet. Bagian ini akan membahas

IaaS secara mendalam mulai dari definisi, arsitektur, dan contoh implementasinya. Selain itu, ada Platform as a Service (PaaS) yang menyediakan alat untuk membuat aplikasi tanpa harus memikirkan teknologi, dan Software as a Service (SaaS) yang menyediakan aplikasi siap pakai seperti email atau aplikasi perkantoran.

Setiap jenis layanan dirancang untuk memenuhi kebutuhan pengguna dengan cara yang berbeda. Komputasi awan semakin populer karena membantu menghemat biaya, memudahkan penyesuaian kapasitas sesuai kebutuhan, dan dapat diakses dari mana saja dengan koneksi internet. Bab ini menjelaskan lebih detail ketiga jenis layanan tersebut, apa kelebihanannya, dan bagaimana komputasi awan mengubah cara kerja dunia digital saat ini.

### 3.1.1 Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) merupakan model layanan cloud computing yang menyediakan infrastruktur teknologi informasi secara virtual melalui Internet (Rezki, 2014). Dengan IaaS, pengguna dapat menyewa komponen dasar seperti server, penyimpanan data, jaringan, dan sistem operasi tanpa harus membeli atau memelihara perangkat keras sendiri.

Model ini sangat fleksibel dan mudah disesuaikan, sehingga organisasi atau perusahaan dapat menambah atau mengurangi kapasitas sesuai kebutuhan tanpa harus mengeluarkan banyak uang untuk membeli perangkat keras (Muttaqin *et al.*, 2023).

Keuntungan utama Infrastruktur sebagai Layanan (IaaS) adalah:

1. Biaya lebih rendah: Pengguna hanya perlu membayar sumber daya yang mereka gunakan, dan tidak perlu mengeluarkan banyak uang untuk membeli atau memelihara perangkat keras.
2. Lebih fleksibel dan mudah beradaptasi: Kapasitas sumber daya dapat dengan mudah ditingkatkan atau diturunkan sesuai kebutuhan, cocok untuk bisnis dengan kebutuhan yang terus berubah.

3. Lebih mudah untuk dikelola: Penyedia layanan IaaS akan bertanggung jawab untuk memelihara infrastruktur seperti server dan jaringan. Dengan cara ini, pengguna dapat lebih fokus pada pengembangan aplikasi atau layanannya dibandingkan harus berurusan dengan masalah teknis.

### **Arsitektur Infrastructure as a Service (IaaS)**

Arsitektur IaaS (Infrastructure as a Service) terdiri dari beberapa elemen utama yang saling berinteraksi untuk menyediakan layanan infrastruktur melalui cloud (Rezki, 2014).

Berikut ini penjelasan singkat mengenai setiap elemennya:

1. Komputasi Virtual (Virtual Machines/VMs dan Kontainer), dengan menggunakan virtual machine (VM) atau kontainer, pengguna dapat menjalankan aplikasi pada perangkat keras yang disediakan oleh penyedia layanan cloud. Baik VM maupun kontainer memungkinkan pengguna untuk menjalankan aplikasi atau sistem operasi tanpa harus memiliki perangkat keras sendiri. Contoh layanan yang populer antara lain Amazon EC2, Google Compute Engine, dan Microsoft Azure Virtual Machines.
2. Penyimpanan (Storage), dalam IaaS menawarkan berbagai pilihan untuk menyimpan data, termasuk block storage, object storage, dan file storage. Tipe penyimpanan ini menjamin data tersimpan dengan aman dan bisa diakses kapan saja lewat internet. Layanan penyimpanan yang terkenal adalah Amazon S3, Google Cloud Storage dan Azure Blob Storage.
3. Networking, Layanan IaaS menawarkan berbagai fitur, termasuk virtual private network (VPN), load balancing, DNS dan perlindungan melalui firewall, untuk menjaga agar komunikasi antara sistem tetap aman dan efisien. Beberapa layanan jaringan

yang terkenal adalah Amazon VPC, Google Cloud Virtual Private Cloud dan Azure Virtual Network.

4. Manajemen dan Otomatisasi, IaaS menawarkan berbagai alat yang membantu pengguna dalam mengatur dan mengotomatiskan infrastruktur mereka, termasuk auto-scaling, monitoring, dan orchestration. Dengan adanya fitur ini, sistem dapat beroperasi dengan efisiensi dan kinerja lebih optimal. Beberapa layanan yang terkenal adalah AWS Auto Scaling, Kubernetes (untuk manajemen kontainer), dan lainnya.
5. Keamanan dan Kepatuhan: Keamanan merupakan prioritas utama dalam IaaS. Penyedia layanan menawarkan fitur seperti enkripsi data, firewall, identity management, dan monitoring untuk melindungi data pengguna dari ancaman keamanan dan memastikan kepatuhan terhadap regulasi. Contoh: AWS Identity and Access Management (IAM), Azure Security Center, Google Cloud IAM.

### **Contoh Implementasi Infrastructure as a Service (IaaS)**

Banyak organisasi dan perusahaan telah menggunakan Infrastructure as a Service (IaaS) untuk meningkatkan efisiensi operasional mereka sekaligus mengurangi biaya infrastruktur teknologi informasi.

Beberapa contoh penerapan IaaS di segala bidang:

1. Layanan website dan aplikasi: Banyak organisasi atau perusahaan mengoperasikan layanan IaaS untuk menjalankan website atau aplikasi mereka tanpa perlu membeli server fisik. Dengan IaaS, mereka dapat menyesuaikan kapasitas sesuai dengan kebutuhan. Misalnya: Netflix menggunakan Amazon Web Services (AWS) menawarkan layanan streaming konten di seluruh dunia dengan skalabilitas tinggi.

2. **Disaster Recovery dan Backup:** Banyak Perusahaan atau organisasi menggunakan IaaS sebagai cara untuk mengatasi bencana dengan menyimpan salinan data mereka di awan. Ini membuat data tetap terlindungi dan dapat diakses kembali ketika ada masalah pada sistem. Contoh: Bank dan lembaga keuangan menggunakan Microsoft Azure untuk menjaga data nasabah dan memastikan data tersebut selalu ada meskipun sistem mengalami kegagalan.
3. **Pengembangan dan Pengujian Aplikasi (DevOps):** Pengembang aplikasi memanfaatkan IaaS untuk merancang, menguji, dan meluncurkan aplikasi di suatu lingkungan yang adaptif tanpa perlu mengurus perangkat keras secara langsung. Hal ini mempercepat tahap pengembangan dan pengujian. Contoh: Start-up memanfaatkan AWS EC2 atau Google Compute Engine untuk menciptakan aplikasi yang berbasis cloud.

### 3.1.2 Platform as a Service (PaaS)

Platform as a Service atau PaaS, merupakan sebuah model dalam cloud computing yang menyediakan tempat untuk mengembangkan dan menerapkan aplikasi berbasis cloud (Yunie Cancer, 2016). Dengan PaaS, para pengembang dapat membuat, menguji, dan menjalankan aplikasi tanpa harus mengurus infrastruktur yang mendasarinya, seperti server, jaringan, atau sistem operasi. PaaS memberikan berbagai macam alat dan layanan, seperti sistem operasi, database, framework pengembangan, serta alat untuk DevOps. Melalui PaaS, para pengembang dapat berkonsentrasi pada pengembangan aplikasi tanpa harus memikirkan pengelolaan infrastruktur.

Keuntungan utama dari Platform as a Service (PaaS) adalah:

1. **Tanpa proses instalasi:** Aplikasi dapat langsung digunakan melalui browser atau aplikasi tanpa perlu memerlukan instalasi yang rumit.

2. Pembaruan otomatis: Penyedia layanan SaaS secara teratur mengelola pembaruan perangkat lunak, penambahan fitur, dan perbaikan kesalahan, sehingga pengguna selalu menggunakan versi terbaru.
3. Akses yang fleksibel: Aplikasi dapat diakses dari berbagai perangkat, seperti laptop, ponsel, atau tablet, selama terhubung ke internet.
4. Skalabilitas tinggi: Pengguna bisa dengan mudah mengubah jumlah pengguna atau kapasitas layanan sesuai kebutuhan bisnis, baik untuk menambah atau mengurangi skala operasional.

### **Arsitektur Platform as a Service (PaaS)**

Arsitektur PaaS terdiri dari beberapa lapisan utama yang saling terhubung untuk mendukung pengembangan dan penerapan aplikasi berbasis cloud.

Berikut penjelasan detail dari PaaS:

1. Infrastruktur virtualisasi, merupakan dasar dari sebuah layanan PaaS. Infrastruktur virtualisasi mencakup server, penyimpanan data, dan jaringan yang berbasis cloud. Semua hal ini diatur oleh penyedia layanan, sehingga pengguna tidak perlu khawatir tentang hardware fisik. Contoh: AWS (Amazon Web Services), Microsoft Azure dan Google Cloud menyediakan infrastruktur virtualisasi yang digunakan oleh layanan PaaS mereka.
2. Sistem Operasi dan Middleware, Layanan PaaS menyediakan sistem operasi (misalnya Linux atau Windows) serta middleware seperti basis data, runtime (lingkungan untuk menjalankan aplikasi), dan messaging services (untuk komunikasi antar sistem).
3. Contoh: Google App Engine menyediakan runtime untuk berbagai bahasa pemrograman seperti Python, Java, dan Node.js.

4. Alat Pengembangan dan API, PaaS menyediakan framework dan API (Application Programming Interface) yang memudahkan para pengembang dalam membangun aplikasi. Framework ini membantu pengembang untuk mempercepat proses pembuatan aplikasi dengan menggunakan kode yang sudah ada. Contoh: Heroku menyediakan framework untuk berbagai bahasa pemrograman seperti Python, Node.js, Ruby.
5. Manajemen Aplikasi dan Otomasi, Layanan ini mencakup alat untuk deployment (penyebaran aplikasi), monitoring (pemantauan performa), dan manajemen aplikasi berbasis cloud. Fitur ini memastikan aplikasi berfungsi dengan baik dan dapat disesuaikan sesuai permintaan. Contoh: AWS Elastic Beanstalk membantu otomatisasi deployment aplikasi berbasis cloud, sehingga pengembang tidak perlu melakukan konfigurasi manual.

### **Contoh Implementasi Platform as a Service (PaaS)**

Platform as a Service (PaaS) telah menjadi pilihan utama bagi perusahaan dan pengembang untuk membangun serta mengelola aplikasi tanpa perlu berurusan dengan infrastruktur yang rumit. Dengan adanya PaaS, pengembang dapat lebih fokus pada pembuatan perangkat lunak tanpa harus memikirkan pengelolaan sistem operasi, server, atau pembaruan perangkat lunak. Model ini menawarkan efisiensi yang lebih baik, meningkatkan skala, dan memudahkan integrasi dengan berbagai layanan dari pihak ketiga.

Beberapa contoh penggunaan PaaS yang telah diterapkan oleh banyak perusahaan dan pengembang di seluruh dunia:

1. Google App Engine adalah sebuah layanan yang memungkinkan para pengembang untuk membuat dan meluncurkan aplikasi web secara otomatis tanpa perlu mengurus server. Semua aspek teknis seperti server, jaringan dan penyesuaian kapasitas ditangani oleh

Google. Salah satu contohnya adalah Snap Inc yang memanfaatkan Google App Engine untuk mengelola jumlah pengguna yang sangat banyak. Dengan platform PaaS ini, Snap Inc dapat lebih mengutamakan pengembangan fitur baru tanpa harus memikirkan masalah infrastruktur.

2. Azure App Services merupakan sebuah platform yang memungkinkan pengembangan dan menjalankan aplikasi web, API, serta backend mobile. Layanan ini kompatibel dengan berbagai bahasa pemrograman seperti .NET, Java, Python, dan PHP. Salah satu contohnya adalah Samsung yang memanfaatkan Azure untuk pengelolaan layanan IoT (Internet of Things) mereka. Melalui Azure, Samsung dapat menciptakan aplikasi yang terhubung dengan perangkat pintar tanpa perlu mengurus infrastruktur.
3. Heroku merupakan Platform sebagai Layanan yang berbasis kontainer dan mendukung banyak bahasa pemrograman untuk membuat aplikasi di cloud. Banyak startup yang sangat menyukai Heroku karena cara penggunaannya yang mudah. Salah satu contohnya adalah Product Hunt, sebuah situs untuk startup dan produk teknologi, yang dibangun dengan Heroku. Dengan menggunakan Heroku, tim pengembang Product Hunt dapat lebih fokus pada inovasi tanpa harus memikirkan infrastruktur.

### 3.1.3 Software as a Service (SaaS)

Software as a Service (SaaS) merupakan jenis layanan berbasis cloud yang paling terkenal dan user-friendly. Melalui SaaS, pengguna dapat menggunakan aplikasi perangkat lunak melalui internet tanpa harus mengurus infrastruktur atau platform yang ada di belakangnya.

Tipe layanan ini memberikan banyak manfaat, seperti kemudahan dalam penggunaan, biaya operasional yang rendah, pembaruan yang otomatis, dan

fleksibilitas akses dari mana saja. SaaS telah menjadi pilihan utama untuk orang-orang dan organisasi yang ingin meningkatkan efisiensi pekerjaan tanpa harus menghadapi masalah teknis yang rumit.

### **Arsitektur SaaS**

Arsitektur SaaS (Software as a Service) merupakan struktur teknis yang memungkinkan aplikasi berbasis cloud yang dapat berjalan dengan efisien, aman, dan dapat diakses oleh banyak pengguna secara bersamaan. Arsitektur ini dirancang untuk mendukung layanan perangkat lunak yang sepenuhnya dikelola oleh penyedia layanan, sehingga pengguna tidak perlu repot mengurus infrastruktur atau pemeliharaan sistem.

Beberapa komponen utama dari arsitektur SaaS:

1. Infrastruktur cloud terdiri dari server, penyimpanan, dan jaringan yang diperlukan untuk menjalankan aplikasi SaaS. yang memungkinkan pengguna dapat mengakses aplikasi melalui internet tanpa harus memiliki perangkat keras. Server akan mengoperasikan aplikasi, menyimpan data pengguna seperti file dan dokumen, sementara jaringan menjamin bahwa koneksi antara pengguna dan aplikasi selalu cepat dan stabil. Dengan menggunakan infrastruktur cloud, penyedia layanan dapat dengan mudah menyesuaikan kapasitas sesuai dengan kebutuhan pengguna, yang membuat biaya operasional lebih efisien dan pemeliharaan sistem dikelola sepenuhnya oleh penyedia layanan.
2. Arsitektur multi-tenant memungkinkan banyak pengguna untuk mengakses satu aplikasi SaaS pada saat yang sama, meskipun mereka memiliki pengaturan dan informasi yang berbeda. Dalam sistem ini, semua pengguna menggunakan aplikasi yang sama secara internal, namun data mereka dipisahkan secara logis untuk melindungi keamanan dan privasi. Model ini sangat efisien karena penyedia layanan hanya perlu mengelola satu versi aplikasi bagi

seluruh pengguna, sehingga pembaruan fitur atau perbaikan kesalahan bisa dilakukan secara tersentralisasi dan langsung diperoleh oleh semua tanpa perlu instalasi manual.

3. API (Application Programming Interface) memungkinkan aplikasi SaaS saling terhubung dengan layanan lain, seperti CRM, ERP, atau layanan pihak ketiga. Melalui API, aplikasi SaaS dapat saling bertukar informasi dengan layanan luar, mengotomatiskan proses tertentu, atau menambahkan fitur baru sesuai kebutuhan pengguna. Misalnya, Salesforce dapat terhubung dengan Mailchimp untuk kampanye pemasaran email, atau Google Workspace dapat diintegrasikan dengan Zoho CRM untuk meningkatkan kolaborasi tim. Integrasi ini membuat aplikasi SaaS lebih fleksibel dan dapat disesuaikan dengan kebutuhan bisnis yang spesifik.
4. Keamanan dan pengelolaan data merupakan elemen yang sangat krusial dalam desain SaaS untuk menjaga informasi rahasia pengguna. Penyedia layanan memanfaatkan teknologi enkripsi guna melindungi data baik saat disimpan maupun saat ditransfer melalui internet. Di samping itu, proses autentikasi pengguna, seperti penggunaan kata sandi yang kuat atau autentikasi dua langkah (2FA), menjamin bahwa hanya orang yang berwenang yang memiliki izin yang bisa mengakses aplikasi tersebut. Sistem pengelolaan identitas juga diaplikasikan untuk menentukan siapa yang diizinkan melihat atau mengubah data tertentu. Selain itu, penyimpanan data secara otomatis dan pemantauan aktivitas pengguna berperan penting dalam mencegah kehilangan data serta mendeteksi ancaman siber secara langsung.

### **Contoh Implementasi Software as a Service (SaaS)**

1. Google Workspace (Gmail, Google Drive, Google Docs, Google Meet), Google Workspace merupakan sekumpulan layanan produktivitas berbasis di cloud, yang menyediakan email, penyimpanan file, dokumen yang bisa dikerjakan secara bersamaan, dan konferensi video. Layanan ini sangat digemari karena mudah digunakan dan mendukung kolaborasi secara langsung antara pengguna. Dengan Google Workspace, pengguna dapat mengakses dokumen, spreadsheet, presentasi, dan alat komunikasi lainnya di berbagai perangkat yang terhubung ke internet. Fitur kolaborasi secara langsung memungkinkan tim untuk bekerja sama tanpa kendala lokasi. Banyak universitas dan perusahaan besar memilih Google Workspace untuk memfasilitasi komunikasi internal, kolaborasi tim, dan pengelolaan proyek secara daring.
2. Microsoft Office 365 merupakan software berbasis cloud yang membantu dalam hal produktivitas. Yang mencakup berbagai aplikasi seperti Word, Excel, PowerPoint, Outlook dan Microsoft Teams. Tujuan layanan ini adalah untuk mendukung kerja dan komunikasi dalam tim di dalam organisasi atau perusahaan. Office 365 menggabungkan aplikasi produktivitas tradisional dengan fitur cloud, termasuk penyimpanan di OneDrive dan kerja sama melalui Microsoft Teams. Dimana pengguna bisa mengakses dokumen mereka dari mana saja dan berbagi file dengan aman. Perusahaan besar internasional seperti Accenture dan PwC menggunakan Office 365 untuk pengelolaan dokumen, komunikasi dalam organisasi, dan kerja sama antar tim dari berbagai departemen.
3. Salesforce, yang merupakan Customer Relationship Management berbasis cloud, adalah layanan CRM terkemuka yang digunakan

untuk mengelola interaksi dengan pelanggan, kegiatan penjualan, pemasaran, dan pengolahan data. Platform ini dirancang untuk membantu bisnis memperbaiki hubungan mereka dengan pelanggan dan menyempurnakan proses operasional. Salesforce menawarkan berbagai alat canggih untuk memantau interaksi dengan pelanggan, mengontrol alur penjualan, dan menganalisis informasi untuk memperoleh pemahaman yang lebih baik tentang bisnis. Dengan desain yang user-friendly dan kapasitas untuk terintegrasi dengan perangkat lain, Salesforce menjadi pilihan yang sangat baik untuk perusahaan yang ingin meningkatkan kualitas pelayanan kepada pelanggan. Perusahaan e-commerce seperti Amazon dan ritel internasional seperti Nike memanfaatkan Salesforce untuk meningkatkan pengalaman pelanggan, mengatur kampanye pemasaran, dan memahami perilaku konsumen.

## 3.2 Keamanan dalam Cloud Computing

Cloud computing menawarkan fleksibilitas dan efisiensi yang luar biasa, tetapi juga membawa tantangan keamanan yang perlu dikelola dengan baik. Pembahasan ini mencakup berbagai aspek keamanan dalam cloud computing, mulai dari ancaman yang mungkin dihadapi hingga strategi perlindungan dan regulasi yang harus dipatuhi oleh organisasi.

### 3.2.1 Ancaman Keamanan pada Cloud Computing

Cloud computing memiliki banyak keuntungan, tetapi juga menimbulkan beberapa risiko keamanan yang dapat memengaruhi data. Salah satu risiko yang paling signifikan adalah hilangnya data dan pencurian informasi, yang sering kali disebabkan oleh pengaturan cloud yang tidak aman atau kesalahan pengguna dalam mengatur izin akses. Sebagai ilustrasi, beberapa

perusahaan pernah mengalami kebocoran data pelanggan karena penyimpanan informasi di cloud yang tidak dilindungi dengan baik.

Selain itu, serangan DDoS, yang merupakan serangan dengan mengirimkan lalu lintas berlebihan ke server cloud, juga menjadi ancaman yang serius, membuat layanan tidak dapat diakses oleh pengguna. Serangan ini dapat memberikan dampak besar pada operasi bisnis, terutama jika cloud digunakan untuk menjalankan aplikasi atau sistem yang penting. Selain itu, kelemahan pada API dan antarmuka cloud sering dimanfaatkan oleh hacker untuk mendapatkan akses ilegal ke sistem.

Misalnya, beberapa perusahaan mengalami masalah akibat eksploitasi API karena pengaturan otorisasi yang tidak ketat. Ancaman dari dalam organisasi, seperti tindakan tidak etis dari karyawan atau orang dalam lainnya, juga perlu diwaspadai karena mereka dapat menyalahgunakan akses untuk mengambil atau merusak data. Sebagai contoh, ada situasi di mana seorang karyawan menghapus data penting setelah dipecat. Kesalahan dalam pengaturan cloud juga merupakan penyebab umum dari kebocoran data, biasanya akibat kurangnya pemahaman dari pengguna tentang cara mengamankan lingkungan cloud.

### 3.2.2 Strategi dan Solusi Keamanan Cloud

Untuk menghadapi ancaman keamanan yang ada dalam cloud computing, terdapat berbagai pendekatan dan solusi yang bisa diimplementasikan untuk melindungi data serta sistem. Salah satu tindakan yang utama adalah penerapan enkripsi untuk data, baik saat disimpan maupun saat dikirim. Dengan enkripsi, data akan tetap tidak bisa dibaca oleh pihak yang tidak berhak meskipun berhasil dicuri.

Selain itu, penerapan otentikasi multi-faktor (MFA) sangat krusial untuk memastikan bahwa hanya pengguna yang resmi yang dapat mengakses sistem cloud tersebut. Alat untuk mendeteksi intrusi dan firewall juga bisa dimanfaatkan untuk menghalangi akses yang tidak sah dan memblokir aktivitas yang mencurigakan secara langsung. Selain teknologi, praktik keamanan yang baik juga harus dijalankan.

Contohnya, melakukan pemantauan dan audit keamanan secara rutin sangat penting untuk menemukan kemungkinan celah keamanan sebelum digunakan oleh orang yang tidak bertanggung jawab. Pelatihan bagi karyawan juga sangat penting guna meningkatkan pemahaman tentang risiko keamanan, seperti phishing atau kesalahan dalam pengaturan.

### 3.2.3 Regulasi dan Kepatuhan Cloud Computing

Penggunaan cloud computing harus sesuai dengan peraturan dan standar keamanan yang ditetapkan di berbagai negara atau sektor tertentu. Salah satu peraturan yang paling dikenal adalah GDPR (Regulasi Perlindungan Data Umum), yang mengatur perlindungan data pribadi warga Uni Eropa. Organisasi atau perusahaan yang memanfaatkan cloud untuk menyimpan atau mengelola data pelanggan dari area tersebut diharuskan untuk mematuhi GDPR agar terhindar dari denda besar dan kehilangan reputasi.

Di Amerika Serikat, HIPAA (Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan) berfungsi sebagai standar untuk perlindungan data kesehatan, sedangkan PCI DSS (Standar Keamanan Data Industri Kartu Pembayaran) mengatur keamanan data terkait kartu pembayaran. Mematuhi peraturan ini tidak hanya berguna untuk melindungi data pelanggan, tetapi juga dapat meningkatkan kepercayaan dari konsumen dan mitra bisnis.

Penyedia layanan cloud biasanya menyediakan fitur-fitur kepatuhan yang membantu organisasi memenuhi syarat hukum, seperti enkripsi data, pencatatan aktivitas, dan audit keamanan. Namun, tanggung jawab utama tetap berada di pihak pengguna layanan cloud untuk memahami dan mematuhi semua peraturan yang relevan. Dengan adanya peningkatan peraturan global, organisasi perlu menjadikan kepatuhan sebagai bagian penting dari strategi keamanan cloud mereka (Giap *et al.*, 2020).

## 3.4 Masa Depan Cloud Computing

Cloud computing mengalami perkembangan yang sangat cepat, memberikan inovasi teknologi yang mengubah cara pandang orang, organisasi dan perusahaan berhubungan dengan data serta aplikasi.

### 3.4.1 Teknologi Baru dalam Cloud Computing

Cloud computing terus didorong oleh munculnya teknologi baru yang meningkatkan fungsi dan efisiensinya. Salah satu perkembangan penting adalah Edge Computing yang memungkinkan data diproses lebih dekat dengan sumbernya, sehingga mengurangi latensi dan meningkatkan kecepatan respons. Selain itu, Kecerdasan Buatan (AI) dan Machine Learning (ML) semakin banyak digunakan di cloud, membuat perusahaan mampu menganalisis data besar dan mengambil keputusan yang lebih baik.

Teknologi lain yang berkembang adalah serverless computing, di mana pengguna dapat menjalankan aplikasi tanpa harus mengelola server secara langsung. Hal ini memberikan lebih banyak fleksibilitas dan menurunkan biaya operasional. Selain itu, Quantum Computing mulai menunjukkan kemampuannya sebagai teknologi masa depan yang dapat berkolaborasi dengan cloud untuk memecahkan masalah rumit yang sulit ditangani oleh komputer biasa.

### 3.4.2 Masa Depan Cloud Computing

Masa depan teknologi cloud terlihat akan semakin terdesentralisasi dan terdistribusi. Dengan meningkatnya pemakaian Multi Cloud dan Hybrid Cloud, perusahaan-perusahaan akan mendapatkan lebih banyak kebebasan untuk memilih kombinasi layanan yang sesuai dengan kebutuhan mereka. Selain itu, adopsi cloud akan dipercepat oleh kehadiran 5G dan teknologi jaringan generasi baru, memungkinkan pengguna untuk mendapatkan layanan dengan kecepatan jauh lebih tinggi dan latensi yang lebih rendah.

Aspek keamanan menjadi hal utama di masa depan, dengan teknologi seperti enkripsi canggih dan blockchain mulai diintegrasikan ke dalam

solusi cloud untuk melindungi data dari ancaman yang semakin rumit. Di sisi lain, otomatisasi serta sistem perbaikan mandiri akan menjadi hal biasa, di mana sistem cloud bisa mendeteksi dan menyelesaikan masalah secara otomatis tanpa perlu campur tangan manusia. Secara keseluruhan, cloud computing akan terus berkembang menjadi fondasi utama teknologi global, mendukung inovasi dan efisiensi di semua sektor.

### 3.4.3 Cloud Computing dan Transformasi Digital

Cloud computing memiliki peranan yang sangat penting dalam memfasilitasi transformasi digital di berbagai sektor. Dengan memberi kemudahan akses ke sumber daya komputasi yang dapat disesuaikan dan diperluas, teknologi cloud memungkinkan perusahaan untuk cepat berinovasi dan lebih responsif terhadap perubahan pasar.

Sebagai contoh, perusahaan dapat memanfaatkan teknologi cloud untuk menerapkan alat seperti Internet of Things (IoT), analisis Big Data, dan Augmented Reality (AR), yang semuanya membutuhkan komputasi yang besar serta penyimpanan data yang aman. Di samping itu, cloud mendukung gaya kerja yang modern, termasuk kerja jarak jauh dan kerjasama tim antar lokasi, yang semakin penting di zaman digital saat ini. Dengan cloud, para pekerja dapat mengakses informasi dan aplikasi dari berbagai lokasi, yang dapat meningkatkan produktivitas serta fleksibilitas.

Transformasi digital yang didorong oleh cloud tidak hanya menguntungkan perusahaan besar tetapi juga Usaha Kecil Menengah (UKM), yang dapat menggunakan teknologi ini untuk bersaing di level global tanpa harus mengeluarkan banyak biaya untuk infrastruktur teknologi. Oleh karena itu, cloud computing akan terus menjadi pendorong utama dalam proses transformasi digital di seluruh dunia.

Cloud computing merupakan teknologi yang menawarkan layanan komputasi melalui internet, dengan tiga model utama yaitu Infrastructure as a Service (IaaS), Platform as a Service (PaaS), dan Software as a Service (SaaS). IaaS menyediakan infrastruktur virtual seperti server, penyimpanan, dan jaringan yang fleksibel dan hemat biaya, sementara PaaS

memungkinkan pengembangan aplikasi tanpa harus mengelola infrastruktur fisik. SaaS, yang paling umum digunakan, memberikan aplikasi siap pakai yang dapat diakses dari mana saja, seperti Google Workspace dan Microsoft Office 365.

Keamanan menjadi tantangan utama dalam cloud computing, dengan ancaman seperti kebocoran data, serangan DDoS, dan kesalahan konfigurasi, sehingga strategi seperti enkripsi, otentikasi multi-faktor, dan regulasi seperti GDPR dan HIPAA sangat penting. Masa depan cloud computing akan semakin terdesentralisasi dan didukung oleh teknologi baru seperti Edge Computing, AI, 5G, dan Quantum Computing yang akan meningkatkan efisiensi dan inovasi. Cloud computing juga memainkan peran sentral dalam transformasi digital, mendukung teknologi seperti IoT, Big Data, dan AR, serta memungkinkan gaya kerja modern seperti kerja jarak jauh, sehingga mendorong efisiensi dan inovasi di semua sektor.



# Bab 4

## Jenis – Jenis Cloud Computing

### 4.1 Public Cloud

Public Cloud (Cloud Publik) adalah model layanan cloud computing di mana infrastruktur dan sumber daya komputasi dikelola oleh penyedia layanan cloud dan disediakan untuk umum atau sejumlah besar pengguna. Layanan ini biasanya disediakan oleh penyedia besar seperti Amazon Web Services (AWS), Microsoft Azure, dan Google Cloud, yang memungkinkan individu dan perusahaan untuk menyewa sumber daya komputasi (seperti server, penyimpanan data, dan perangkat lunak) melalui internet. Dalam model Public Cloud, pengguna dapat mengakses layanan sesuai dengan kebutuhan mereka tanpa harus mengelola atau memelihara infrastruktur fisik (Kahn et al., 2022).

Public Cloud menawarkan akses ke berbagai layanan teknologi tanpa memerlukan investasi besar dalam perangkat keras dan pengelolaan sumber daya TI secara langsung. Pengguna hanya membayar untuk sumber daya yang mereka gunakan, dengan model pembayarannya yang fleksibel seperti "pay-as-you-go". Layanan ini umumnya tersedia dalam skala besar dan

dapat diakses melalui internet oleh siapa saja yang memiliki koneksi dan akun dengan penyedia layanan cloud (Soundararajan Guru, 2024).

### 4.1.1 Karakteristik Public Cloud

Public Cloud adalah model komputasi awan di mana layanan infrastruktur TI seperti penyimpanan data, daya komputasi, dan aplikasi disediakan oleh pihak ketiga melalui internet dan dapat diakses secara umum oleh berbagai pengguna. Layanan ini biasanya ditawarkan oleh penyedia besar seperti Amazon Web Services (AWS), Microsoft Azure, dan Google Cloud Platform (GCP). Public Cloud menjadi solusi yang populer karena kemudahannya dalam akses, skalabilitas tinggi, dan biaya yang relatif lebih rendah dibandingkan dengan pengelolaan infrastruktur sendiri.

Salah satu karakteristik utama Public Cloud adalah *shared infrastructure*, yang berarti bahwa sumber daya TI seperti server dan storage digunakan secara bersama-sama oleh banyak pelanggan (Ang et al., 2023). Meski begitu, penyedia cloud menggunakan teknologi virtualisasi dan sistem keamanan canggih untuk menjaga agar data dan layanan masing-masing pelanggan tetap terisolasi dan aman. Ini memungkinkan skala penggunaan yang sangat fleksibel, karena pengguna dapat menambah atau mengurangi sumber daya sesuai kebutuhan mereka dalam waktu singkat.

Skalabilitas dan elastisitas juga menjadi ciri khas dari Public Cloud. Sistem ini memungkinkan bisnis untuk mengelola beban kerja yang fluktuatif tanpa harus berinvestasi dalam perangkat keras tambahan. Misalnya, saat permintaan meningkat secara mendadak (seperti saat promo besar atau *peak season*), pengguna dapat meningkatkan kapasitas layanan mereka dengan cepat. Ketika beban menurun, kapasitas dapat diturunkan kembali, sehingga efisien secara biaya.

Selain itu, Public Cloud bersifat *on-demand* dan *pay-as-you-go*, artinya pengguna hanya membayar sumber daya yang mereka gunakan tanpa perlu melakukan pembelian infrastruktur permanen. Hal ini memberikan fleksibilitas dan efisiensi biaya yang tinggi, terutama bagi startup, UKM, atau organisasi yang ingin menghindari beban biaya investasi awal.

Terakhir, Public Cloud mendukung aksesibilitas global dan kolaborasi real-time. Karena layanan disediakan lewat internet, pengguna dari berbagai lokasi geografis dapat mengakses sistem yang sama, bekerja bersama dalam dokumen atau aplikasi yang tersinkronisasi, dan memanfaatkan jaringan pusat data global untuk meningkatkan kecepatan dan reliabilitas akses.

### 4.1.2 Keuntungan Penggunaan Public Cloud

Salah satu keuntungan utama dari penggunaan public cloud adalah pengurangan biaya yang signifikan dalam hal infrastruktur teknologi informasi. Pengguna tidak perlu lagi membeli perangkat keras atau perangkat lunak yang mahal, karena penyedia layanan cloud sudah menyediakan sumber daya yang dibutuhkan. Dengan model pembayaran berbasis pemakaian (pay-as-you-go), perusahaan hanya membayar untuk apa yang mereka gunakan, membuatnya lebih efisien dalam hal pengelolaan anggaran.

Public cloud juga menawarkan skalabilitas yang sangat tinggi, memungkinkan pengguna untuk menyesuaikan kapasitas sesuai dengan kebutuhan secara fleksibel. Ketika permintaan meningkat, perusahaan dapat dengan cepat menambah kapasitas komputasi atau penyimpanan, dan sebaliknya, dapat mengurangnya ketika tidak diperlukan. Hal ini memberikan keuntungan besar dalam hal efisiensi operasional dan menghindari pemborosan sumber daya.

Akses yang mudah dan global merupakan keuntungan lain dari public cloud. Dengan hanya membutuhkan koneksi internet, pengguna dapat mengakses data dan aplikasi dari mana saja, yang mendukung kolaborasi antar tim yang tersebar di berbagai lokasi. Selain itu, penyedia cloud terus memperbarui dan mengembangkan layanan mereka, memberi pelanggan akses ke teknologi terbaru tanpa biaya tambahan. Ini memungkinkan perusahaan untuk selalu berada di garis depan dalam hal inovasi tanpa perlu berinvestasi dalam perangkat keras atau perangkat lunak baru.

### 4.1.3 Tantangan Penggunaan Public Cloud

Meski menawarkan banyak manfaat, penggunaan public cloud juga menghadirkan beberapa tantangan, terutama dalam hal keamanan dan privasi data. Data yang disimpan di server pihak ketiga bisa menjadi sasaran serangan atau kebocoran, meskipun penyedia cloud biasanya mengimplementasikan teknologi keamanan yang canggih. Namun, risiko tersebut tetap ada, dan perusahaan perlu memastikan bahwa data mereka terlindungi dengan baik, serta mematuhi standar keamanan yang ketat (Hajare et al., 2021).

Ketergantungan pada penyedia layanan cloud juga menjadi tantangan. Jika penyedia mengalami masalah teknis atau downtime, perusahaan yang bergantung pada cloud tersebut bisa mengalami gangguan operasional. Selain itu, peralihan dari satu penyedia cloud ke penyedia lain bisa menjadi hal yang rumit dan mahal, terutama karena adanya masalah vendor lock-in, di mana data dan aplikasi sulit dipindahkan.

Masalah kepatuhan dan regulasi juga perlu diperhatikan (Rizal et al., 2022), terutama bagi perusahaan yang beroperasi di sektor yang teratur secara ketat. Beberapa penyedia public cloud mungkin tidak dapat memenuhi persyaratan hukum atau industri tertentu, yang dapat menimbulkan risiko bagi perusahaan. Selain itu, meskipun cloud menawarkan banyak fleksibilitas, beberapa aplikasi atau kebutuhan infrastruktur mungkin memerlukan tingkat kustomisasi yang tidak dapat dipenuhi oleh solusi public cloud standar (Ilahi et al., 2024).

Akhirnya, meskipun public cloud menawarkan kinerja yang baik, masalah latensi dan kinerja mungkin terjadi, terutama ketika data harus diproses atau ditransfer ke lokasi yang jauh dari pusat data penyedia cloud. Hal ini dapat memengaruhi aplikasi yang membutuhkan waktu respons yang sangat cepat atau pengolahan data dalam jumlah besar.

### 4.1.4 Infrastruktur Perangkat Keras

Server Server merupakan komponen utama dalam infrastruktur public cloud, yang menyediakan daya komputasi untuk menjalankan aplikasi dan

layanan. Server ini biasanya dikelompokkan dalam pusat data besar yang terletak di berbagai lokasi geografis. Server harus memiliki kapasitas pemrosesan yang cukup untuk menangani beban kerja yang besar dan dapat diskalakan sesuai kebutuhan pengguna (Garg et al., 2022).

Penyimpanan Data (Storage) Infrastruktur penyimpanan data dalam cloud dapat berupa disk keras (HDD) atau solid-state drive (SSD) yang digunakan untuk menyimpan data pengguna. Penyimpanan cloud harus mampu menangani jumlah data yang sangat besar dan memberikan kecepatan akses yang tinggi. Penggunaan teknologi seperti storage area networks (SAN) dan network-attached storage (NAS) sangat umum dalam pengelolaan penyimpanan untuk mendukung fleksibilitas dan skalabilitas.

Jaringan (Networking) Jaringan adalah aspek krusial dalam membangun layanan cloud, karena menghubungkan berbagai server, perangkat penyimpanan, dan pusat data dengan pengguna. Infrastruktur jaringan cloud harus memiliki kapasitas bandwidth tinggi dan latensi rendah agar layanan dapat diakses dengan cepat dan tanpa gangguan. Penggunaan teknologi seperti virtual private network (VPN), load balancer, dan content delivery networks (CDN) sering digunakan untuk mengoptimalkan jaringan dan mengurangi latensi.

Perangkat Keras Pendukung Lainnya Selain server, penyimpanan, dan jaringan, perangkat keras lain yang dibutuhkan meliputi sistem pendingin untuk mencegah overheating pada server, serta sistem daya cadangan untuk memastikan layanan tetap beroperasi jika terjadi gangguan listrik. Pusat data juga dilengkapi dengan sistem keamanan fisik untuk melindungi perangkat keras dari ancaman fisik seperti pencurian atau kebakaran.

Infrastruktur Perangkat Lunak:

1. Sistem Operasi (Operating System)

Sistem operasi adalah perangkat lunak yang mengelola perangkat keras dan menyediakan platform untuk aplikasi dan layanan cloud berjalan. Penyedia layanan cloud menggunakan berbagai sistem operasi, seperti Linux, Windows Server, atau sistem operasi

berbasis Unix untuk mendukung aplikasi dan beban kerja mereka. Sistem operasi ini juga harus mampu mendukung virtualisasi, yang memungkinkan pengalokasian sumber daya secara dinamis.

## 2. Platform Virtualisasi

Virtualisasi adalah komponen penting dalam layanan cloud, memungkinkan penyedia cloud untuk membagi sumber daya fisik menjadi beberapa instansi virtual yang lebih kecil dan terisolasi. Teknologi virtualisasi seperti VMware, KVM (Kernel-based Virtual Machine), atau Hyper-V digunakan untuk membuat mesin virtual (VM) yang menjalankan aplikasi di cloud (Firdha Aisyah et al., 2022). Dengan virtualisasi, pengguna dapat memanfaatkan sumber daya secara efisien dan mengelola beban kerja dengan lebih fleksibel.

## 3. Manajemen dan Orkestrasi

Platform manajemen dan orkestrasi memungkinkan penyedia cloud untuk mengelola sumber daya secara efisien dan memastikan bahwa layanan dapat disediakan secara otomatis. Alat orkestrasi seperti Kubernetes (untuk aplikasi berbasis kontainer) dan OpenStack (untuk pengelolaan infrastruktur cloud) memungkinkan pengelolaan otomatis dari aplikasi, sumber daya komputasi, dan penyimpanan. Ini juga memastikan bahwa sumber daya dapat disesuaikan dengan kebutuhan pengguna secara otomatis.

## 4. Keamanan dan Pengelolaan Akses

Perangkat lunak keamanan sangat penting dalam layanan public cloud untuk melindungi data dan aplikasi dari ancaman. Ini mencakup enkripsi data, kontrol akses berbasis identitas, firewall, serta alat untuk memantau dan mendeteksi ancaman (misalnya, Intrusion Detection System/IDS). Selain itu, penyedia cloud juga

mengimplementasikan alat untuk memastikan bahwa pengguna dan administrator memiliki akses yang tepat dan dapat memitigasi potensi pelanggaran keamanan.

#### 5. Middleware dan API

Middleware adalah lapisan perangkat lunak yang berada antara sistem operasi dan aplikasi, yang memungkinkan aplikasi untuk berkomunikasi dengan layanan cloud dan sumber daya lainnya. Application Programming Interfaces (API) sangat penting dalam cloud, karena memungkinkan integrasi antara aplikasi pengguna dengan layanan cloud seperti penyimpanan, komputasi, dan jaringan. Penyedia cloud biasanya menawarkan API untuk memungkinkan pengembang mengotomatisasi dan mengelola layanan cloud mereka (Namruddin et al., 2025).

#### 6. Layanan dan Aplikasi

Layanan perangkat lunak seperti penyimpanan file, analitik data, komputasi berbasis cloud (misalnya, mesin virtual atau kontainer), dan aplikasi berbasis SaaS (Software as a Service) adalah bagian integral dari platform cloud. Layanan ini harus didesain untuk berjalan secara efisien di infrastruktur cloud dan mampu menangani permintaan pengguna dengan skalabilitas yang tinggi.

#### 7. Pusat Data dan Pengelolaan Infrastruktur

Pusat data adalah fasilitas fisik tempat penyedia cloud menyimpan semua perangkat keras dan infrastruktur yang diperlukan untuk menyediakan layanan cloud. Pusat data ini harus dilengkapi dengan sistem keamanan fisik yang kuat, seperti pengawasan 24/7, akses terbatas, dan perlindungan terhadap bencana. Penyedia layanan cloud sering memiliki pusat data di berbagai lokasi geografis untuk memastikan redundansi dan ketahanan layanan

### **Contoh pemanfaatan Public Cloud**

Sebuah perusahaan rintisan (startup) di bidang e-commerce ingin memperluas jangkauan pemasarannya ke seluruh wilayah Indonesia. Untuk menunjang kebutuhan operasional dan memastikan performa situs web serta aplikasi yang optimal, perusahaan tersebut memutuskan memanfaatkan layanan Public Cloud seperti AWS, Microsoft Azure, atau Google Cloud Platform. Melalui pilihan ini, mereka dapat meng-host situs web dan aplikasi secara mudah, menyimpan basis data produk dan pelanggan, serta mengelola sistem transaksi yang aman dan andal.

Ketersediaan sumber daya di Public Cloud juga memungkinkan mereka memproses data dalam skala besar (big data) untuk menganalisis perilaku pelanggan secara real-time, mulai dari preferensi produk hingga pola pembelian, guna menyusun strategi pemasaran yang lebih efektif.

Salah satu keunggulan paling menonjol dalam pemanfaatan Public Cloud adalah efisiensi biaya. Dengan menerapkan skema bayar sesuai penggunaan (pay-as-you-go), perusahaan dapat menekan pengeluaran awal untuk infrastruktur fisik. Mereka tidak perlu membeli server, perangkat jaringan, ataupun merancang data center yang mahal. Kapasitas komputasi pun dapat ditingkatkan atau diturunkan sesuai kebutuhan. Ketika volume transaksi sedang tinggi, penambahan sumber daya untuk menjaga kinerja situs bisa dilakukan tanpa proses rumit. Sebaliknya, saat penjualan menurun, beban infrastruktur dapat dikurangi sehingga pengeluaran menjadi lebih terkendali.

Selanjutnya, pemeliharaan dan pembaruan perangkat keras serta perangkat lunak tidak lagi menjadi beban utama tim teknis di perusahaan rintisan tersebut. Penyedia Public Cloud memiliki tanggung jawab untuk menjaga performa server, melakukan pembaruan sistem, dan memastikan keamanan fisik data center. Hal ini memberi kesempatan kepada tim internal perusahaan untuk lebih fokus pada pengembangan produk inti dan inovasi layanan, ketimbang menyita waktu mereka untuk mengurus kerumitan infrastruktur. Dampaknya, proses adaptasi pasar dan peningkatan mutu layanan dapat berjalan lebih gesit.

Dari segi aksesibilitas, Public Cloud memberikan kemudahan dan jangkauan global. Pengguna atau pelanggan dapat mengakses layanan e-commerce dari mana saja dengan waktu respons yang lebih cepat, berkat jaringan data center yang tersebar di berbagai wilayah. Selain itu, jaminan ketersediaan layanan (service availability) juga tinggi karena penyedia Public Cloud biasanya menandatangani perjanjian level layanan (Service Level Agreement/SLA) dengan tingkat uptime tertentu. Aspek ini sangat krusial bagi perusahaan e-commerce yang mengharapkan transaksi berlangsung secara terus-menerus tanpa kendala signifikan.

Terakhir, Public Cloud menawarkan beragam layanan penunjang yang dapat diintegrasikan dengan mudah, misalnya sistem kecerdasan buatan (AI), analitik prediktif, hingga platform IoT. Perusahaan rintisan tersebut tidak perlu membangun segalanya dari nol dan bisa langsung memanfaatkan ekosistem yang tersedia untuk mengembangkan fitur baru.

Keamanan juga menjadi prioritas yang dikelola oleh penyedia Public Cloud dengan protokol canggih, sehingga perlindungan data pelanggan maupun transaksi dapat terjaga. Dengan kombinasi seluruh aspek tersebut, penggunaan Public Cloud terbukti mendorong skala dan efisiensi bisnis secara signifikan, yang pada akhirnya membantu perusahaan memfokuskan energi pada inovasi produk demi memenangkan persaingan di pasar

## 4.2 Private Cloud

Private Cloud adalah model komputasi awan yang infrastruktur dan layanannya diperuntukkan secara eksklusif bagi satu organisasi atau perusahaan tertentu. Berbeda dengan Public Cloud yang sumber dayanya dibagikan untuk banyak pengguna, Private Cloud memberikan kendali penuh dan tingkat keamanan yang lebih tinggi karena seluruh lingkungan awan hanya digunakan oleh satu entitas (Golightly et al., 2022). Infrastruktur ini dapat dikelola secara internal oleh tim TI organisasi tersebut, atau dapat juga dikelola oleh pihak ketiga yang menyediakan

layanan khusus untuk perusahaan, asalkan akses dan sumber dayanya tetap terjaga hanya untuk organisasi tersebut.

Karena arsitektur Private Cloud dipusatkan pada satu organisasi, pengaturan jaringan, penyimpanan, dan sumber daya komputasinya dapat disesuaikan lebih fleksibel dengan kebutuhan bisnis serta kebijakan keamanan yang berlaku. Dengan kata lain, Private Cloud menghadirkan solusi yang memungkinkan organisasi memperoleh benefit komputasi awan—seperti skalabilitas dan efisiensi tanpa mengorbankan privasi dan kendali penuh atas data dan operasionalnya.

Karakteristik Private Cloud:

1. Eksklusivitas dan Kepemilikan Penuh

Salah satu karakteristik utama Private Cloud adalah akses yang terbatas untuk satu organisasi saja. Hal ini menjamin penguasaan penuh terhadap sumber daya, sehingga perusahaan dapat mengonfigurasi dan memonitor keamanan, kinerja, serta kepatuhan sesuai regulasi yang berlaku.

2. Keamanan dan Kepatuhan Tinggi

Karena sumber daya dan infrastruktur tidak dibagikan dengan pihak lain, risiko kebocoran data dapat ditekan lebih jauh. Organisasi dapat menentukan dan menerapkan kebijakan keamanan (misalnya enkripsi data, firewall, sistem deteksi intrusi) dengan lebih bebas. Selain itu, kepatuhan pada regulasi industri seperti ISO, HIPAA, atau GDPR dapat diimplementasikan dan diawasi dengan lebih ketat.

3. Pengelolaan dan Pemeliharaan Mandiri

Dalam Private Cloud, tanggung jawab untuk memelihara infrastruktur, memperbaiki perangkat lunak, serta menangani masalah teknis berada pada tim internal atau penyedia layanan khusus. Hal ini memungkinkan organisasi menyesuaikan setiap

aspek arsitektur cloud mereka dengan kebutuhan bisnis dan operasional. Namun, di sisi lain, organisasi perlu menyiapkan sumber daya dan keahlian TI internal yang memadai untuk menjaga kinerja dan keandalannya.

#### 4. Skalabilitas Internal

Meskipun sumber dayanya terbatas pada lingkungan internal, Private Cloud tetap memberikan kemampuan untuk menambah atau mengurangi kapasitas sesuai kebutuhan. Penggunaan virtualisasi dan otomatisasi memungkinkan perusahaan menyesuaikan beban kerja yang berubah-ubah tanpa harus melalui proses pengadaan infrastruktur fisik baru yang panjang dan berbiaya besar.

#### 5. Kostumisasi Fleksibel

Private Cloud dapat dirancang sesuai preferensi organisasi. Mulai dari sistem operasi, platform pengembangan, hingga perangkat lunak pendukung lainnya, semua dapat diatur dan diintegrasikan dengan proses bisnis yang sudah berjalan. Tingkat fleksibilitas ini memberikan keuntungan lebih bagi perusahaan yang memerlukan penyesuaian tinggi terhadap standar operasional dan arsitektur TI yang unik.

### 4.2.1 Keuntungan dan Kelemahan

Private Cloud, dengan infrastruktur dan layanannya yang didedikasikan khusus untuk satu entitas atau organisasi, memberikan jaminan kontrol dan keamanan yang lebih tinggi. Keuntungan ini sangat membantu perusahaan yang beroperasi di sektor sensitif, misalnya kesehatan atau keuangan, yang perlu mematuhi regulasi ketat terkait perlindungan data. Karena infrastruktur tidak dibagi dengan entitas lain, organisasi dapat secara leluasa menetapkan, menerapkan, dan memantau kebijakan keamanan sesuai kebutuhan.

Selain itu, pengaturan sumber daya bisa dioptimalkan untuk mengakomodasi aplikasi-aplikasi yang memerlukan kustomisasi khusus (Xu et al., 2024). Hal ini memudahkan tim TI dalam melakukan penyesuaian konfigurasi, mengelola beban kerja internal, serta memastikan kinerja sistem tetap stabil walaupun beban meningkat. Dengan memiliki kendali penuh atas infrastruktur, perusahaan pun memiliki fleksibilitas untuk melakukan inovasi secara lebih terstruktur dan aman.

Namun, penggunaan Private Cloud tidak lepas dari tantangan tersendiri. Salah satu kekurangannya adalah biaya awal yang relatif besar, karena perusahaan harus menyiapkan investasi untuk membangun dan memelihara infrastruktur fisik termasuk server, jaringan, dan data center. Biaya operasional ini juga mencakup gaji tenaga TI yang andal untuk mengelola sistem dan memperbarui teknologi agar tetap mutakhir. Selain itu, skalabilitas yang ditawarkan oleh Private Cloud umumnya tidak setinggi Public Cloud, sebab penambahan kapasitas masih dibatasi oleh sumber daya internal yang tersedia.

Proses penambahan server atau perangkat keras baru dapat memakan waktu dan biaya, sehingga perusahaan mesti cermat dalam merencanakan pertumbuhan dan mengelola beban kerja. Meski demikian, bagi organisasi yang memprioritaskan kendali dan keamanan, Private Cloud tetap menjadi pilihan unggul yang mampu menjawab kebutuhan bisnis yang sangat spesifik

#### **4.2.2 Infrastruktur Perangkat Keras dan Software**

Untuk membangun infrastruktur Private Cloud, sebuah organisasi memerlukan pondasi perangkat keras (hardware) dan perangkat lunak (software) yang kuat serta saling terintegrasi. Dari sisi hardware, elemen utamanya meliputi server fisik yang cukup tangguh untuk menampung beragam beban kerja, baik dari segi komputasi (CPU) maupun memori (RAM). Server-server ini umumnya ditempatkan di data center internal milik perusahaan atau lokasi colocation yang memiliki fasilitas penunjang

seperti pengaturan kelistrikan, pendingin (cooling system), dan sistem keamanan fisik yang memadai.

Di samping itu, jaringan (network) juga berperan penting. Perusahaan harus menyiapkan perangkat jaringan seperti switch, router, firewall, dan load balancer yang mampu menangani lalu lintas data dalam skala besar, sekaligus memastikan keamanan dan kualitas koneksi tetap terjaga. Penyimpanan data pun perlu diperhatikan, sehingga diperlukan sistem storage yang andal misalnya Network Attached Storage (NAS) atau Storage Area Network (SAN) serta mekanisme pencadangan (backup) dan pemulihan bencana (disaster recovery) untuk menjaga ketersediaan informasi.

Sementara itu, dari sisi software, pemanfaatan teknologi virtualisasi menjadi kunci untuk mengoptimalkan penggunaan sumber daya hardware. Hypervisor seperti VMware vSphere, Microsoft Hyper-V, atau KVM (Kernel-based Virtual Machine) digunakan untuk menciptakan lingkungan komputasi virtual yang dapat dijalankan di atas server fisik. Lingkungan virtual ini memungkinkan organisasi melakukan konsolidasi server, mempermudah proses skalabilitas, dan meningkatkan efisiensi pemanfaatan sumber daya.

Selain virtualisasi, perusahaan juga membutuhkan platform manajemen cloud yang dapat mengatur, memonitor, dan mengotomasi berbagai layanan infrastruktur. Contoh perangkat lunak manajemen cloud yang populer di kalangan Private Cloud adalah OpenStack, Apache CloudStack, atau solusi komersial semisal VMware vCloud Suite. Platform tersebut memfasilitasi pengelolaan sumber daya (komputasi, penyimpanan, dan jaringan) melalui antarmuka yang terpusat dan terintegrasi.

Agar operasional Private Cloud berjalan lancar, organisasi memerlukan juga lapisan manajemen dan orkestrasi yang menyeluruh. Perangkat lunak orkestrasi seperti Ansible, Chef, atau Puppet dapat digunakan untuk mengotomasi penerapan konfigurasi dan penerapan aplikasi di seluruh lingkungan cloud. Langkah ini membantu mengurangi risiko kesalahan

manusia, mempersingkat waktu pengaturan, dan meningkatkan konsistensi konfigurasi.

Tidak kalah pentingnya, mekanisme pemantauan (monitoring) dan logging yang andal juga harus dipasang untuk memastikan kinerja setiap komponen berjalan optimal. Solusi seperti Zabbix, Nagios, atau Prometheus dapat membantu tim TI mengawasi resource usage dan mendeteksi gangguan sedini mungkin. Dengan kombinasi hardware yang tepat dan software manajemen yang andal, perusahaan dapat membangun Private Cloud yang stabil, aman, serta mampu menyesuaikan diri dengan kebutuhan bisnis yang terus berkembang.

### 4.2.3 Contoh Penggunaan Private Cloud

Sebuah perusahaan manufaktur otomotif berskala besar memutuskan untuk membangun infrastruktur Private Cloud untuk menampung seluruh aplikasi pentingnya. Contohnya, aplikasi perencanaan sumber daya perusahaan (ERP), sistem manajemen rantai pasok (SCM), serta perangkat lunak desain berbasis Computer-Aided Design (CAD) yang dijalankan oleh para insinyur.

Dalam prosesnya, mereka mendirikan data center internal dengan rangkaian server fisik yang sudah dilengkapi teknologi virtualisasi dan platform manajemen cloud. Melalui Private Cloud tersebut, tim TI perusahaan mengatur, mengelola, serta mengamankan sumber daya komputasi agar dapat digunakan oleh seluruh divisi sesuai kebutuhan.

Pada tahap implementasi, perusahaan menerapkan mekanisme otomasi untuk penugasan sumber daya (resource allocation) dan penyeimbangan beban (load balancing). Hal ini memastikan setiap unit bisnis dapat mengakses layanan, menyimpan data, dan menjalankan aplikasi penting secara efisien tanpa berebut kapabilitas server.

Selain itu, departemen riset dan pengembangan produk (R&D) juga terbantu dengan kemudahan membuat, menguji, dan men-deploy lingkungan uji coba (development/test environment) baru dalam hitungan

menit. Dengan kata lain, seluruh ekosistem TI dalam organisasi tersebut berjalan dalam satu lingkup Private Cloud yang terintegrasi dan aman.

Membangun Private Cloud memberikan sejumlah manfaat krusial bagi perusahaan atau lembaga yang menginginkan kendali penuh atas infrastruktur teknologinya. Karena segala sumber daya hanya digunakan oleh satu entitas, privasi dan keamanan informasi dapat dijaga dengan lebih ketat. Kebebasan untuk melakukan kustomisasi juga menjadi nilai tambah, sebab setiap komponen dari konfigurasi server hingga manajemen jaringan dapat diatur sesuai dengan kebutuhan proses bisnis maupun regulasi yang berlaku.

Dengan kendali ini, konsistensi kinerja menjadi lebih terjamin, terlebih jika perusahaan menerapkan pemantauan yang terstruktur dan pemeliharaan berkala. Kolaborasi internal pun semakin lancar karena seluruh divisi mengakses platform yang sama, sehingga proses produksi hingga inovasi dapat dijalankan dengan lebih efektif.

Di sisi lain, penggunaan Private Cloud juga menyimpan tantangan yang tidak bisa diabaikan. Investasi awal yang dibutuhkan untuk membangun data center dan menyiapkan perangkat keras dapat tergolong besar, belum lagi biaya operasional untuk memastikan sistem selalu mutakhir dan aman. Skalabilitasnya pun terbatas karena peningkatan kapasitas bergantung pada penambahan server atau alat fisik lain, sehingga perusahaan harus cermat merencanakan pertumbuhan beban kerja.

Di samping itu, kompetensi tim TI menjadi kunci keberhasilan penerapan Private Cloud keterampilan dan ketersediaan sumber daya manusia sangat diperlukan agar pengelolaan sistem berjalan optimal. Terakhir, perusahaan juga bertanggung jawab penuh terhadap rencana pemulihan bencana, yang berarti persiapan backup dan disaster recovery harus dilakukan dengan matang agar infrastruktur tetap aman di tengah situasi darurat.

## 4.3 Hybrid Cloud

Hybrid Cloud merupakan model komputasi awan yang menggabungkan dua atau lebih infrastruktur cloud berbeda biasanya mencakup Private Cloud dan Public Cloud yang dikaitkan oleh teknologi standar maupun milik penyedia layanan. Dengan pendekatan ini, organisasi dapat memanfaatkan fleksibilitas dan skalabilitas tinggi yang ditawarkan Public Cloud, sekaligus menjaga kendali atas data atau aplikasi yang sensitif melalui Private Cloud. Model Hybrid Cloud sering dipilih oleh perusahaan yang ingin menyeimbangkan efisiensi biaya dan fleksibilitas, tetapi juga dihadapkan pada peraturan atau kebutuhan internal yang mewajibkan tingkat keamanan dan kontrol lebih ketat.

Karakteristik utama dari Hybrid Cloud terletak pada keberagaman platform dan integrasi yang mulus antara keduanya. Dalam satu sisi, Public Cloud menyediakan sumber daya komputasi yang dapat ditingkatkan kapasitasnya secara cepat sesuai kebutuhan. Sementara itu, Private Cloud mengelola data atau aplikasi kritis yang memerlukan perlindungan ekstra, serta memungkinkan kustomisasi yang lebih mendalam terhadap infrastruktur dan kebijakan keamanan.

Kedua lingkungan ini saling terhubung melalui jaringan dan mekanisme manajemen cloud yang terintegrasi, sehingga data dan beban kerja dapat berpindah secara dinamis. Berkat sifatnya yang adaptif, Hybrid Cloud memudahkan perusahaan untuk menempatkan aplikasi dan data pada platform yang paling sesuai, baik dari sisi keamanan, biaya, maupun performa operasional (Achar, 2021).

Hybrid Cloud memberi perusahaan fleksibilitas untuk menggabungkan kelebihan dari Private Cloud dan Public Cloud dalam satu lingkungan terintegrasi. Di satu sisi, aplikasi atau data yang bersifat sangat sensitif tetap bisa ditempatkan di infrastruktur Private Cloud agar keamanan dan kepatuhan terhadap regulasi terjamin. Pada saat yang sama, beban kerja yang bersifat sementara atau membutuhkan kapasitas besar secara

mendadak dapat dialihkan ke Public Cloud dengan biaya relatif lebih efisien.

Hal ini membuat alokasi sumber daya menjadi lebih adaptif dan ramping, karena perusahaan tidak perlu terus-menerus menyediakan infrastruktur fisik untuk menampung beban puncak yang terjadi sesekali. Dengan demikian, Hybrid Cloud mendorong inovasi dan kelincahan operasional, tanpa harus mengorbankan kontrol atau stabilitas pada layanan yang tergolong kritis.

Namun, penggunaan Hybrid Cloud juga diiringi berbagai tantangan teknis dan manajerial. Integrasi antara Private dan Public Cloud menuntut jaringan yang andal, sistem manajemen terpusat, serta orkestrasi yang mampu mengatur perpindahan beban kerja secara mulus. Kesalahan dalam pengaturan tersebut dapat memicu masalah latensi, inkonsistensi konfigurasi, hingga potensi ancaman keamanan jika data sensitif tidak ditangani dengan benar saat melewati batas-batas platform.

Selain itu, perusahaan perlu menanamkan investasi dalam keahlian tim TI dan teknologi pendukung guna memastikan setiap bagian dari Hybrid Cloud berfungsi selaras. Kegagalan dalam mengantisipasi tantangan ini dapat menghambat tercapainya efisiensi biaya dan fleksibilitas yang menjadi tujuan utama penerapan Hybrid Cloud

### 4.3.1 Contoh Penerapan Hybrid Cloud

Sebuah perusahaan perbankan besar memutuskan untuk mengadopsi model Hybrid Cloud untuk menjalankan berbagai layanannya. Misalnya, data dan aplikasi yang bersifat sensitif seperti informasi nasabah, transaksi keuangan, serta laporan kepatuhan pada regulator ditempatkan di Private Cloud yang dikelola di data center internal. Dengan cara ini, perusahaan dapat menjaga keamanan data secara ketat dan mematuhi regulasi keuangan yang menuntut kontrol penuh atas informasi sensitif.

Di sisi lain, kebutuhan komputasi bersifat dinamis, seperti analisis big data untuk memprediksi tren pasar atau pengembangan aplikasi baru, dialihkan

ke Public Cloud. Pendekatan ini memungkinkan perusahaan untuk dengan cepat meningkatkan kapasitas (misalnya saat melakukan simulasi beban transaksi tinggi) tanpa harus melakukan pengadaan perangkat keras baru.

### 4.3.2 Keuntungan yang Diperoleh

Menggabungkan Private Cloud dan Public Cloud dalam satu ekosistem memberi keluwesan (fleksibilitas) yang tinggi. Perusahaan dapat mengutamakan keamanan untuk data kritis di Private Cloud, sementara tetap memanfaatkan skalabilitas dan efisiensi biaya Public Cloud untuk kebutuhan yang lebih variatif. Model Hybrid Cloud semacam ini membuat proses bisnis lebih adaptif: beban kerja yang membutuhkan kapasitas besar namun tidak kritis dapat dengan mudah “dipinjamkan” ke Public Cloud.

Hal ini menghemat belanja modal (capital expenditure) karena perusahaan tidak perlu membeli atau menyewa server tambahan di data center internal yang barangkali hanya akan digunakan secara maksimal pada waktu-waktu tertentu saja. Selain itu, penggunaan Private Cloud dalam model Hybrid memberi jaminan bahwa proses inti (core processes) tetap dijaga dalam lingkungan yang dapat dikelola sepenuhnya, sehingga kepatuhan terhadap standar industri dan regulasi masih dapat diawasi secara ketat.

### 4.3.3 Tantangan Penggunaan Private Cloud dalam Hybrid Cloud

Di dalam arsitektur Hybrid Cloud, bagian Private Cloud tetap menghadirkan beberapa tantangan tersendiri. Pertama, investasi awal untuk membangun dan memelihara infrastruktur fisik (server, jaringan, sistem penyimpanan, hingga keamanan) cukup besar. Perusahaan juga perlu menyiapkan tenaga ahli TI yang mampu menangani kompleksitas pengelolaan dan pembaruan teknologi. Kedua, skalabilitas Private Cloud tidak semudah Public Cloud, karena penambahan kapasitas server atau penyimpanan mensyaratkan pengadaan perangkat keras baru proses yang membutuhkan waktu dan biaya.

Di samping itu, penanganan perpindahan (transfer) beban kerja atau data antara Private dan Public Cloud harus direncanakan secara teliti agar tidak menimbulkan celah keamanan atau menyebabkan lonjakan latensi. Jika tidak dikelola dengan baik, penggabungan dua lingkungan cloud ini justru dapat menimbulkan kompleksitas tambahan, baik dari segi keamanan maupun orkestrasi layanan. Meskipun demikian, bagi perusahaan yang memerlukan perlindungan data sekaligus menginginkan kecepatan serta keluwesan Public Cloud, Hybrid Cloud tetap menjadi pendekatan yang menarik dan strategis

## 4.4 Community Cloud

Community Cloud merupakan model komputasi awan di mana infrastruktur, platform, serta layanannya digunakan oleh sekelompok organisasi atau entitas yang memiliki kepentingan, tujuan, dan kebutuhan serupa. Biasanya, organisasi-organisasi ini beroperasi dalam sektor atau industri yang sama, sehingga mereka memiliki persyaratan keamanan, kepatuhan, dan tata kelola yang relatif mirip.

Dalam Community Cloud, sumber daya cloud dibangun secara bersama-sama baik dari segi pembiayaan maupun pengelolaannya untuk memenuhi kebutuhan kolektif anggota komunitas tersebut. Meskipun infrastruktur ini bisa dikelola oleh salah satu anggota atau pihak ketiga, aksesnya tetap terbatas hanya untuk organisasi yang menjadi bagian dari komunitas.

### 4.4.1 Karakteristik Community Cloud

Karakteristik pertama yang menonjol dalam Community Cloud adalah kesamaan kepentingan di antara para penggunanya. Karena lingkungan ini dirancang untuk menyokong kebutuhan spesifik, misalnya kepatuhan terhadap regulasi ketat di sektor keuangan, kesehatan, atau pemerintahan, setiap anggota komunitas memiliki prioritas yang relatif sama terhadap keamanan, ketersediaan layanan, dan integritas data. Dengan demikian,

Community Cloud dapat dioptimalkan untuk menyediakan mekanisme enkripsi, pengelolaan akses, serta pemantauan yang memenuhi standar industri tersebut.

Di samping itu, Community Cloud mengedepankan konsep kolaborasi dan efisiensi biaya. Dengan membangun infrastruktur secara kolektif, beban pengeluaran yang biasanya cukup besar dapat ditanggung bersama, sehingga setiap entitas bisa memperoleh layanan cloud berkualitas tanpa harus menanamkan modal sendiri-sendiri (N'Goran et al., 2023). Proses berbagi sumber daya ini juga mendorong adanya pertukaran pengetahuan dan praktik terbaik antaranggota komunitas.

Namun, karena komunitas ini bersifat tertutup dan memang ditujukan untuk kelompok organisasi tertentu, aspek skalabilitas serta fleksibilitasnya tidak seluas Public Cloud. Meski demikian, Community Cloud tetap menawarkan tingkat keamanan serta kustomisasi yang lebih tinggi bila dibandingkan dengan solusi umum yang dibagikan ke banyak pihak di luar komunitas.

#### 4.4.2 Alasan Pemilihan Penggunaan Community Cloud

Community Cloud biasanya diadopsi oleh sekelompok organisasi yang memiliki kepentingan, tujuan, serta persyaratan serupa baik dari segi regulasi, keamanan, maupun arsitektur TI. Misalnya, dalam sektor pemerintahan, terdapat standar kepatuhan dan keamanan yang ketat dan sama-sama berlaku bagi seluruh instansi. Membentuk infrastruktur Community Cloud memungkinkan setiap institusi memenuhi standar tersebut tanpa perlu membangun dan mengelola infrastruktur cloud sendiri-sendiri.

Selain itu, konsep saling berbagi biaya (*cost-sharing*) menekan pengeluaran total karena investasi untuk membangun fasilitas cloud dapat ditanggung oleh seluruh anggota komunitas. Hasilnya, setiap anggota dapat memanfaatkan layanan cloud dengan tingkat keamanan dan ketersediaan yang memadai, sambil tetap menjaga efisiensi finansial.

Organisasi juga memilih Community Cloud karena lingkungan ini menyediakan wadah yang lebih kondusif untuk berkolaborasi. Dalam satu ekosistem bersama, pengaturan hak akses, mekanisme enkripsi, serta prosedur backup dapat diselaraskan demi mencapai keseragaman standar pengelolaan data. Adanya kesamaan kebutuhan pun memungkinkan setiap anggota komunitas untuk saling berbagi praktik terbaik (best practices). Berkat kolaborasi tersebut, proses inovasi atau pengembangan fitur baru bisa dilakukan secara lebih cepat dan efektif, sebab seluruh pihak terlibat dalam membentuk fondasi teknis yang sama.

#### 4.4.3 Keuntungan Penggunaan Community Cloud

Salah satu keuntungan utama Community Cloud adalah peningkatan efisiensi biaya. Dengan membagi tanggungan pengadaan, pemeliharaan, dan peningkatan infrastruktur cloud di antara seluruh anggota komunitas, setiap organisasi bisa mendapatkan sumber daya yang lebih canggih dan tangguh dibanding jika mereka berusaha membangunnya sendiri. Selain itu, pengelolaan dan administrasi cloud dapat menjadi lebih efektif karena para anggota memiliki persyaratan dan target kinerja yang serupa mulai dari keamanan hingga kapasitas penyimpanan. Hal ini memudahkan proses koordinasi serta penerapan kebijakan yang terpusat.

Keuntungan lainnya ialah tingginya tingkat kustomisasi dan keamanan, hampir sebanding dengan Private Cloud. Karena Community Cloud ditujukan untuk sekelompok organisasi yang berada dalam ranah kepentingan yang sama, infrastruktur dan sistem keamanan dapat dioptimalkan sesuai kebutuhan khusus mereka.

Mekanisme enkripsi, sistem otentikasi, hingga level akses dapat disesuaikan untuk menjawab regulasi industri dan risiko keamanan tertentu yang dihadapi oleh komunitas tersebut. Semua ini memungkinkan Community Cloud menyatukan kelebihan Private Cloud dan efisiensi Public Cloud, namun tetap dalam lingkup komunitas yang lebih tertutup dan terstandarisasi.

#### 4.4.4 Tantangan dalam Penggunaan Community Cloud

Walau banyak menawarkan kelebihan, Community Cloud juga tak luput dari tantangan. Salah satu di antaranya adalah kerumitan koordinasi. Setiap organisasi dalam komunitas tentu memiliki struktur kepemimpinan, kebijakan TI, dan prosedur internal yang berbeda. Menyatukan semua kepentingan dalam satu kerangka kerja bisa menguras waktu dan energi, terutama ketika perlu menentukan standar dan pembagian tanggung jawab. Proses penetapan metode pembayaran, pembagian sumber daya, serta mekanisme pemecahan masalah juga perlu dirumuskan secara jelas agar setiap anggota merasa diuntungkan.

Selain itu, aspek skalabilitas Community Cloud tidak setinggi Public Cloud. Meskipun kolaboratif, penambahan kapasitas atau perubahan teknologi besar sering kali memerlukan diskusi dan kesepakatan di antara anggota komunitas. Bila satu pihak ingin mengembangkan fitur khusus atau menambah kapasitas secara sepihak, hal itu mungkin terkendala oleh sumber daya atau kesepakatan yang sudah ditetapkan bersama.

Dari sisi teknis, pemeliharaan infrastruktur juga bisa menjadi tantangan jika keahlian dan komitmen setiap anggota komunitas tidak merata. Oleh karena itu, suksesnya implementasi Community Cloud bergantung pada kemampuan anggota komunitas dalam berkolaborasi secara efisien, mengelola kepentingan bersama, dan merencanakan strategi pengembangan jangka panjang.

# Bab 5

## Arsitektur Cloud Computing

### 5.1 Pendahuluan

Arsitektur Cloud merupakan kerangka konsep dan rancangan yang mengatur bagaimana sumber daya komputasi seperti server, penyimpanan data, dan jaringan diintegrasikan dan dikelola dalam lingkungan komputasi awan. Dalam kerangka ini, penyedia layanan cloud menyatukan seluruh infrastruktur fisik di data center yang tersebar secara geografis, lalu menempatkan lapisan virtualisasi di atasnya.

Lapisan virtualisasi memecah sumber daya fisik menjadi beragam mesin virtual atau kontainer, sehingga dapat disewakan atau diakses secara fleksibel oleh para pengguna. Mekanisme pengelolaan ini ditunjang oleh teknologi orkestrasi yang berperan dalam mengatur otomatisasi penugasan, pemantauan, dan pembaruan sumber daya, agar kapasitas dapat disesuaikan dengan kebutuhan secara tepat waktu.

## 5.2 Infrastruktur Konvensional

Server on-premise mengharuskan organisasi mengelola seluruh infrastruktur fisik meliputi server, storage, jaringan, dan fasilitas data center di lokasi mereka sendiri. Tim TI internal bertanggung jawab atas keamanan fisik, pemeliharaan, serta pemantauan seluruh perangkat keras. Sebaliknya, arsitektur cloud menjalankan infrastruktur di data center milik penyedia layanan (seperti AWS, Azure, atau GCP), di mana pengguna cukup menyewa sumber daya dan mengelola lingkup layanan (IaaS, PaaS, atau SaaS) yang dibutuhkan, tanpa harus memikirkan detail operasional perangkat keras.

Keuntungan utama dari infrastruktur on-premise adalah kendali penuh atas seluruh aset dan konfigurasi teknis. Hal ini memberikan kelonggaran untuk menyesuaikan infrastruktur dengan kebutuhan bisnis yang sangat spesifik, termasuk kebijakan keamanan khusus atau kepatuhan pada regulasi tertentu. Dari sisi keamanan, beberapa organisasi merasa lebih nyaman karena dapat mengelola akses fisik dan prosedur pengamanan secara langsung, terutama di sektor yang sangat diatur, seperti keuangan atau pemerintahan (Gaianu, 2023).

Namun, menerapkan infrastruktur on-premise memerlukan investasi awal yang besar untuk pengadaan perangkat keras, pembangunan ruangan server, dan pengadaan pendingin atau daya cadangan. Selain itu, tim TI juga perlu menyiapkan keahlian untuk menangani perawatan, pembaruan, dan pemecahan masalah pada level perangkat keras maupun perangkat lunak. Proses skalabilitas seringkali berjalan lambat karena penambahan kapasitas berarti harus melakukan pengadaan fisik baru, yang memakan waktu dan biaya signifikan.

Di sisi lain, arsitektur cloud menawarkan fleksibilitas dan efisiensi biaya yang lebih baik berkat skema “pay-as-you-go.” Pengguna hanya membayar sumber daya yang benar-benar dipakai, sehingga belanja modal (capital expenditure) dapat ditekan (Soundararajan Guru, 2024). Skalabilitas dan elastisitas juga menjadi keunggulan, karena penambahan atau pengurangan

kapasitas dapat dilakukan dengan cepat melalui portal atau antarmuka pemrograman (API). Selain itu, tanggung jawab pemeliharaan perangkat keras dan pembaruan sistem sebagian besar ditangani oleh penyedia layanan cloud.

Meskipun demikian, pengguna arsitektur cloud memiliki kendali yang lebih terbatas atas konfigurasi dan pemeliharaan infrastruktur fisik. Bagi perusahaan yang memerlukan penyesuaian ekstrem, hal ini bisa menjadi hambatan. Dari sisi kepatuhan, terdapat pula potensi hambatan hukum atau regulasi yang melarang data keluar dari wilayah tertentu. Di samping itu, arsitektur cloud sangat bergantung pada koneksi internet; gangguan jaringan bisa menurunkan performa atau bahkan menghentikan operasional layanan.

## 5.3 Lapisan Arsitektur Cloud

Di dalam Arsitektur Cloud Computing, secara umum dapat diuraikan beberapa lapisan (layers) yang saling terkait untuk memberikan layanan komputasi awan kepada pengguna.

Meskipun penamaan dan urutan lapisan dapat sedikit berbeda dalam berbagai referensi (Khoer & Heryana, 2024), berikut adalah lapisan-lapisan yang paling umum beserta fungsinya:

1. Lapisan Fisik (Physical Layer)
  - a. Terdiri dari: Server fisik (CPU, RAM), perangkat penyimpanan (storage), jaringan (router, switch), dan fasilitas data center (kelistrikan, pendingin).
  - b. Fungsi: Menyediakan pondasi utama bagi seluruh layanan cloud. Infrastruktur fisik ini dikelola oleh penyedia layanan atau organisasi yang membangun cloud-nya sendiri (dalam kasus Private Cloud). Keandalan, skalabilitas, dan keamanan data center sangat memengaruhi kinerja keseluruhan sistem cloud.

2. Lapisan Virtualisasi (Virtualization Layer)
  - a. Terdiri dari: Hypervisor (misalnya VMware, Hyper-V, KVM), container runtime (Docker, containerd), serta komponen pendukung virtualisasi (network & storage virtualization).
  - b. Fungsi: Memisahkan (abstraction) sumber daya fisik menjadi mesin virtual atau kontainer yang lebih mudah dikelola. Lapisan ini memungkinkan penggunaan sumber daya menjadi lebih efisien, karena beberapa lingkungan virtual dapat berjalan di atas satu perangkat keras fisik.
3. Lapisan Orkestrasi dan Manajemen (Orchestration & Management Layer)
  - a. Terdiri dari: Platform manajemen cloud (misalnya OpenStack, CloudStack, atau solusi dari penyedia cloud), alat orkestrasi (Kubernetes, Ansible, Terraform), serta modul pemantauan (monitoring tools seperti Prometheus, Nagios, Zabbix).
  - b. Fungsi: Mengatur proses penempatan (deployment) layanan, otomatisasi konfigurasi, pemantauan kinerja, serta pengelolaan lifecycle mesin virtual/kontainer. Di lapisan inilah skema otomatisasi seperti auto-scaling dan load balancing dikendalikan, sehingga lingkungan cloud dapat merespons perubahan beban kerja secara dinamis.
4. Lapisan Layanan (Service Layer)
  - a. Terdiri dari: Model layanan Cloud—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), dan Software as a Service (SaaS).
  - b. Fungsi: Menyediakan berbagai bentuk layanan kepada pengguna:

- 1) IaaS: Pengguna dapat mengatur sendiri sistem operasi dan aplikasi di atas server virtual, penyimpanan, dan jaringan yang sudah disediakan.
  - 2) PaaS: Pengguna fokus pada pengembangan dan penempatan aplikasi, sementara platform (sistem operasi, middleware, basis data) dikelola oleh penyedia.
  - 3) SaaS: Pengguna memanfaatkan aplikasi secara langsung (misalnya email, CRM, office suite) tanpa perlu mengurus instalasi atau pengelolaan server.
5. Lapisan Antarmuka/Front-End (Interface Layer)
- a. Terdiri dari: Portal web, API, CLI (Command Line Interface), atau GUI lain yang disediakan penyedia cloud.
  - b. Fungsi: Memberikan sarana bagi pengguna untuk berinteraksi dengan layanan cloud—membuat dan mengelola mesin virtual, menyimpan data, atau mengonfigurasi aplikasi. Lapisan ini juga meliputi mekanisme autentikasi, otorisasi, dan manajemen akun (identity management) bagi pengguna akhir.
6. Lapisan Keamanan (Security Layer) [Bersifat Lintas Lapisan]
- a. Terdiri dari: Firewall, sistem deteksi dan pencegahan intrusi, enkripsi, manajemen identitas dan akses (IAM), serta kebijakan kepatuhan (compliance)
  - b. Fungsi: Meskipun tidak selalu dinyatakan sebagai lapisan terpisah, keamanan merupakan aspek yang menyeluruh dan harus diterapkan di setiap lapisan—mulai dari fisik, virtualisasi, orkestrasi, hingga penggunaan aplikasi. Melalui mekanisme ini, integritas data, akses terkontrol, dan perlindungan terhadap ancaman siber dapat terjaga

## 5.4 Cara Kerja Arsitektur Cloud

Berikut adalah gambaran singkat mengenai cara kerja arsitektur cloud yang terdiri dari berbagai lapisan (layer) untuk memenuhi beragam fungsi dan layanan komputasi awan (Cantika Humendru, 2025).

Walaupun dapat bervariasi antara satu penyedia layanan dan yang lain, prinsip dasarnya kurang lebih sama:

1. Lapisan Fisik (Physical Layer)

Pada lapisan paling dasar, penyedia cloud mengoperasikan infrastruktur fisik di data center mereka, yang mencakup server (dengan CPU dan RAM), perangkat penyimpanan (storage), sistem kelistrikan, dan jaringan (router, switch). Selain itu, data center dilengkapi sistem pendingin, cadangan daya (UPS dan genset), serta sistem keamanan fisik (misalnya biometrik dan CCTV) untuk memastikan sumber daya fisik selalu tersedia dan terlindungi. Infrastruktur inilah yang nantinya menjadi pondasi bagi layanan cloud.

2. Lapisan Virtualisasi (Virtualization Layer)

Di atas infrastruktur fisik, penyedia cloud memasang perangkat lunak virtualisasi (hypervisor) yang memecah sumber daya fisik menjadi mesin virtual (VM) atau kontainer. Dengan demikian, sebuah server fisik dapat mendukung banyak lingkungan komputasi terisolasi. Virtualisasi juga mencakup abstraksi jaringan (Software-Defined Networking) dan penyimpanan (Software-Defined Storage). Melalui lapisan ini, penggunaan sumber daya menjadi efisien, serta memudahkan penyediaan (provisioning) dan pemindahan (migration) beban kerja antarserver.

### 3. Lapisan Orkestrasi dan Manajemen (Orchestration & Management Layer)

Setelah sumber daya berhasil di-virtualisasi, dibutuhkan alat orkestrasi dan manajemen untuk mengendalikan seluruh lingkungan tersebut. Di lapisan ini, platform manajemen cloud (seperti OpenStack atau sistem proprietary dari penyedia layanan) mengoordinasikan penugasan VM/kontainer, penyeimbangan beban (load balancing), hingga pemantauan (monitoring) sumber daya. Melalui orkestrasi, proses seperti auto-scaling dan otomatisasi penyebaran aplikasi dapat diterapkan, sehingga cloud dapat merespons dinamika permintaan dengan cepat tanpa intervensi manual yang rumit.

### 4. Lapisan Layanan (Service Layer)

Berbagai layanan cloud (IaaS, PaaS, SaaS) dijalankan di atas lapisan orkestrasi dan manajemen ini:

- a. Infrastructure as a Service (IaaS): Pengguna menyewa sumber daya dasar (VM, penyimpanan, jaringan) dan mengatur sistem operasi, aplikasi, serta keamanan di atasnya.
- b. Platform as a Service (PaaS): Penyedia cloud menyiapkan platform dan alat pengembangan (OS, runtime, database). Pengguna tinggal membangun, menguji, dan men-deploy aplikasi tanpa memikirkan manajemen infrastruktur.
- c. Software as a Service (SaaS): Penyedia cloud menyediakan aplikasi siap pakai (misalnya email, CRM, office suite), dan pengguna cukup memanfaatkan fitur-fiturnya melalui antarmuka web atau aplikasi klien.

### 5. Lapisan Antarmuka/Front-End (Interface Layer)

Ini adalah lapisan yang berinteraksi langsung dengan pengguna atau administrator, meliputi portal web, Command Line Interface

(CLI), maupun Application Programming Interface (API). Melalui antarmuka ini, pengguna dapat membuat VM baru, memantau pemakaian sumber daya, mengelola aplikasi, atau mengakses layanan SaaS. Lapisan front-end juga mencakup fitur autentikasi dan manajemen identitas (identity management), memastikan hanya pengguna sah yang bisa mengakses layanan.

6. Lapisan Keamanan (Security) [Lintas Lapisan]

Keamanan menembus semua lapisan dalam arsitektur cloud. Mulai dari pengamanan fisik data center, konfigurasi firewall dan sistem deteksi intrusi pada lapisan jaringan, enkripsi data pada lapisan penyimpanan, hingga pengaturan hak akses di lapisan aplikasi. Penyediaan mekanisme keamanan yang memadai di setiap layer memastikan integritas, kerahasiaan, dan ketersediaan data serta layanan cloud bagi para penggunanya.

## 5.5 Fungsi Arsitektur Cloud Computing

1. Penyediaan Layanan On-Demand

Arsitektur Cloud memungkinkan pengguna untuk memperoleh dan melepaskan sumber daya komputasi dengan cepat melalui antarmuka yang telah disediakan, seperti portal web atau API. Kemudahan ini mempercepat proses pengembangan aplikasi, percobaan layanan baru, ataupun penambahan kapasitas untuk menampung beban kerja yang meningkat (Setiawan et al., 2022).

2. Optimasi Penggunaan Sumber Daya

Melalui virtualisasi, sumber daya fisik yang besar dapat dibagi dan dikelola secara efisien, sehingga pemanfaatannya menjadi optimal dan tidak terbuang percuma. Selain itu, mekanisme orkestrasi

membantu memindahkan beban kerja dari satu server ke server lain secara otomatis untuk menjaga kestabilan dan performa.

### 3. Skalabilitas dan Elastisitas

Berkat pengaturan terpusat dan adanya teknologi otomatisasi, arsitektur Cloud mendukung kemampuan untuk menaikkan (scale up) atau menurunkan (scale down) kapasitas secara cepat. Hal ini memudahkan perusahaan dalam menghadapi lonjakan permintaan sesaat, misalnya saat musim promosi, tanpa harus menginvestasikan perangkat keras tambahan secara permanen.

### 4. Keamanan dan Ketersediaan Layanan

Arsitektur Cloud modern menempatkan keamanan di setiap lapisan, mulai dari perlindungan fisik data center hingga enkripsi data dan pengelolaan identitas pengguna. Keandalan pun ditingkatkan dengan menempatkan beban kerja di banyak zona atau wilayah (region) data center, sehingga layanan tetap berjalan bahkan jika terjadi gangguan di salah satu lokasi.

### 5. Mendukung Berbagai Model Layanan

Arsitektur Cloud dirancang agar dapat mendukung beberapa model layanan, seperti Infrastructure as a Service (IaaS), Platform as a Service (PaaS), dan Software as a Service (SaaS). Hal ini memungkinkan pengguna untuk memilih jenis layanan yang paling sesuai dengan kebutuhan, apakah hanya memerlukan server virtual (IaaS), lingkungan pengembangan (PaaS), atau aplikasi siap pakai (SaaS).

## 5.6 Prinsip Desain Arsitektur Cloud

Prinsip-prinsip desain arsitektur berfungsi sebagai pedoman untuk merancang sistem komputasi termasuk infrastruktur cloud agar memenuhi standar keandalan, kinerja, keamanan, dan efisiensi. Salah satu prinsip utama adalah desain modular (*modularity*), di mana komponen-komponen sistem dipisahkan menjadi bagian-bagian yang lebih kecil dan spesifik. Dengan cara ini, setiap modul dapat dikembangkan, diuji, dan dikelola secara independen tanpa memengaruhi keseluruhan sistem. Selain memudahkan penambahan fitur baru, pendekatan modular ini juga menekan risiko kegagalan sistem secara total; jika satu modul bermasalah, komponen lain tetap dapat beroperasi.

Selain modularitas, prinsip penting lain adalah skalabilitas (*scalability*) dan elastisitas (*elasticity*). Skalabilitas mengacu pada kemampuan sistem untuk menampung peningkatan jumlah pengguna atau permintaan (*workload*) tanpa menurunkan kinerja secara signifikan (Junaedy et al., 2024). Elastisitas menekankan pada kecepatan adaptasi infrastruktur dalam mengurangi atau menambah sumber daya secara otomatis, sesuai dengan kebutuhan. Prinsip-prinsip ini sangat relevan di lingkungan cloud, di mana beban kerja bisa berfluktuasi secara dinamis. Dengan menerapkan desain yang memprioritaskan skalabilitas dan elastisitas, perusahaan dapat memastikan layanan tetap responsif sekaligus menghindari biaya infrastruktur berlebih.

Reliabilitas (*reliability*) dan ketersediaan (*availability*) juga menjadi kunci dalam prinsip desain arsitektur. Reliabilitas berarti sistem dirancang agar toleran terhadap kegagalan, misalnya melalui replikasi data atau mekanisme *failover* yang otomatis. Sementara itu, ketersediaan merujuk pada kemampuan sistem untuk terus aktif dan dapat diakses oleh pengguna kapan pun dibutuhkan. Dengan menerapkan prinsip ini, sistem cloud mampu meminimalkan waktu henti (*downtime*) yang dapat mengganggu operasional bisnis (Ramsari & Ginanjar, 2022).

Di samping itu, keamanan (security) dan kepatuhan (compliance) tidak bisa diabaikan (Juliansyah & Afrianto, 2023). Arsitektur cloud perlu mendefinisikan mekanisme perlindungan data seperti enkripsi, manajemen identitas dan akses (IAM), serta pemisahan lingkungan (network segmentation). Semua langkah ini memastikan kerahasiaan dan integritas informasi terjaga, sekaligus membantu perusahaan memenuhi standar atau regulasi industri. Melalui penerapan prinsip keamanan sejak tahap perancangan, risiko kebocoran data atau serangan siber dapat ditekan sedini mungkin

## 5.7 Cloud Computing Life Cycle

Cloud Computing Life Cycle adalah rangkaian tahapan yang menuntun organisasi atau entitas bisnis dalam memanfaatkan komputasi awan secara efektif dan terukur. Proses ini dimulai dengan perencanaan (planning) yang bertujuan untuk mengidentifikasi kebutuhan spesifik, misalnya seberapa besar kapasitas yang harus disiapkan, model layanan (IaaS, PaaS, atau SaaS), serta jenis implementasi (Public, Private, Community, Hybrid) yang akan dipilih. Pada tahap awal ini, tim pengambil keputusan perlu menganalisis persyaratan bisnis, anggaran, serta risiko keamanan untuk memastikan inisiatif cloud selaras dengan strategi organisasi (Salem et al., 2020).

Tahap berikutnya adalah perancangan arsitektur (architecture design). Di sinilah kerangka teknis mulai dibentuk, mencakup pemilihan platform virtualisasi, sistem orkestrasi, dan susunan infrastruktur jaringan. Dalam konteks bab Arsitektur Cloud, aspek-aspek seperti desain jaringan (network design), pemilihan data center, dan konfigurasi penyimpanan (storage) mendapat penekanan khusus. Setiap komponen harus direncanakan agar dapat diintegrasikan secara mulus, termasuk menetapkan kebijakan auto-scaling dan mekanisme load balancing untuk menghadapi lonjakan beban .

Setelah rancangan selesai, organisasi memasuki tahap implementasi dan penyebaran (deployment). Di sini, tim teknis membangun atau

mengonfigurasi sumber daya cloud sesuai desain yang telah ditetapkan. Mereka menyiapkan server virtual, mengatur sistem keamanan (firewall, IAM), hingga memastikan bahwa aliran data di antara layanan berjalan stabil. Uji coba (testing) pun dilakukan pada skala kecil sebelum lingkungan cloud dibuka untuk produksi (go-live). Proses ini mencakup pemeriksaan reliabilitas, kinerja, serta kepatuhan terhadap standar yang berlaku misalnya keamanan data atau regulasi industri.

Ketika layanan mulai aktif digunakan, proses operasional dan pemantauan (operation & monitoring) menjadi fokus utama. Organisasi memanfaatkan alat pemantauan (monitoring tools) untuk mengevaluasi kondisi server, lalu lintas jaringan, dan penggunaan sumber daya. Jika terdeteksi anomali, tim TI harus segera melakukan tindakan korektif. Pada fase ini pula, penyesuaian kapasitas (scaling) bisa dilakukan secara otomatis atau manual guna menjaga performa sistem. Selain itu, pencadangan (backup), replikasi data, dan pemulihan bencana (disaster recovery) menjadi bagian penting untuk memastikan kontinuitas layanan (Alshazly et al., 2021).

Terakhir, tahap peningkatan dan evaluasi (upgrade & evaluation) menutup siklus sekaligus menjadi awal untuk siklus berikutnya. Tim TI dan manajemen meninjau kembali semua aspek, mulai dari kinerja aplikasi, efisiensi biaya, hingga keamanan. Berdasarkan hasil evaluasi, perbaikan desain arsitektur, pembaruan teknologi (misalnya adopsi kontainerisasi atau serverless), dan optimalisasi konfigurasi dilakukan untuk menghadapi tantangan baru. Dengan mengulangi seluruh proses secara iteratif, Cloud Computing Life Cycle menjamin infrastruktur cloud terus berkembang dan relevan, sekaligus mendukung pertumbuhan bisnis secara berkelanjutan

## 5.8 Referensi Arsitektur Cloud Computing

Referensi Arsitektur Cloud Computing adalah seperangkat panduan, pola desain, dan best practices yang membantu organisasi dalam merancang, mengimplementasikan, serta mengelola sistem komputasi awan. Dokumen atau kerangka referensi ini umumnya disusun oleh berbagai lembaga, seperti NIST (National Institute of Standards and Technology), Cloud Security Alliance (CSA), maupun vendor teknologi besar semisal AWS, Microsoft, dan Google (Chauhan & Shiaeles, 2023). Tujuan utamanya adalah memberikan kerangka konseptual yang terstandardisasi, sehingga para arsitek dan pengembang TI dapat membangun lingkungan cloud yang konsisten, aman, dan sesuai kebutuhan bisnis.

Salah satu contoh yang banyak diacu adalah NIST Cloud Computing Reference Architecture. Dalam kerangka ini, NIST mendefinisikan para pemangku kepentingan (cloud consumer, cloud provider, cloud broker, cloud carrier, dan cloud auditor), serta menjelaskan bagaimana interaksi di antara mereka terjadi. Pendekatan tersebut membantu perusahaan memahami peran masing-masing entitas dalam ekosistem cloud, termasuk menyoroti aspek keamanan, pengawasan, dan manajemen data yang perlu mendapat perhatian khusus. Dengan adanya standar rujukan semacam ini, implementasi cloud di lapangan dapat dijalankan dengan persepsi yang sama atas tanggung jawab dan proses teknisnya.

Selain NIST, Cloud Security Alliance turut menerbitkan referensi terkait aspek keamanan dalam arsitektur cloud, seperti CSA Security Guidance dan Cloud Controls Matrix (CCM). Dokumen-dokumen ini membahas langkah-langkah pengamanan di tiap lapisan, dari infrastruktur fisik hingga aplikasi dan data. Adapun dalam cakupan vendor, AWS menyediakan Well-Architected Framework, Microsoft menawarkan Azure Architecture Center, sementara Google Cloud memiliki Google Cloud Architecture Framework. Masing-masing memberikan rekomendasi dan praktik terbaik

(best practices), misalnya prinsip desain untuk skalabilitas, performa, efisiensi biaya, serta pengelolaan risiko.

Secara umum, referensi arsitektur cloud computing mencakup topik-topik mulai dari pemilihan model layanan (IaaS, PaaS, SaaS) dan model implementasi (Public, Private, Hybrid, Community), hingga penerapan keamanan, orkestrasi, dan otomatisasi. Referensi ini juga menekankan pentingnya pendekatan modular dan terukur (scalable), agar perusahaan dapat dengan mudah menyesuaikan kapasitas cloud sesuai permintaan bisnis yang dinamis. Dengan berpegangan pada kerangka acuan yang sudah diakui, organisasi dapat meminimalkan risiko kegagalan, menekan biaya operasional, dan memastikan bahwa solusi cloud yang dibangun selaras dengan standar industri serta praktik terbaik yang telah teruji

## 5.9 Load Balancing

Pendekatan load balancing dalam konteks komputasi awan merujuk pada upaya mengoptimalkan distribusi beban kerja atau lalu lintas (traffic) ke berbagai server, mesin virtual, maupun kontainer agar keseluruhan sistem berjalan lebih efisien dan andal. Dengan menempatkan load balancer di depan kumpulan sumber daya, setiap permintaan (request) dari pengguna akan dialirkan ke node atau instance yang paling siap, sehingga mencegah terjadinya penumpukan beban di satu titik. Pendekatan ini penting bagi aplikasi dengan banyak pengguna secara simultan seperti situs e-commerce, layanan streaming, dan platform media sosial karena dapat menjaga kecepatan respons dan meminimalkan risiko downtime (Denny et al., 2021).

Salah satu metode load balancing yang umum adalah round-robin, di mana permintaan dialihkan secara bergiliran ke setiap server yang tersedia. Metode ini efektif bila setiap node memiliki kapabilitas yang relatif sama. Namun, jika kondisi server beragam, pendekatan least connection atau least load menjadi lebih relevan, karena request akan dialirkan ke server dengan

sisia kapasitas atau jumlah koneksi paling rendah. Selain itu, load balancer modern juga mampu memeriksa kesehatan (health checks) setiap node, sehingga permintaan dapat dialihkan secara otomatis jika terdeteksi ada server yang mengalami gangguan. Hal ini meningkatkan reliabilitas sistem secara signifikan.

Dalam arsitektur cloud, load balancing bukan hanya bekerja di level komputasi atau server aplikasi, melainkan juga di level penyimpanan (storage) dan layanan lainnya. Banyak penyedia cloud seperti AWS, Google Cloud, dan Microsoft Azure menyertakan layanan load balancer terkelola (managed load balancing) yang memungkinkan pengguna mengonfigurasi aturan routing, SSL termination, serta skema failover dengan mudah. Pendekatan ini selaras dengan konsep auto-scaling, di mana jumlah instance bisa otomatis bertambah atau berkurang sesuai beban.

Ketika instance baru ditambahkan, load balancer akan mulai mendistribusikan permintaan ke node-node baru tersebut tanpa mengganggu proses yang sedang berjalan. Sebaliknya, jika beban kerja menurun, instance yang tidak lagi diperlukan dapat dihentikan, dan load balancer menyesuaikan pembagian lalu lintasnya.

Keuntungan utama pendekatan load balancing adalah peningkatan performa dan ketersediaan layanan. Aplikasi yang menggunakan load balancer dapat menyebarkan beban ke beberapa server, sehingga tidak mudah tumbang bila terjadi peningkatan lalu lintas mendadak atau ketika salah satu server mengalami kegagalan. Dari sisi bisnis, hal ini berimbas pada kepuasan pengguna yang lebih tinggi karena waktu respon lebih singkat dan downtime yang lebih jarang terjadi.

Meskipun demikian, penerapan load balancing memerlukan perencanaan yang matang terkait topologi jaringan, kapasitas server, serta strategi keamanan (misalnya enkripsi lalu lintas dan proteksi DDoS). Dengan demikian, pendekatan load balancing yang tepat menjadi salah satu elemen kunci untuk mewujudkan arsitektur cloud yang responsif, skalabel, dan andal.



# Bab 6

## Keamanan dalam Cloud Computing

### 6.1 Pendahuluan

Perkembangan teknologi informasi yang sangat pesat telah mendorong lahirnya berbagai inovasi dalam pengelolaan dan penyimpanan data, salah satunya adalah Cloud Computing. Teknologi Cloud Computing atau komputasi awan merupakan paradigma baru dalam pengelolaan sumber daya komputasi yang memungkinkan pengguna untuk mengakses layanan komputasi seperti penyimpanan data, aplikasi, dan infrastruktur secara virtual melalui jaringan internet (Mell & Grance, n.d.).

Dengan berbagai keunggulan seperti fleksibilitas, skalabilitas, dan efisiensi biaya, teknologi ini telah banyak diadopsi oleh perusahaan, institusi pendidikan, sektor pemerintahan, dan organisasi lainnya dalam menunjang operasional bisnis serta pengelolaan data digital. Namun, seiring dengan

semakin meluasnya penggunaan cloud computing, isu keamanan (security) menjadi salah satu tantangan utama yang harus dihadapi.

Keamanan dalam cloud computing mencakup berbagai aspek penting seperti kerahasiaan data (confidentiality), integritas data (integrity), ketersediaan layanan (availability), serta mekanisme autentikasi dan otorisasi (authentication & authorization) (Hashizume et al., 2013). Ancaman keamanan pada lingkungan cloud sangat beragam, mulai dari serangan peretasan (hacking), pencurian data (data breach), serangan Distributed Denial of Service (DDoS), hingga ancaman internal dari pengguna yang memiliki hak akses tertentu (Insider Threats).

Salah satu karakteristik unik dari cloud computing adalah sifat multi-tenant, di mana banyak pengguna atau organisasi menggunakan sumber daya cloud yang sama. Hal ini menimbulkan potensi ancaman baru seperti kebocoran data antar tenant (data leakage), penyalahgunaan sumber daya, serta serangan yang memanfaatkan kelemahan konfigurasi sistem cloud (Mai & Khalil, 2017). Selain itu, adanya ketergantungan pada penyedia layanan cloud (cloud service provider) dalam hal keamanan juga menimbulkan tantangan tersendiri, terutama terkait transparansi dalam pengelolaan keamanan dan kebijakan privasi data.

Upaya untuk meningkatkan keamanan dalam cloud computing terus berkembang melalui pengembangan teknologi kriptografi, pengamanan jaringan, sistem deteksi intrusi, serta penerapan manajemen risiko berbasis kebijakan keamanan. Implementasi enkripsi data baik saat penyimpanan (data at rest) maupun saat transmisi (data in transit) menjadi salah satu strategi utama dalam melindungi data pengguna di lingkungan cloud (Ali et al., 2015). Selain itu, teknologi seperti Multi-Factor Authentication, Zero Trust Architecture, serta penggunaan blockchain mulai diterapkan dalam meningkatkan keamanan dan kepercayaan pada layanan cloud.

Penelitian-penelitian terkini juga mengkaji penerapan Machine Learning dan Artificial Intelligence untuk mendeteksi dan memitigasi ancaman keamanan secara otomatis dalam lingkungan Cloud Computing. Dengan kemampuan untuk melakukan real-time monitoring dan anomaly

detection, teknologi ini diharapkan mampu meningkatkan ketahanan sistem terhadap ancaman yang semakin kompleks dan dinamis (Singh et al., 2016).

Berdasarkan uraian tersebut, penelitian mengenai keamanan dalam Cloud Computing sangat relevan untuk dikaji lebih lanjut, mengingat pentingnya perlindungan data dan layanan di era digital saat ini. Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan model keamanan Cloud Computing yang lebih adaptif, aman, dan sesuai dengan kebutuhan pengguna di berbagai sektor (Teo et al., 2018)

## 6.2 Konsep Dasar Cloud Computing

### 6.2.1 Definisi Cloud Computing

Cloud Computing atau komputasi awan adalah model layanan teknologi informasi yang menyediakan berbagai sumber daya komputasi — seperti server, penyimpanan data, aplikasi, dan layanan jaringan — melalui koneksi internet. Menurut National Institute of Standards and Technology (NIST), Cloud Computing didefinisikan sebagai:

*“A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (Mell & Grance, n.d.)*

Cloud Computing memungkinkan pengguna untuk mengakses layanan dan sumber daya teknologi tanpa harus memiliki atau mengelola infrastruktur fisik secara langsung. Hal ini menciptakan efisiensi biaya dan fleksibilitas tinggi dalam penggunaan sumber daya TI (Singh et al., 2016).

## 6.2.2 Karakteristik Utama Cloud Computing

Karakteristik Utama Cloud Computing Menurut NIST, Cloud Computing memiliki lima karakteristik utama yang membedakannya dari model komputasi tradisional, yaitu:



**Gambar 6.1:** Karakteristik Utama Cloud Computing

1. On-Demand Self-Service  
Pengguna dapat mengakses layanan komputasi sesuai kebutuhan secara mandiri, tanpa memerlukan interaksi manusia dengan penyedia layanan.
2. Broad Network Access  
Layanan cloud dapat diakses melalui jaringan internet menggunakan berbagai perangkat seperti laptop, smartphone, atau tablet.
3. Resource Pooling  
Sumber daya komputasi seperti server, penyimpanan, dan bandwidth dikelola secara dinamis dan melayani banyak pengguna (multi-tenancy).

#### 4. Rapid Elasticity

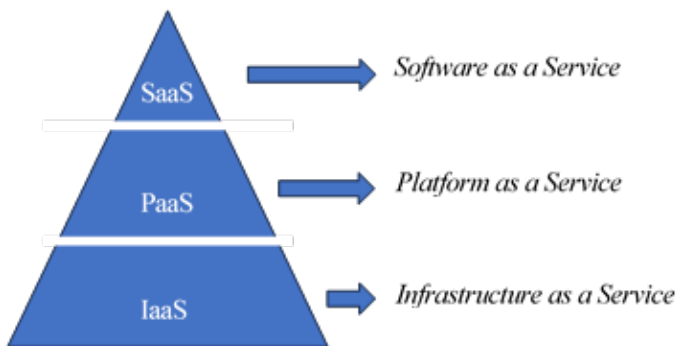
Kemampuan untuk melakukan skalabilitas sumber daya secara cepat sesuai kebutuhan pengguna, baik memperbesar maupun memperkecil.

#### 5. Measured Service

Penggunaan layanan cloud dimonitor, dikendalikan, dan dilaporkan sehingga dapat dilakukan sistem pembayaran berdasarkan pemakaian (pay-as-you-go).

### 6.2.3 Model Layanan Cloud Computing

Cloud Computing menyediakan tiga model layanan utama yang dikenal dengan istilah Cloud Service Models, yaitu:



**Gambar 6.2:** Model Layanan Cloud Computing

#### 1. Software as a Service (SaaS)

Layanan berbasis perangkat lunak yang diakses pengguna melalui internet tanpa perlu menginstalnya di perangkat lokal. Contoh: Google Workspace, Microsoft Office 365.

#### 2. Platform as a Service (PaaS)

Platform layanan yang memungkinkan pengguna untuk mengembangkan, menguji, dan menerapkan aplikasi tanpa

mengelola infrastruktur. Contoh: Google App Engine, Microsoft Azure.

3. Infrastructure as a Service (IaaS)

Menyediakan infrastruktur virtual seperti server, penyimpanan, dan jaringan kepada pengguna. Contoh: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform.

## 6.3 Jenis Ancaman Keamanan dalam Cloud Computing

Cloud Computing memiliki risiko keamanan yang kompleks dan dinamis karena sifatnya yang terdistribusi, berbagi sumber daya (multi-tenant), dan bergantung pada akses jaringan internet. Ancaman keamanan ini dapat berasal dari pihak internal maupun eksternal dan dapat menyerang berbagai lapisan sistem cloud, mulai dari infrastruktur, platform, hingga aplikasi (Subashini & Kavitha, 2011).

Berikut adalah jenis-jenis ancaman keamanan dalam cloud computing beserta penjelasannya:

1. Data Breach (Kebocoran Data)

Data Breach adalah ancaman paling umum dalam lingkungan cloud, di mana data sensitif seperti informasi pribadi, informasi finansial, atau data perusahaan berhasil diakses atau dicuri oleh pihak yang tidak berwenang. Serangan ini sering kali terjadi karena lemahnya pengamanan data, kesalahan konfigurasi cloud, atau serangan hacker (Armbrust et al., 2010).

2. Account Hijacking (Pembajakan Akun)

Account Hijacking adalah ancaman di mana akun pengguna atau administrator dalam cloud berhasil diretas melalui teknik seperti

phishing, pencurian kredensial, atau serangan brute force. Dengan akses ini, penyerang bisa memodifikasi, mencuri, atau menghapus data penting.

3. Denial of Service (DoS/DDoS)

Serangan DoS atau DDoS bertujuan untuk membanjiri server cloud dengan lalu lintas data yang sangat besar sehingga layanan menjadi lambat atau bahkan tidak dapat diakses sama sekali.

4. Insider Threat (Ancaman Internal)

Ancaman ini berasal dari orang dalam organisasi, seperti pegawai atau penyedia layanan cloud yang memiliki akses ke sistem. Mereka bisa saja secara sengaja atau tidak sengaja menyebabkan kebocoran data atau merusak sistem.

5. Insecure Interfaces and APIs

Cloud Computing sangat bergantung pada API (Application Programming Interface) untuk mengatur layanan. Namun, API yang tidak aman atau tidak terproteksi dengan baik dapat menjadi celah masuk bagi penyerang.

6. Misconfiguration of Cloud Services

Konfigurasi yang salah dalam layanan cloud sering menjadi sumber ancaman terbesar. Contohnya seperti bucket penyimpanan yang dibuat publik secara tidak sengaja atau firewall yang tidak dikonfigurasi dengan baik.

7. Malware Injection Attack

Ancaman ini melibatkan penyisipan kode berbahaya (malware) ke dalam layanan cloud, aplikasi, atau data yang dapat menyebabkan kerusakan sistem atau pencurian data.

#### 8. Advanced Persistent Threat (APT)

APT adalah serangan siber yang dilakukan secara terus-menerus, canggih, dan tersembunyi dengan tujuan mencuri data atau mengendalikan sistem dalam jangka waktu lama.

#### 9. Data Loss (Kehilangan Data)

Data loss terjadi ketika data dalam cloud hilang secara permanen, baik karena kesalahan pengguna, kerusakan perangkat keras, kegagalan penyedia layanan, atau serangan ransomware.

## 6.4 Jenis-Jenis Keamanan dalam Cloud Computing

Keamanan dalam Cloud Computing mencakup berbagai aspek perlindungan terhadap data, aplikasi, infrastruktur, dan jaringan dari berbagai ancaman dan serangan siber (Almorsy et al., 2016).

Berikut adalah jenis-jenis keamanan utama dalam cloud computing beserta penjelasannya:

#### 1. Data Security

Data Security merupakan langkah perlindungan data pengguna agar tetap aman saat disimpan (data at rest) maupun saat dikirimkan (data in transit) dalam lingkungan cloud. Teknik utama dalam data security adalah enkripsi data, manajemen kunci (key management), dan teknik data masking untuk melindungi data sensitif dari akses tidak sah (Ali et al., 2015).

#### 2. Identity and Access Management (IAM)

Identity and Access Management (IAM) merupakan sistem yang mengelola identitas pengguna dan pengaturan hak akses ke sumber daya cloud. IAM berfungsi untuk memastikan bahwa hanya

pengguna yang memiliki hak dan otorisasi yang tepat yang dapat mengakses data atau aplikasi tertentu (Hashizume et al., 2013).

### 3. Network Security

Network Security pada Cloud Computing melibatkan pengamanan lalu lintas jaringan antara pengguna dan server cloud dari ancaman seperti serangan Man-in-the-Middle (MITM), sniffing, dan serangan DDoS. Perlindungan ini biasanya dilakukan melalui penggunaan firewall, VPN, IDS/IPS, dan segmentasi jaringan (Mai & Khalil, 2017).

### 4. Application Security

Application Security mencakup perlindungan terhadap aplikasi berbasis cloud dari serangan seperti SQL Injection, Cross-Site Scripting (XSS), dan malware. Pendekatan keamanan ini dilakukan mulai dari tahap pengembangan perangkat lunak (secure coding) hingga penerapan Web Application Firewall (WAF) (Modi et al., 2013).

### 5. Virtualization Security

Karena Cloud Computing menggunakan teknologi virtualisasi, maka keamanan pada hypervisor dan virtual machine (VM) menjadi aspek penting. Ancaman yang mungkin muncul antara lain VM escape attack dan VM hopping attack. Untuk itu, diperlukan perlindungan khusus terhadap lapisan virtualisasi (Zissis & Lekkas, 2012).

### 6. Compliance and Data Privacy

Dalam konteks Cloud Computing, organisasi harus mematuhi standar keamanan dan regulasi privasi data seperti GDPR, HIPAA, atau ISO 27001. Keamanan ini memastikan perlindungan data pribadi serta audit terhadap kegiatan pengolahan data di cloud (Ali et al., 2015).

## 7. Disaster Recovery and Business Continuity

Jenis keamanan ini memastikan bahwa layanan cloud tetap berjalan meskipun terjadi bencana atau kegagalan sistem. Strategi utamanya meliputi backup, failover, dan disaster recovery plan untuk menjaga ketersediaan layanan (Mell & Grance, n.d.).

# 6.5 Teknologi Keamanan Cloud

Keamanan dalam cloud computing membutuhkan kombinasi teknologi, kebijakan, dan prosedur untuk melindungi data, aplikasi, dan infrastruktur dari ancaman (kacha & Zitouni, 2018).

Berikut adalah teknologi utama yang digunakan dalam pengamanan cloud:

### 1. Data Encryption

Enkripsi data adalah proses mengubah data menjadi format yang tidak dapat dibaca tanpa kunci tertentu. Enkripsi digunakan untuk melindungi data saat disimpan (data at rest) dan saat ditransmisikan (data in transit).

### 2. Identity and Access Management (IAM)

IAM digunakan untuk mengatur siapa saja yang memiliki akses ke sistem dan data. IAM mengelola identitas pengguna, otentikasi, otorisasi, dan audit akses.

### 3. Firewall dan Intrusion Detection System (IDS)

Firewall digunakan untuk memblokir akses tidak sah, sedangkan IDS digunakan untuk mendeteksi aktivitas mencurigakan dalam jaringan cloud.

### 4. Multi-Factor Authentication (MFA)

MFA adalah sistem keamanan yang memerlukan lebih dari satu metode verifikasi untuk mengakses sistem cloud, seperti password

dan OTP (One-Time Password). Contoh: Google Authenticator, Microsoft Authenticator.

#### 5. Blockchain Security

Blockchain digunakan untuk menciptakan keamanan data berbasis desentralisasi. Teknologi ini memberikan transparansi, integritas, dan pencatatan aktivitas yang tidak dapat diubah.

#### 6. Security Information and Event Management (SIEM)

SIEM merupakan teknologi untuk mengumpulkan, menganalisis, dan memantau log keamanan secara real-time. SIEM membantu dalam deteksi dini ancaman dan respons insiden.

## 6.6 Strategi Implementasi Keamanan dalam Cloud Computing

Keamanan dalam Cloud Computing tidak hanya bergantung pada teknologi saja, tetapi juga memerlukan strategi implementasi yang terencana, terstruktur, dan berkelanjutan (Zhang et al., 2010). Strategi ini bertujuan untuk memastikan bahwa perlindungan terhadap data, aplikasi, dan infrastruktur cloud berjalan optimal, serta mampu memitigasi risiko dari berbagai ancaman yang ada.

Berikut adalah strategi implementasi keamanan dalam Cloud Computing yang penting untuk diterapkan:

#### 1. Security Policy and Governance (Kebijakan dan Tata Kelola Keamanan)

Organisasi perlu membuat kebijakan keamanan cloud yang jelas dan mendetail, meliputi aturan penggunaan cloud, pengelolaan data, pengendalian akses, serta perlindungan privasi pengguna.

Langkah Implementasi:

- a. Menetapkan Cloud Security Policy berbasis standar industri (ISO 27001, NIST, GDPR).
- b. Menentukan peran dan tanggung jawab pengguna cloud.
- c. Membuat pedoman keamanan untuk akses data sensitif.

## 2. Risk Management (Manajemen Risiko Cloud)

Manajemen risiko cloud dilakukan untuk mengidentifikasi, menilai, dan mengontrol risiko-risiko keamanan yang mungkin terjadi dalam penggunaan layanan cloud.

Langkah Implementasi:

- a. Melakukan Risk Assessment secara berkala.
- b. Menggunakan framework manajemen risiko seperti ISO 31000.
- c. Menentukan level risiko yang dapat diterima (risk appetite).

## 3. Data Protection Strategy (Strategi Perlindungan Data)

Melindungi data dari ancaman kebocoran, kehilangan, dan pencurian menjadi prioritas utama dalam keamanan cloud.

Langkah Implementasi:

- a. Enkripsi data (data at rest dan data in transit).
- b. Backup dan Disaster Recovery Plan.
- c. Data Masking untuk data sensitif.

## 4. Identity and Access Management (IAM)

Mengatur sistem autentikasi dan otorisasi pengguna agar hanya pihak yang memiliki hak akses yang bisa menggunakan sumber daya cloud.

Langkah Implementasi:

- a. Penggunaan Multi-Factor Authentication (MFA).
- b. Role-Based Access Control (RBAC).
- c. Manajemen identitas pengguna dan audit log.

## 5. Continuous Monitoring and Incident Response

Monitoring sistem cloud secara real-time untuk mendeteksi dan merespons ancaman keamanan sejak dini.

Langkah Implementasi:

- a. Menggunakan Security Information and Event Management (SIEM).
- b. Mengaktifkan alerting system untuk aktivitas mencurigakan.
- c. Membentuk Tim Respons Insiden Keamanan.

## 6. Compliance and Regulatory Adherence

Memastikan seluruh aktivitas pengolahan data cloud sesuai dengan regulasi dan standar keamanan yang berlaku.

Langkah Implementasi:

- a. Audit keamanan secara rutin.
- b. Mematuhi standar GDPR, HIPAA, PCI DSS, ISO 27001.
- c. Menjalankan Cloud Security Assessment dari pihak ketiga.

## 7. Employee Awareness and Security Training

Ancaman terbesar sering kali berasal dari kelalaian manusia (human error), sehingga edukasi keamanan bagi seluruh karyawan sangat penting.

Langkah Implementasi:

- a. Melakukan training keamanan berkala.
- b. Simulasi serangan phishing.
- c. Meningkatkan kesadaran keamanan informasi.

## 6.7 Tren dan Perkembangan Teknologi Keamanan Cloud Computing

Seiring dengan semakin tingginya adopsi Cloud Computing di berbagai sektor, ancaman keamanan juga semakin berkembang dan kompleks. Oleh karena itu, teknologi keamanan dalam Cloud Computing terus mengalami inovasi untuk menghadapi tantangan yang semakin dinamis (Kaliappan et al., 2016).

Berikut adalah tren dan perkembangan teknologi keamanan terbaru dalam Cloud Computing:

1. Zero Trust Architecture (ZTA)  
Zero Trust adalah model keamanan terbaru yang menghilangkan kepercayaan default pada jaringan internal atau eksternal. Dalam konsep ini, setiap akses ke sumber daya cloud harus diverifikasi, baik dari pengguna internal maupun eksternal.
2. Cloud Security Posture Management (CSPM)  
CSPM merupakan teknologi untuk mengelola konfigurasi keamanan cloud secara otomatis. CSPM mendeteksi kesalahan konfigurasi (misconfiguration), melakukan audit keamanan, dan membantu organisasi dalam kepatuhan terhadap regulasi (Khiat et al., 2020).
3. Artificial Intelligence (AI) and Machine Learning (ML) for Cloud Security  
AI dan ML digunakan untuk meningkatkan efektivitas deteksi ancaman secara otomatis di lingkungan cloud. AI mampu mendeteksi pola anomali dari aktivitas pengguna dan sistem.
4. Security Automation and Orchestration (SOAR)  
SOAR adalah teknologi yang menggabungkan otomasi keamanan dengan orkestrasi proses respons insiden. Dengan SOAR,

organisasi dapat mempercepat proses mitigasi ancaman dan mengurangi intervensi manual.

5. Confidential Computing

Teknologi ini memungkinkan data untuk tetap terenkripsi bahkan saat sedang diproses di dalam memori (in-use encryption). Hal ini dilakukan menggunakan Trusted Execution Environment (TEE) (Soveizi et al., 2022).

6. Blockchain for Cloud Security

Blockchain digunakan untuk menciptakan sistem audit log terdesentralisasi dan tidak dapat dimodifikasi. Teknologi ini membantu meningkatkan integritas data dan transparansi (Gholami & Laure, 2015).



# Bab 7

## Keuntungan dan Kerugian Cloud Computing

### 7.1 Pendahuluan

Dalam era transformasi digital yang semakin pesat, cloud computing atau komputasi awan menjadi salah satu teknologi kunci yang mendorong efisiensi operasional dan inovasi dalam berbagai sektor. Teknologi ini memungkinkan akses ke sumber daya komputasi melalui jaringan internet tanpa perlu memiliki infrastruktur fisik secara langsung. Dengan skema penggunaan berbasis langganan (subscription-based) dan kemampuan skalabilitas yang tinggi, cloud computing menjadi alternatif yang menjanjikan dibandingkan pendekatan konvensional.

Namun demikian, pemanfaatan cloud computing tidak lepas dari sejumlah tantangan. Ketergantungan pada koneksi internet, potensi pelanggaran privasi data, serta isu kepatuhan terhadap regulasi lokal dan internasional

menjadi faktor penting yang harus dipertimbangkan sebelum mengadopsi layanan berbasis cloud.

Melalui bab ini, pembaca akan diajak untuk memahami secara komprehensif berbagai keuntungan dan kerugian cloud computing sebagai dasar pertimbangan dalam menentukan strategi teknologi informasi yang efektif dan berkelanjutan.

## 7.2 Keuntungan Cloud Computing

### 7.2.1 Efisiensi Biaya

Efisiensi biaya merupakan salah satu daya tarik utama dari cloud computing, yang menjadikannya solusi strategis bagi organisasi dalam pengelolaan teknologi informasi (TI). Dalam pendekatan konvensional, pengadaan infrastruktur TI memerlukan investasi modal (capital expenditure/CAPEX) yang tinggi, seperti pengadaan server, sistem penyimpanan data, perangkat lunak, serta pembangunan pusat data fisik. Selain itu, terdapat biaya tambahan untuk pemeliharaan, pembaruan sistem, pendinginan, dan konsumsi energi yang terus meningkat seiring dengan skala kebutuhan organisasi.

Cloud computing menghadirkan model operasional berbasis langganan atau penggunaan (operational expenditure/OPEX) yang memungkinkan perusahaan untuk mengakses sumber daya TI sesuai kebutuhan tanpa harus membeli dan mengelola perangkat keras sendiri. Model pay-as-you-go ini memberi fleksibilitas dalam penggunaan, sehingga perusahaan hanya membayar sumber daya yang digunakan, seperti penyimpanan, pemrosesan, atau bandwidth, yang dapat disesuaikan secara real-time.

Efisiensi ini tidak hanya mengurangi biaya pengeluaran awal, tetapi juga meminimalkan pengeluaran jangka panjang, khususnya bagi usaha kecil dan menengah yang memiliki keterbatasan modal. Selain itu, dengan infrastruktur yang dikelola oleh penyedia cloud, organisasi dapat

menghindari biaya terkait pemeliharaan teknis, pembaruan perangkat keras, serta kebutuhan akan tenaga ahli internal dalam jumlah besar. Hal ini berdampak langsung terhadap penurunan Total Cost of Ownership (TCO) dan peningkatan Return on Investment (ROI).

Lebih lanjut, penyedia layanan cloud biasanya sudah menerapkan ekonomi skala (economies of scale) dalam pengelolaan infrastrukturnya, sehingga biaya yang ditanggung pengguna per unit layanan menjadi lebih rendah dibandingkan jika infrastruktur tersebut dikelola secara mandiri. Dengan demikian, efisiensi biaya yang ditawarkan oleh cloud computing bukan hanya bersifat teknis, tetapi juga strategis dalam mendukung keberlangsungan dan pertumbuhan organisasi dalam jangka panjang.

## 7.2.2 Skalabilitas dan Fleksibilitas

Cloud computing menawarkan keunggulan signifikan dalam hal skalabilitas dan fleksibilitas, dua aspek penting dalam mendukung dinamika dan pertumbuhan organisasi modern. Skalabilitas merujuk pada kemampuan sistem untuk meningkatkan atau menurunkan kapasitas sumber daya TI sesuai kebutuhan, sedangkan fleksibilitas berkaitan dengan kemudahan dalam menyesuaikan penggunaan layanan tanpa batasan infrastruktur fisik.

Dalam lingkungan bisnis yang berubah dengan cepat, kebutuhan akan sumber daya TI dapat berfluktuasi secara drastis, terutama pada sektor-sektor seperti e-commerce, layanan streaming, atau perusahaan rintisan berbasis teknologi. Melalui cloud computing, organisasi dapat secara otomatis atau manual mengalokasikan sumber daya tambahan (misalnya komputasi, penyimpanan, atau jaringan) ketika permintaan meningkat, dan mengurangnya kembali ketika kebutuhan menurun. Proses ini dapat dilakukan dalam hitungan menit, berbeda dengan pendekatan tradisional yang memerlukan waktu berhari-hari atau bahkan berminggu-minggu untuk melakukan ekspansi infrastruktur.

Selain itu, cloud computing memungkinkan pengguna untuk mengakses layanan dari berbagai perangkat dan lokasi selama terkoneksi dengan internet. Hal ini memberikan fleksibilitas tinggi, khususnya dalam

mendukung model kerja jarak jauh (remote work), kolaborasi lintas negara, serta mobilitas pegawai. Pengembangan dan pengujian aplikasi juga dapat dilakukan lebih cepat karena pengembang tidak perlu menyiapkan infrastruktur secara manual, melainkan cukup memanfaatkan lingkungan cloud yang siap pakai.

Dari perspektif manajerial, skalabilitas dan fleksibilitas ini memungkinkan organisasi untuk lebih responsif terhadap perubahan pasar, mengurangi risiko overprovisioning (kelebihan kapasitas) atau underprovisioning (kekurangan kapasitas), serta mengoptimalkan efisiensi operasional secara keseluruhan.

### 7.2.3 Aksesibilitas Global

Salah satu keunggulan utama dari cloud computing adalah aksesibilitas global, yaitu kemampuan pengguna untuk mengakses data, aplikasi, dan layanan dari mana saja dan kapan saja, selama terdapat koneksi internet yang memadai. Kemampuan ini merupakan hasil dari arsitektur cloud yang terdistribusi, di mana sumber daya dan data tidak lagi terbatas pada perangkat atau lokasi fisik tertentu, melainkan disimpan dan dikelola di pusat data global yang dioperasikan oleh penyedia layanan cloud.

Aksesibilitas global sangat relevan dalam konteks mobilitas kerja, kolaborasi lintas geografis, dan kerja jarak jauh (remote working). Dalam model cloud, karyawan di berbagai lokasi dapat mengakses sistem yang sama secara bersamaan tanpa perlu menggunakan VPN atau koneksi lokal yang kompleks. Hal ini mempercepat proses kolaboratif dan meningkatkan produktivitas, terutama dalam organisasi multinasional atau yang menerapkan kebijakan kerja fleksibel.

Selain itu, akses terhadap sistem cloud tidak terbatas pada satu perangkat. Layanan dapat diakses melalui komputer desktop, laptop, tablet, hingga perangkat seluler. Ini mendukung pendekatan device-agnostic, di mana produktivitas tidak lagi terikat pada perangkat tertentu, melainkan pada identitas dan otorisasi pengguna.

Bagi perusahaan yang beroperasi di banyak wilayah atau negara, aksesibilitas global memungkinkan penyebaran sistem dan layanan secara lebih cepat dan efisien tanpa perlu membangun infrastruktur lokal di setiap wilayah. Cloud computing juga memfasilitasi pengembangan pasar baru, karena perusahaan dapat menjalankan aplikasi dan menyajikan layanan digital secara real-time kepada pengguna dari berbagai belahan dunia, dengan latensi yang minimal berkat dukungan pusat data regional.

Namun, aksesibilitas global juga perlu didukung dengan manajemen hak akses yang ketat dan kebijakan keamanan siber yang kuat, agar tidak menimbulkan risiko kebocoran data akibat akses yang tidak sah dari lokasi atau perangkat yang tidak terverifikasi.

#### 7.2.4 Pemulihan Bencana dan Backup Otomatis

Dalam manajemen teknologi informasi, keandalan sistem dalam menghadapi gangguan merupakan aspek krusial untuk menjaga kontinuitas bisnis. Salah satu keunggulan utama cloud computing adalah kemampuan pemulihan bencana (disaster recovery) dan backup data secara otomatis, yang mendukung ketahanan organisasi terhadap insiden tak terduga seperti kegagalan sistem, serangan siber, atau bencana alam.

Penyedia layanan cloud umumnya memiliki infrastruktur redundan yang tersebar secara geografis di berbagai pusat data. Dengan demikian, apabila terjadi gangguan pada satu lokasi, data dan layanan dapat dialihkan ke lokasi lain dengan dampak minimal terhadap operasional pengguna. Fitur ini dikenal sebagai geo-redundancy atau multi-region failover, dan menjadi bagian integral dari strategi pemulihan bencana yang terotomatisasi dalam platform cloud modern.

Selain itu, layanan cloud biasanya menawarkan mekanisme backup terjadwal dan otomatis. Ini menghilangkan kebutuhan akan proses backup manual yang berisiko tidak konsisten atau terlupakan. Data dapat disalin secara berkala ke lokasi penyimpanan yang aman, dan pengguna dapat mengatur kebijakan retensi data, enkripsi, serta versi cadangan sesuai dengan kebutuhan dan tingkat risiko yang dihadapi.

Kemampuan ini tidak hanya mempercepat proses pemulihan pasca-kerusakan (recovery time objective/RTO) tetapi juga meminimalisasi kerugian data (recovery point objective/RPO). Dengan cloud computing, baik organisasi besar maupun kecil dapat memperoleh solusi pemulihan bencana yang dulu hanya bisa diakses oleh perusahaan dengan anggaran besar, karena tingginya biaya infrastruktur fisik dan sistem backup konvensional.

Namun, penting dicatat bahwa meskipun cloud menawarkan solusi backup dan pemulihan bencana yang andal, tanggung jawab akhir atas pengelolaan dan pengujian sistem pemulihan tetap berada di tangan pengguna. Oleh karena itu, praktik terbaik tetap menyarankan adanya disaster recovery plan (DRP) yang terstruktur dan diuji secara berkala.

### 7.2.5 Infrastruktur yang Dikelola Pihak Ketiga

Salah satu keunggulan strategis dari cloud computing terletak pada kemampuannya untuk mengalihkan tanggung jawab pengelolaan infrastruktur TI kepada pihak ketiga, yaitu penyedia layanan cloud. Dalam model tradisional, organisasi bertanggung jawab penuh atas pengadaan, pemeliharaan, pemantauan, dan pengamanan infrastruktur TI mereka sendiri—tugas yang membutuhkan sumber daya besar, baik dari segi biaya, waktu, maupun keahlian teknis.

Dengan adopsi cloud computing, penyedia layanan bertanggung jawab atas operasional harian infrastruktur, termasuk pembaruan sistem, pemantauan keamanan, penanganan kegagalan perangkat keras, serta peningkatan kapasitas sesuai permintaan. Hal ini memungkinkan organisasi untuk mengurangi beban kerja departemen TI internal dan memfokuskan sumber daya pada aspek strategis, seperti inovasi produk, pengalaman pelanggan, dan pengembangan bisnis inti.

Penyedia cloud umumnya memiliki tim ahli dan infrastruktur berskala besar yang dirancang dengan praktik terbaik industri, seperti sistem redundansi, manajemen insiden otomatis, serta pusat data dengan sertifikasi keamanan dan ketersediaan tinggi (misalnya ISO 27001, SOC 2, atau Tier

III/IV data centers). Oleh karena itu, pengguna layanan dapat memperoleh tingkat keandalan, ketersediaan, dan keamanan yang tinggi tanpa perlu membangun sistem tersebut secara internal.

Selain itu, karena penyedia layanan cloud beroperasi berdasarkan model multi-tenant, biaya pengelolaan infrastruktur dibagi di antara banyak pengguna, sehingga memberikan ekonomi skala yang tidak dapat dicapai oleh organisasi individu secara efisien.

Namun demikian, meskipun penyedia layanan bertanggung jawab atas infrastruktur, pengguna tetap bertanggung jawab atas pengelolaan data dan konfigurasi aplikasi mereka sendiri—sebuah prinsip yang dikenal sebagai *shared responsibility model*. Oleh karena itu, organisasi tetap harus memiliki kebijakan tata kelola yang baik dalam penggunaan cloud agar manfaat dari model ini dapat dioptimalkan tanpa mengorbankan kontrol atas data dan sistem kritis.

## 7.3 Kerugian Cloud Computing

### 7.3.1 Ketergantungan pada Koneksi Internet

Salah satu kelemahan paling mendasar dari cloud computing adalah ketergantungan total terhadap koneksi internet sebagai sarana utama untuk mengakses data, aplikasi, dan infrastruktur layanan yang disediakan oleh penyedia cloud. Dalam model cloud, baik pemrosesan data maupun penyimpanan dilakukan secara eksternal melalui jaringan, bukan secara lokal. Hal ini menjadikan ketersediaan dan stabilitas koneksi internet sebagai prasyarat utama dalam menjalankan operasional yang berbasis cloud.

Dalam konteks geografis yang belum merata akses teknologinya, seperti wilayah pedesaan atau negara berkembang, keterbatasan infrastruktur internet dapat menjadi hambatan serius dalam implementasi cloud computing secara optimal. Koneksi internet yang lambat, tidak stabil, atau

sering mengalami gangguan akan langsung berdampak pada produktivitas pengguna dan kelancaran operasional sistem. Bahkan di daerah dengan konektivitas yang baik sekalipun, risiko gangguan dari penyedia layanan internet (ISP), cuaca buruk, hingga aktivitas pemeliharaan jaringan tetap dapat memicu downtime akses cloud.

Kondisi ini juga menjadi tantangan serius bagi organisasi yang menjalankan sistem mission-critical atau layanan yang bersifat waktu nyata (real-time), seperti aplikasi keuangan, sistem kesehatan, atau sistem produksi. Keterlambatan atau kehilangan akses akibat gangguan jaringan dapat menyebabkan kerugian operasional, reputasi, bahkan finansial yang signifikan.

Lebih lanjut, dalam beberapa kasus, tingginya latensi jaringan dapat menurunkan kinerja aplikasi berbasis cloud, terutama untuk aplikasi dengan kebutuhan pemrosesan data intensif atau interaksi pengguna yang tinggi. Meskipun penyedia cloud besar telah mengembangkan infrastruktur global dan edge computing untuk mengurangi latensi, tidak semua wilayah pengguna memiliki akses ke pusat data terdekat.

Oleh karena itu, ketergantungan pada koneksi internet menjadikan resiliensi jaringan dan perencanaan cadangan (failover connection, offline access) sebagai elemen penting dalam strategi adopsi cloud. Organisasi disarankan untuk memiliki kebijakan mitigasi risiko terhadap gangguan konektivitas agar operasional tetap dapat berjalan, setidaknya dalam bentuk terbatas, saat akses cloud terputus.

### **7.3.2 Risiko Keamanan dan Privasi**

Meskipun cloud computing menawarkan solusi efisien dan fleksibel dalam pengelolaan teknologi informasi, salah satu isu paling krusial yang masih menjadi perhatian utama adalah keamanan dan privasi data. Dalam model cloud, data organisasi disimpan di pusat data yang dikelola oleh pihak ketiga, dan diakses melalui jaringan publik atau semi-publik (internet). Hal ini menimbulkan kekhawatiran mengenai bagaimana data dikendalikan, dilindungi, dan siapa saja yang dapat mengaksesnya.

Dari perspektif keamanan, potensi ancaman mencakup serangan siber, seperti Distributed Denial of Service (DDoS), peretasan (hacking), pencurian kredensial, hingga serangan internal oleh personel penyedia layanan cloud. Selain itu, adanya multi-tenancy—yaitu kondisi di mana satu server fisik digunakan oleh beberapa pelanggan meningkatkan kompleksitas dan potensi kerentanan terhadap kebocoran data antar pengguna.

Sementara itu, dari sisi privasi, risiko muncul ketika data disimpan di server yang berlokasi di yurisdiksi hukum yang berbeda, di mana aturan perlindungan data pribadi mungkin tidak seketat atau sekompatibel dengan regulasi lokal pengguna. Misalnya, penyimpanan data pengguna Uni Eropa di luar wilayah Uni Eropa harus mematuhi General Data Protection Regulation (GDPR), yang mensyaratkan kontrol ketat atas pengolahan dan transfer data pribadi.

Keterbatasan kontrol langsung terhadap infrastruktur dan sistem keamanan pada penyedia layanan cloud juga membuat organisasi rentan terhadap insiden kebocoran data (data breach), serta berisiko mengalami kesulitan dalam audit keamanan, penghapusan data secara permanen (data sanitization), atau pemulihan data secara independen.

Sebagai respons, penyedia cloud besar telah mengembangkan sistem keamanan berlapis yang mencakup enkripsi data, manajemen identitas dan akses (IAM), firewall cerdas, dan pengawasan proaktif terhadap ancaman. Namun demikian, tanggung jawab keamanan bersifat terbagi (shared responsibility): penyedia cloud bertanggung jawab atas keamanan infrastruktur, sementara pengguna bertanggung jawab atas konfigurasi sistem, manajemen akses, dan perlindungan data yang mereka simpan di cloud.

Dengan demikian, meskipun cloud computing mampu menawarkan tingkat keamanan tinggi secara teknis, tetap diperlukan pemahaman mendalam dan kebijakan tata kelola keamanan data yang ketat dari pihak pengguna agar risiko-risiko yang muncul tidak berkembang menjadi insiden yang merugikan.

### 7.3.3 Downtime dan Ketergantungan pada Vendor

Meskipun cloud computing menjanjikan ketersediaan layanan tinggi dengan infrastruktur canggih yang dimiliki oleh penyedia layanan, risiko downtime tetap menjadi salah satu tantangan utama. Downtime merujuk pada kondisi ketika layanan cloud tidak tersedia atau tidak dapat diakses oleh pengguna karena gangguan teknis, pemeliharaan sistem, atau kegagalan infrastruktur penyedia cloud. Dalam konteks bisnis, downtime berdampak langsung terhadap penurunan produktivitas, kerugian finansial, dan kerusakan reputasi, terlebih bagi organisasi yang sangat bergantung pada layanan digital secara real-time.

Beberapa penyebab umum downtime meliputi kesalahan konfigurasi, serangan siber (misalnya DDoS), kerusakan perangkat keras di pusat data, hingga pembaruan sistem yang tidak berjalan sesuai rencana. Meskipun penyedia cloud terkemuka seperti Amazon Web Services (AWS), Microsoft Azure, dan Google Cloud memiliki tingkat availability yang tinggi (seringkali di atas 99,9%), catatan sejarah menunjukkan bahwa insiden besar tetap dapat terjadi, bahkan menyebabkan gangguan layanan dalam skala global.

Selain itu, cloud computing juga menghadirkan risiko vendor lock-in, yaitu ketergantungan jangka panjang terhadap satu penyedia layanan. Ini terjadi karena perbedaan format data, arsitektur sistem, serta layanan eksklusif yang ditawarkan oleh masing-masing penyedia cloud, sehingga migrasi ke penyedia lain menjadi sulit, mahal, dan kompleks. Akibatnya, organisasi kehilangan fleksibilitas dalam memilih solusi terbaik atau menyesuaikan strategi teknologi seiring dengan perubahan kebutuhan.

Vendor lock-in juga dapat mempersempit kemampuan organisasi dalam melakukan negosiasi harga, memilih lokasi pusat data, atau mengontrol penuh terhadap pembaruan sistem. Dalam situasi ekstrem seperti perubahan kebijakan harga, kebangkrutan vendor, atau konflik hukum lintas negara, pengguna dapat menghadapi kendala besar dalam memindahkan data atau aplikasi ke lingkungan alternatif.

Untuk memitigasi risiko ini, strategi yang umum diterapkan adalah multi-cloud deployment (menggunakan lebih dari satu penyedia cloud), atau hybrid cloud approach yang memadukan penggunaan cloud publik dan infrastruktur lokal. Selain itu, pemilihan layanan berbasis standar terbuka (open standards) dan penyedia yang mendukung interoperabilitas lintas platform dapat membantu mengurangi ketergantungan terhadap satu vendor tunggal.

### 7.3.4 Biaya Jangka Panjang Bisa Membengkak

Meskipun cloud computing sering dipromosikan sebagai solusi yang hemat biaya, terutama karena menghilangkan kebutuhan akan investasi awal yang besar (capital expenditure/CAPEX), dalam praktiknya penggunaan cloud dapat menyebabkan pembengkakan biaya dalam jangka panjang apabila tidak dikelola dengan baik. Hal ini menjadikan aspek ekonomi cloud bersifat paradoks: efisien di awal, namun berpotensi mahal seiring waktu.

Model pembayaran berbasis konsumsi (pay-as-you-go) memang fleksibel, tetapi juga menyimpan risiko pengeluaran yang sulit diprediksi, terutama jika penggunaan sumber daya tidak dimonitor secara ketat. Penggunaan otomatis layanan komputasi, penyimpanan data, transfer bandwidth, dan layanan tambahan (seperti AI, database, atau keamanan tingkat lanjut) dapat meningkat secara signifikan seiring pertumbuhan operasional atau lonjakan trafik mendadak.

Organisasi juga berisiko menghadapi biaya tersembunyi (hidden costs) seperti:

1. Transfer data keluar (egress) ke luar cloud yang biasanya lebih mahal daripada transfer internal.
2. Kenaikan harga layanan dari penyedia cloud secara sepihak tanpa kontrak jangka panjang yang tetap.
3. Lisensi perangkat lunak tambahan yang dijalankan di dalam lingkungan cloud.

4. Biaya untuk layanan premium seperti SLA (Service Level Agreement) yang lebih tinggi atau dukungan teknis khusus.

Selain itu, ketergantungan terhadap satu vendor (vendor lock-in) seperti yang dijelaskan sebelumnya, dapat meningkatkan beban biaya migrasi dan integrasi jika di masa depan organisasi memutuskan untuk berpindah platform. Migrasi data dan aplikasi dari satu penyedia ke penyedia lain (atau kembali ke on-premises) tidak hanya membutuhkan biaya teknis, tetapi juga waktu dan risiko downtime.

Karena itu, pengelolaan biaya cloud menjadi tantangan penting dalam strategi adopsi teknologi ini. FinOps (Financial Operations) muncul sebagai pendekatan baru untuk menggabungkan praktik keuangan dan operasional TI dalam rangka mengontrol biaya cloud, meningkatkan transparansi penggunaan, dan mengoptimalkan pengeluaran.

### 7.3.5 Isu Kepatuhan dan Lokasi Data

Salah satu tantangan yang kompleks dalam penerapan cloud computing adalah isu kepatuhan hukum dan lokasi penyimpanan data (data residency). Ketika data disimpan di cloud, pengguna tidak selalu memiliki kendali langsung atas di mana secara geografis data tersebut disimpan. Hal ini menimbulkan potensi masalah hukum dan regulasi, terutama ketika data pelanggan atau organisasi disimpan di pusat data yang berada di luar yurisdiksi hukum tempat data tersebut dikumpulkan.

Beberapa negara dan wilayah memiliki regulasi perlindungan data yang ketat, seperti General Data Protection Regulation (GDPR) di Uni Eropa, Health Insurance Portability and Accountability Act (HIPAA) di Amerika Serikat, atau Peraturan Perlindungan Data Pribadi (PDP) di Indonesia. Aturan-aturan ini mewajibkan penyimpanan, pengolahan, dan transfer data dilakukan dengan mempertimbangkan prinsip kedaulatan data (data sovereignty) dan izin eksplisit dari subjek data.

Jika penyedia layanan cloud menyimpan data di pusat data yang berada di luar wilayah hukum yang ditentukan, maka data tersebut dapat tunduk

pada hukum negara lain, termasuk potensi akses oleh otoritas asing. Hal ini dapat menyebabkan pelanggaran kepatuhan, tuntutan hukum, atau bahkan denda administratif terhadap organisasi pengguna.

Lebih lanjut, ketidaksesuaian antara kebijakan penyedia cloud dan persyaratan regulasi lokal dapat menimbulkan kerumitan dalam audit, pelaporan, dan penghapusan data (data erasure/right to be forgotten). Organisasi mungkin juga kesulitan untuk membuktikan bahwa mereka mematuhi standar tertentu jika tidak memiliki visibilitas penuh terhadap lokasi dan mekanisme pengelolaan data yang dilakukan oleh penyedia layanan cloud.

Untuk mengatasi masalah ini, banyak penyedia cloud kini menawarkan opsi lokasi penyimpanan data yang dapat dipilih oleh pelanggan, serta fitur geo-fencing atau penyimpanan data di wilayah tertentu. Beberapa bahkan membentuk lokalisasi pusat data di negara-negara dengan regulasi ketat sebagai bentuk adaptasi terhadap tuntutan hukum lokal.

Namun demikian, tanggung jawab akhir untuk memastikan bahwa penggunaan cloud mematuhi semua peraturan yang relevan tetap berada pada organisasi pengguna. Oleh karena itu, evaluasi menyeluruh terhadap aspek hukum dan kepatuhan sangat diperlukan sebelum mengadopsi solusi cloud secara luas.

## 7.4 Analisis Singkat

Cloud computing telah menjadi paradigma utama dalam transformasi digital organisasi modern. Namun, sebagaimana halnya teknologi lainnya, penerapannya membawa dampak yang bersifat dua sisi, yaitu keuntungan yang signifikan di satu sisi, serta risiko dan tantangan di sisi lainnya. Oleh karena itu, diperlukan pendekatan yang seimbang dan berbasis bukti dalam menganalisis manfaat serta keterbatasan teknologi ini.

Dari sisi keuntungan, cloud computing menawarkan sejumlah keunggulan strategis dan operasional. Efisiensi biaya menjadi salah satu aspek paling mencolok, mengingat model pay-as-you-go mengubah pengeluaran modal (CAPEX) menjadi pengeluaran operasional (OPEX), memungkinkan organisasi menyesuaikan sumber daya sesuai kebutuhan aktual. Di samping itu, skalabilitas, aksesibilitas global, kemampuan backup otomatis, dan pemulihan bencana yang cepat menjadikan cloud sebagai solusi yang adaptif dan resilien terhadap perubahan lingkungan bisnis.

elain itu, dengan infrastruktur yang dikelola oleh pihak ketiga, organisasi dapat mengurangi beban teknis dan memfokuskan sumber dayanya pada aktivitas inti. Penggunaan teknologi mutakhir, seperti edge computing, machine learning, dan layanan berbasis API, juga memperkuat posisi cloud computing sebagai katalis inovasi.

Namun, cloud computing juga memiliki kerugian yang perlu diantisipasi secara strategis. Ketergantungan terhadap koneksi internet menghadirkan risiko operasional, khususnya di wilayah dengan infrastruktur jaringan yang belum stabil. Risiko keamanan dan privasi, termasuk potensi pelanggaran data dan akses tidak sah, masih menjadi kekhawatiran utama. Selain itu, biaya jangka panjang dapat membengkak jika penggunaan tidak dimonitor dengan cermat, dan vendor lock-in dapat membatasi fleksibilitas organisasi.

Di sisi regulasi, isu terkait kepatuhan hukum dan lokasi data semakin menantang, mengingat banyak organisasi harus memastikan data mereka dikelola sesuai yurisdiksi hukum yang berlaku. Hal ini menuntut pemahaman mendalam terhadap tata kelola TI, termasuk pengawasan terhadap penyedia layanan cloud.

Dalam konteks ini, analisis manfaat dan risiko cloud computing sebaiknya dilakukan dengan mempertimbangkan kebutuhan spesifik organisasi, karakteristik industri, kesiapan infrastruktur, dan kapasitas sumber daya manusia. Strategi mitigasi risiko seperti hybrid cloud deployment, multi-cloud adoption, dan implementasi kebijakan keamanan berbasis zero-

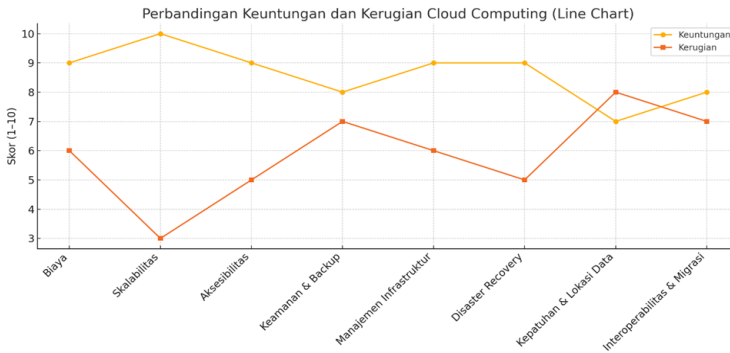
trust—dapat meningkatkan efektivitas pemanfaatan cloud tanpa mengorbankan aspek keamanan, kontrol, dan efisiensi biaya.

Dengan demikian, cloud computing bukanlah solusi universal untuk semua organisasi, melainkan sebuah pendekatan teknologi yang membutuhkan perencanaan matang, evaluasi berkelanjutan, dan integrasi strategis agar dapat memberikan nilai tambah yang maksimal.

**Tabel 7.1:** Tabel perbandingan keuntungan vs kerugian Cloud Computing.

Aspek	Keuntungan	Kerugian
Biaya	Model pay-as-you-go mengurangi investasi awal (CAPEX).	Biaya jangka panjang bisa membengkak jika tidak dikontrol (hidden cost, transfer data).
Skalabilitas dan Fleksibilitas	Sumber daya dapat ditingkatkan atau diturunkan sesuai kebutuhan.	Potensi over-provisioning saat tidak ada pengawasan terhadap penggunaan sumber daya.
Aksesibilitas Global	Akses data dan aplikasi dari mana saja dan berbagai perangkat.	Bergantung sepenuhnya pada koneksi internet yang stabil dan aman.
Keamanan dan Backup	Penyedia cloud menyediakan sistem keamanan dan backup otomatis.	Risiko pelanggaran data, kehilangan kendali langsung atas keamanan, dan serangan siber.
Manajemen Infrastruktur	Infrastruktur dikelola oleh pihak ketiga yang profesional dan tersertifikasi.	Ketergantungan terhadap vendor dan kurangnya kontrol langsung terhadap konfigurasi sistem.
Pemulihan Bencana (Disaster Recovery)	Solusi failover dan pemulihan cepat bila terjadi gangguan sistem.	Ketersediaan SLA tinggi bergantung pada tingkat layanan; layanan premium menambah biaya.

Kepatuhan dan Lokasi Data	Beberapa penyedia sudah menawarkan layanan berbasis lokasi data tertentu.	Tantangan kepatuhan terhadap regulasi (GDPR, HIPAA, PDP) jika data tersimpan di luar negeri.
Interoperabilitas dan Migrasi	Adanya API standar dan dukungan integrasi lintas platform di beberapa provider.	Vendor lock-in membuat migrasi ke platform lain mahal dan kompleks.



**Gambar 7.1:** Grafik perbandingan keuntungan vs kerugian Cloud Computing

### 7.4.1 Kapan Cocok Menggunakan Cloud.

Keputusan untuk mengadopsi cloud computing sebaiknya tidak didasarkan semata pada tren atau janji efisiensi, melainkan melalui analisis kebutuhan organisasi, kesiapan infrastruktur, dan konteks operasional.

Penggunaan cloud akan sangat menguntungkan dan relevan dalam kondisi-kondisi berikut:

1. Skala Usaha Dinamis atau Bertumbuh Cepat

Organisasi dengan kebutuhan sumber daya TI yang fluktuatif atau berkembang pesat akan sangat terbantu oleh sifat elastisitas cloud. Cloud memungkinkan peningkatan atau penurunan kapasitas sistem secara instan tanpa harus menambah perangkat keras fisik.

## 2. Anggaran Investasi Awal Terbatas

Usaha kecil dan menengah (UKM/UMKM) yang tidak memiliki dana besar untuk membeli server, lisensi, dan membentuk tim TI internal dapat memanfaatkan cloud karena model pembiayaan operational expenditure (OPEX) lebih ringan dibanding capital expenditure (CAPEX) tradisional.

## 3. Organisasi yang Membutuhkan Mobilitas Tinggi

Cloud sangat cocok digunakan oleh organisasi dengan tim yang tersebar secara geografis atau menerapkan sistem kerja jarak jauh (remote work). Dengan akses global melalui internet, data dan aplikasi dapat digunakan dari berbagai lokasi dan perangkat.

## 4. Bisnis dengan Kebutuhan Kolaboratif

Sektor seperti pendidikan, media, pengembangan perangkat lunak, dan proyek multinasional sangat diuntungkan dengan kolaborasi real-time dan dokumen yang dapat diakses serta diedit secara simultan melalui layanan cloud.

## 5. Kebutuhan Backup dan Disaster Recovery yang Andal

Organisasi yang memiliki data sensitif dan bergantung pada ketersediaan sistem sangat cocok menggunakan cloud, karena banyak penyedia layanan menawarkan solusi disaster recovery otomatis, yang sebelumnya hanya bisa dilakukan oleh perusahaan besar dengan infrastruktur khusus.

## 6. Kebutuhan Uji Coba atau Pengembangan Cepat (Dev/Test Environment)

Cloud sangat cocok untuk startup teknologi atau pengembang software yang memerlukan lingkungan pengujian yang cepat disiapkan, terisolasi, dan mudah dimodifikasi.

#### 7. Bisnis yang Menargetkan Skalabilitas Global

Cloud mempermudah peluncuran produk digital yang ditujukan untuk pasar internasional, tanpa harus membangun server fisik di banyak negara. Penyedia cloud besar umumnya memiliki pusat data global dengan dukungan low latency.

#### 7.4.2 Namun, Cloud Belum Ideal Digunakan Jika

1. Koneksi internet sangat tidak stabil atau belum merata (misalnya di daerah terpencil).
2. Organisasi memiliki persyaratan regulasi ketat terkait lokasi dan pengendalian data (misalnya sektor pemerintahan atau militer).
3. Sistem yang digunakan sangat bergantung pada hardware khusus atau latensi rendah ekstrem (seperti industri manufaktur realtime dengan IoT lokal).
4. Biaya penggunaan cloud tidak dapat diprediksi atau dipantau dengan baik, sehingga berisiko membengkak.

# Bab 8

## Virtualisasi dan Penggunaan Cloud

### 8.1 Definisi Virtualisasi

Teknologi virtualisasi memungkinkan perangkat lunak cloud vendor untuk secara otomatis memindahkan data dari perangkat keras yang rusak atau ditarik offline ke bagian sistem atau perangkat keras yang berfungsi atau beroperasi. Oleh karena itu, klien mendapatkan akses mulus ke data. Sistem pencadangan terpisah, dengan strategi pemulihan terhadap ancaman cloud, menyediakan lapisan ketergantungan dan keandalan lainnya.

Komputasi awan juga mempromosikan alternatif ramah lingkungan untuk fungsi kantor yang padat kertas. Itu karena membutuhkan lebih sedikit perangkat keras komputasi on-premise, dan semua tugas yang berhubungan dengan komputasi berlangsung dari jarak jauh dengan kebutuhan perangkat keras komputasi minimal dengan bantuan inovasi teknologi seperti virtualisasi dan multitenancy (Haryadi, 2024).

Teknologi virtualisasi adalah teknologi untuk membuat komputer fisik bertindak seolah-olah komputer tersebut adalah dua komputer nonfisik (komputer virtual) atau lebih. Masing-masing komputer nonfisik tersebut memiliki arsitektur dasar yang sama dengan komputer fisiknya. Ada berbagai cara untuk melakukan hal ini, tiap cara mempunyai kelebihan dan kekurangan masing-masing. Untuk membuat komputer fisik menjadi dua atau lebih komputer virtual, karakteristik perangkat kerasnya harus dikonstruksi kembali melalui perangkat lunak.

Virtualisasi adalah konsep yang mengizinkan komputer untuk dibagi dalam beberapa lingkungan pada saat yang sama. Lingkungan ini dapat saling berhubungan atau bahkan tanpa saling berhubungan sama sekali (Umar, 2013).

## 8.2 Virtualisasi di Cloud Computing

Virtualisasi dalam cloud Computing adalah teknologi yang memungkinkan kita membuat sumber daya virtual seperti server, jaringan dan penyimpanan di cloud. Semua sumber daya ini dialokasikan dari mesin fisik yang berjalan di suatu tempat didunia dan akan memperoleh perangkat lunak untuk menyediakan dan mengelola sumber daya virtual.

Mesin Fisik ini dioperasikan oleh penyediaan cloud yang menangani pemeliharaan dan pasokan perangkat keras. Virtualisasi di Cloud Computing juga memungkinkan kita mengatur kontrol akses atas sumber daya untuk mengamankannya. Ini juga memungkinkan berbagi sumber daya di antara banyak aplikasi.

Virtualisasi juga memungkinkan pemanfaatan sumber daya secara efisien, karena hanya menyediakan jumlah sumber daya yang diminta dan tidak lebih. Dan menyediakan sumber daya tambahan seperti memori tambahan, penyimpanan, atau prosesor semudah mengklik beberapa tombol pada perangkat lunak cloud.

Beberapa contoh virtualisasi dalam cloud computing adalah sebagai berikut (Haryadi, 2024):

1. Layanan EC2 dari Amazon Web Service
2. Mesin komputasi dari Google Cloud
3. Mesin Virtual Azure dari Microsoft Azure

## 8.3 Konsep Virtualisasi

Ada beberapa konsep-konsep utama yang terkait dengan teknologi virtualisasi diantaranya (Huawei Technologies Co., 2023):

### 1. Hypervisor

Hypervisor adalah komponen sentral yang mengelola perangkat keras komputer secara asli dan memungkinkan beberapa lingkungan terisolasi satu sama lainnya. Ini sebagai dasar dari komputasi awan dimana aplikasi, server, penyimpanan dan jaringan semuanya dapat divirtualisasikan.

### 2. Mesin Virtual (VM)

Mesin Virtual (VM) adalah emulasi system computer dengan sistem operasi tamu virtualnya sendiri yang berjalan di hypervisor. Penyedia cloud biasanya menawarkan banyak jenis Mesin Virtual (VM) terkelola yang juga dikenal sebagai instans komputasi. Ini semua termasuk yang dioptimalkan, memori yang dioptimalkan dan instans dengan akselerasi perangkat keras.

### 3. Wadah (Kontainer)

Kontainer adalah unit perangkat lunak standar yang mengemas kode dan semua dependensinya sehingga aplikasi dapat berjalan dengan cepat dan andal di lingkungan komputasi yang berbeda. Sehingga berbeda dengan Virtual Mesin (VM), Kontainer

menvirtualisasikan sistem operasi dibandingkan dengan perangkat keras yang mendasarinya sehingga membuatnya lebih portable dan efisien.

#### 4. Perangkat Lunak Virtualisasi

Perangkat Lunak Virtualisasi adalah lapisan abstraksi yang memungkinkan pemanfaatan perangkat keras komputer fisik secara lebih efisien. Ini semua didasarkan dari komputasi awam dimana aplikasi, server, penyimpanan dan jaringan semuanya dapat divirtualisasikan.

#### 5. Jaringan Virtual (Jaringan Maya)

Jaringan Virtual adalah jaringan komputer dimana semua perangkat, server dan pusat data terhubung melalui perangkat lunak sehingga memungkinkan memiliki jangkauan lebih lanjut dibandingkan jika hanya dihubungkan dengan kabel secara fisik saja. (Haryadi, 2024)

## 8.4 Jenis-jenis Virtualisasi didalam Cloud Computing

Ada beberapa jenis – jenis virtualisasi yang dapat digunakan dalam cloud computing, beberapa diantaranya yaitu (Haryadi, 2024):

### 1. Virtualisasi Server

Merupakan teknologi yang digunakan untuk membuat satu atau lebih lingkungan virtual dalam satu fisik server. Virtualisasi server memungkinkan pengguna untuk menjalankan beberapa sistem operasi dan aplikasi di dalam satu fisik server secara bersamaan.

## 2. Virtualisasi Storage

Merupakan teknologi yang digunakan untuk membuat lingkungan penyimpanan virtual dari beberapa sumber penyimpanan fisik yang tersedia. Virtualisasi storage memungkinkan pengguna untuk mengelola, mengoptimalkan, dan mengakses sumber penyimpanan secara efisien.

## 3. Virtualisasi Desktop

Merupakan teknologi yang digunakan untuk membuat lingkungan desktop virtual yang dapat diakses darimana saja. Virtualisasi desktop memungkinkan pengguna untuk menjalankan aplikasi dan sistem operasi di dalam lingkungan virtual yang dapat diakses dari berbagai perangkat, seperti PC, laptop, atau perangkat mobile.

## 4. Virtualisasi Jaringan

Merupakan teknologi yang digunakan untuk membuat lingkungan jaringan virtual dari beberapa perangkat jaringan fisik yang tersedia. Virtualisasi jaringan memungkinkan pengguna untuk mengelola, mengoptimalkan, dan mengakses jaringan secara efisien.

## 5. Virtualisasi Aplikasi

Merupakan teknologi yang digunakan untuk membuat lingkungan aplikasi virtual dari beberapa aplikasi yang tersedia. Virtualisasi aplikasi memungkinkan pengguna untuk mengelola, mengoptimalkan, dan mengakses aplikasi secara efisien.

## 8.5 Perbedaan antara Virtualisasi dan Cloud Computing

Komputasi cloud adalah pengiriman sumber daya komputasi sesuai permintaan melalui internet dengan harga bayar sesuai pemakaian. Untuk membeli, memiliki dan memelihara pusat data fisik, Anda dapat mengakses layanan teknologi, seperti daya komputasi, penyimpanan, dan basis data, sesuai kebutuhan dari penyedia cloud.

Teknologi virtualisasi memungkinkan komputasi cloud. Penyedia cloud menyiapkan dan memelihara pusat data mereka sendiri. Mereka membuat lingkungan virtual berbeda yang menggunakan sumber daya perangkat keras yang mendasari. Kemudian, kita dapat memprogram sistem untuk mengakses sumber daya cloud ini menggunakan API. Kebutuhan infrastruktur Anda dapat dipenuhi sebagai layanan terkelola penuh (Haryadi, 2024).

## 8.6 Cara Kerja Virtualisasi di Cloud Computing

Virtualisasi di cloud dicapai dengan menggabungkan beberapa lapisan virtualisasi, lapisan ini mencakup virtualisasi perangkat keras atau fisik, jaringan, penyimpanan dan aplikasi. Lapisan ini dapat dikustomisasi dan dikontrol oleh perangkat lunak cloud oleh pengguna. Interaksi dengan virtualisasi dimulai dengan pengguna mengirimkan permintaan sumber daya virtual melalui perangkat lunak cloud yang mentransfer permintaan tersebut ke hypervisor.

Hypervisor kemudian memeriksa sumber daya yang tersedia dan mengalokasikan jumlah sumber daya yang diminta kepada pengguna. Karena interaksi yang disederhanakan ini, pengguna dapat menyiapkan seluruh infrastruktur mereka dalam waktu yang lebih singkat dan

pemeliharaan yang lebih sedikit daripada harus menyiapkan seluruh infrastruktur fisik dan memeliharanya sendiri (Haryadi, 2024).

## 8.7 Karakteristik Virtualisasi di Cloud Computing

### 1. Sumber Daya yang Dikelola

VM atau sumber daya apa pun yang disediakan dari cloud sepenuhnya dikelola oleh penyedia cloud, yang berarti selain menentukan persyaratan, pengguna tidak perlu memelihara atau khawatir tentang perangkat keras yang mendasarinya dan konfigurasi sumber daya mereka. Misalnya, penyedia cloud menangani semua pekerjaan seperti persediaan perangkat keras, pencadangan, pemantauan, dll.

### 2. Alokasi Sumber Daya

Penjataan sumber daya menjadi sederhana dengan teknologi virtualisasi, prosesnya sesederhana mengklik beberapa tombol. Pengguna dapat menyiapkan seluruh infrastrukturnya dalam hitungan jam, dan mereka dapat menyesuaikannya nanti tanpa kesulitan.

### 3. Isolasi Sumber Daya

Isolasi sumber daya adalah salah satu karakteristik penting dari virtualisasi di cloud. Hal ini memungkinkan aplikasi berjalan di lingkungan yang sepenuhnya didedikasikan untuk aplikasi tersebut. Hal ini juga membantu mencegah pelanggaran data dan memastikan pemanfaatan sumber daya yang efisien.

#### 4. Penyeimbangan Beban

Penyeimbang beban seperti namanya menangani beban permintaan server. Platform virtualisasi memastikan bahwa permintaan masuk didistribusikan ke server yang sesuai. Hal ini memungkinkan server untuk melayani permintaan lebih cepat daripada kelebihan beban oleh permintaan dalam jumlah besar.

#### 5. Protabilitas

Sumber daya virtualisasi bersifat portabel, artinya dapat disalin dan dipindahkan dari satu sistem ke sistem lainnya, dan fungsi yang sama dapat diharapkan. Hal ini memungkinkan pengguna untuk membuat dan menggunakan kembali konfigurasi alih-alih mengulanginya (Haryadi, 2024).

## 8.8 Tipe Virtualisasi

### 1. Full Virtualization (Virtualisasi Penuh)

Virtualisasi penuh yang biasa disebut dengan native virtualization. Model ini menggunakan mesin virtual yang menjembatani antara sistem operasi tamu dan perangkat keras aslinya.

Virtualisasi penuh lebih cepat daripada emulasi perangkat keras, tapi performanya lebih lambat dari perangkat keras langsung, karena jembatan/mediasi hypervisor. Keuntungan terbesar dari virtualisasi penuh adalah sistem operasi dapat dijalankan tanpa dimodifikasi. Batasan yang dimiliki hanyalah bahwa sistem operasi harus mendukung perangkat keras dibawahnya (Huawei Technologies Co., 2023).

## 2. Paravirtualization

Paravirtualization adalah teknik lain yang populer yang mempunyai virtualisasi menggunakan kemiripan penuh. Dengan Metode hypervisor ini untuk berbagi akses ke perangkat keras dibawahnya, tapi menyatukan kode yang sadar virtualisasi ke sistem operasi, Pendekatan ini. Menghilangkan rekompilasi atau pemerangkapan, karena sistem operasi berkooperasi dengan proses virtualisasi (Umar, 2013).

## 3. Virtualisasi Berbantuan Perangkat Keras

Teknik virtualisasi berbantuan perangkat keras menghilangkan terjemahan biner dan paravirtualisasi. Di sini, permintaan OS langsung menjebak hypervisor tanpa terjemahan apa pun. Seperti dalam pendekatan virtualisasi lainnya, permintaan pengguna langsung dieksekusi tanpa terjemahan apa pun (Santoso, 2023).

# 8.9 Manfaat Virtualisasi dan Cloud Computing

Virtualisasi dan cloud Computing menawarkan berbagai manfaat bagi individu maupun organisasi.

Beberapa manfaat utama yang dapat kita ketahui (Haryadi, 2024):

### 1. Efisiensi dan Penghematan Biaya

Dengan memanfaatkan virtualisasi, Anda dapat meningkatkan penggunaan sumber daya perangkat keras dan mengurangi jumlah server fisik yang diperlukan. Hal ini mengurangi biaya operasional, seperti energi dan pendinginan, serta biaya pemeliharaan. Cloud computing memungkinkan Anda untuk membayar sesuai dengan

penggunaan, sehingga Anda tidak perlu menginvestasikan dalam infrastruktur yang mahal.

## 2. Stabilitas dan Fleksibilitas

Virtualisasi dan cloud computing memungkinkan Anda untuk menyesuaikan sumber daya komputasi sesuai dengan kebutuhan, tanpa harus menambah atau mengurangi perangkat keras secara fisik. Anda dapat dengan mudah menambah kapasitas penyimpanan atau memproses saat dibutuhkan, dan mengurangnya saat tidak lagi diperlukan.

## 3. Aksesibilitas dan Mobilitas

Cloud computing memungkinkan Anda mengakses data dan aplikasi dari mana saja, kapan saja, asalkan Anda memiliki koneksi internet. Hal ini memudahkan kolaborasi antar pengguna dan meningkatkan produktivitas, terutama bagi pekerja jarak jauh atau tim yang tersebar di berbagai lokasi.

## 4. Pemeliharaan dan Pembaharuan Otomatis

Dalam model cloud computing, penyedia layanan bertanggung jawab untuk pemeliharaan dan pembaharuan infrastruktur dan perangkat lunak. Hal ini mengurangi beban pemeliharaan sistem di pihak Anda dan memastikan bahwa Anda selalu memiliki versi terbaru dari aplikasi yang digunakan.

## 5. Keamanan dan Pemulihan Data

Penyedia layanan cloud computing umumnya memiliki kebijakan keamanan yang ketat dan redundansi data untuk melindungi informasi. Selain itu, penyedia layanan sering menawarkan solusi pemulihan data dalam hal kehilangan atau kerusakan data, sehingga kita tidak perlu khawatir tentang kehilangan informasi penting lagi.

## 8.10 Sumber Daya Yang Dapat Divirtualisasi

Virtualisasi adalah proses mengabstraksi sumber daya fisik ke kumpulan sumber daya virtual yang dapat diberikan ke mesin virtual (VM) apa pun. Sumber daya yang berbeda seperti memori, prosesor, penyimpanan, dan jaringan dapat divirtualisasikan menggunakan teknologi virtualisasi yang tepat.

Beberapa sumber daya yang dapat divirtualisasikan (Santoso, 2023):

### 1. Virtualisasi Prosesor

Virtualisasi prosesor memungkinkan VM untuk berbagi prosesor virtual yang disarikan dari prosesor fisik yang tersedia di infrastruktur dasar. Lapisan virtualisasi memisahkan prosesor fisik ke kumpulan prosesor virtual yang digunakan bersama oleh VM. Lapisan virtualisasi biasanya berupa hypervisor apa saja.

### 2. Virtualisasi Memori

Teknik virtualisasi sumber daya penting lainnya adalah virtualisasi memori. Proses penyediaan memori utama virtual ke VM dikenal sebagai virtualisasi memori atau virtualisasi memori utama. Dalam virtualisasi memori utama, memori utama fisik dipetakan ke memori utama virtual seperti pada konsep memori virtual di sebagian besar OS. Ide utama virtualisasi memori utama adalah memetakan nomor halaman virtual ke nomor halaman fisik. Semua prosesor x86 modern mendukung virtualisasi memori utama.

Virtualisasi memori utama juga dapat dicapai dengan menggunakan perangkat lunak hypervisor. Biasanya, di pusat data tervirtualisasi, memori utama yang tidak terpakai dari berbagai

server akan dikonsolidasikan sebagai kumpulan memori utama virtual dan dapat diberikan ke VM.

### 3. Virtualisasi Penyimpanan

Virtualisasi penyimpanan adalah bentuk virtualisasi sumber daya di mana beberapa disk penyimpanan fisik diabstraksikan sebagai kumpulan disk penyimpanan virtual ke VM. Biasanya, penyimpanan virtual akan disebut penyimpanan logis.

Virtualisasi penyimpanan terutama digunakan untuk memelihara cadangan atau replika data yang disimpan di VM. Ini dapat diperluas lebih lanjut untuk mendukung ketersediaan data yang tinggi. Itu juga dapat dicapai melalui hypervisor. Ini secara efisien menggunakan penyimpanan fisik yang mendasarinya. Teknik virtualisasi penyimpanan lanjutan lainnya adalah jaringan area penyimpanan (SAN) dan penyimpanan yang terpasang di jaringan (NAS).

### 4. Virtualisasi Jaringan

Virtualisasi jaringan adalah jenis virtualisasi sumber daya di mana jaringan fisik dapat diabstraksi untuk membuat jaringan virtual. Biasanya, komponen jaringan fisik seperti router, switch, dan Network Interface Card (NIC) akan dikendalikan oleh perangkat lunak virtualisasi untuk menyediakan komponen jaringan virtual. Jaringan virtual adalah entitas berbasis perangkat lunak tunggal yang berisi perangkat keras jaringan dan sumber daya perangkat lunak.

Virtualisasi jaringan dapat dicapai dari jaringan internal atau dengan menggabungkan banyak jaringan eksternal. Keuntungan lain dari virtualisasi jaringan adalah memungkinkan komunikasi antara VM yang berbagi jaringan fisik. Ada berbagai jenis akses

jaringan yang diberikan ke VM seperti jaringan yang dijembatani, terjemahan alamat jaringan (NAT), dan host saja.

#### 5. Virtualisasi Data

Virtualisasi data adalah kemampuan untuk mengambil data tanpa mengetahui jenisnya dan lokasi fisik tempat penyimpanannya. Ini mengumpulkan data heterogen dari sumber yang berbeda ke volume data logis/virtual tunggal. Data logis ini dapat diakses dari berbagai aplikasi seperti layanan web, aplikasi E-commerce, portal web, aplikasi Software as a Service (SaaS), dan aplikasi seluler.

Virtualisasi data menyembunyikan jenis data dan lokasi data untuk aplikasi yang mengaksesnya. Ini juga memastikan akses titik tunggal ke data dengan menggabungkan data dari berbagai sumber. Ini terutama digunakan dalam integrasi data, intelijen bisnis, dan komputasi awan.

#### 6. Virtualisasi Aplikasi

Virtualisasi aplikasi menawarkan kemampuan kepada pengguna untuk menggunakan aplikasi tanpa perlu menginstal perangkat lunak atau alat apa pun di mesin. Di sini, kerumitan penginstalan alat klien atau perangkat lunak lain yang didukung berkurang. Biasanya, aplikasi akan dikembangkan dan dihosting di server pusat. Aplikasi yang dihosting akan divirtualisasikan lagi, dan pengguna akan diberikan salinan virtual yang terpisah/terisolasi untuk diakses (Huawei Technologies Co., 2023).

## 8.11 Keuntungan dari Virtualisasi

Keuntungan operasional dan finansial dari virtualisasi adalah kunci dari komputasi enterprise dan lingkungan pengembangan perangkat lunak dapat disediakan oleh Virtualisasi.

Berikut ini adalah keuntungan utama dari virtualisasi (Umar, 2013):

1. Menggunakan perangkat keras yang ada dengan lebih baik  
Beberapa dekade terakhir, prosesor telah berubah dari 8bit ke 16bit ke 32bit dan sekarang ke 64 bit. Tiap perkembangan ini akan menaikkan ukuran prosesor dan meningkatkan jumlah memori dan ukuran media penyimpan yang dapat diakses oleh prosesor. Begitu juga dengan kecepatan dan kepadatan prosesor terus bertambah, dimana saat ini prosesor dapat dengan mudah melampaui 2GHz, dan mempunyai banyak inti prosesor di tiap cipnya.  
Menjalankan beberapa mesin virtual pada server yang telah ada akan mengefisienkan penggunaan server tersebut. Multi prosesor atau multi-core system bahkan dapat menjalankan mesin virtual yang berbeda pada inti prosesor yang berbeda, hal ini mengambil keuntungan dari tiap inti prosesor.
2. Mengurangi Harga Perangkat Keras  
Dengan virtualisasi tidak diperlukan lagi untuk membeli perangkat keras baru bila diinginkan untuk menambah server atau layanan. Menambah server atau layanan akan menambah kepuasan pelanggan/pengguna.
3. Mengurangi Infrastruktur IT  
Setiap server fisik menggunakan listrik tertentu, ruang tertentu dan sistem pendinginan tertentu. Dengan mesin virtual maka kebutuhan listrik, kebutuhan ruang dan sistem pendingin tetap.

#### 4. Menyederhanakan Sistem Administrasi

Menjalankan beberapa mesin virtual pada sebuah mesin fisik, memengaruhi kesehatan dari sistem tersebut dan membutuhkan sebuah infrastruktur perangkat lunak untuk migrasi atau cloning bila terjadi kesalahan perangkat keras.

#### 5. Meningkatkan Uptime Dan Mempercepat Failure Recovery

Portabilitas dari mesin virtual akan membuatnya mudah untuk dipindahkan dari server yang lain jika ada kesalahan perangkat keras. Mesin virtual Xen dapat dipindahkan tanpa mengganggu performanya, proses migrasinya transparan bila dilihat oleh pengguna, dan proses yang menggunakannya.

#### 6. Menyederhanakan Ekspansi Kapasitas

Mesin virtual dapat dipindahkan dari satu mesin fisik ke mesin fisik yang lain sehingga bisa mengambil keuntungan dari peningkatan perangkat keras, seperti CPU yang lebih kuat, tambahan inti CPU, tambahan memori, tambahan dan kartu jaringan dan lain-lain.

#### 7. Lebih sederhana dalam dukungan perangkat lunak asli

Dengan menjalankan sistem operasi dalam partisi logika, pengguna dapat meningkatkan ke sistem operasi yang baru, tanpa kehilangan kemampuan untuk mengoperasikan perangkat lunak aslinya.

#### 8. Menyederhanakan Pengembangan System-Level

Solusi tradisional untuk testing kernel dan driver adalah dengan me-reboot kernel tersebut, tapi dengan adanya mesin virtual, maka reboot menjadi lebih cepat dari pada reboot pada mesin fisik. Pendekatan ini juga penting untuk low-level debugging jika memakai mesin virtual karena lingkungan pengembangan, sistem pengembangan dan mesin virtual semuanya dapat berada dalam satu desktop pada waktu yang sama.

#### 9. Menyederhanakan Instalasi dan Deployment Sistem

Dengan menggunakan sistem pengembangan yang tidak tergantung dengan perangkat keras tertentu, maka akan sangat mudah untuk migrasi sistem tersebut ke tempat yang lebih cepat, lebih kuat, lebih baik perangkat input outputnya dan seterusnya.

#### 10. Menyederhanakan sistem dan Testing Aplikasi

Instalasi produk perangkat lunak yang tidak membutuhkan perangkat keras khusus dan mengujinya pada banyak sistem operasi yang berbeda akan menjadi mudah dengan adanya virtualisasi server.

## 8.12 Kerugian dari Virtualisasi

Banyak alasan untuk menggunakan virtualisasi dalam lingkungan komputasi.

Walau demikian tetap saja masih ada kekurangan dari adanya teknologi virtualisasi yaitu (Umar, 2013):

#### 1. Satu Titik Kesalahan

Kelemahan dari virtualisasi server adalah menaikkan kemungkinan kesalahan pada sebuah perangkat keras yang ditempati oleh beberapa server virtual. Jika banyak server dan layanan yang berhubungan dengannya berjalan pada mesin masing-masing, maka kesalahan pada satu mesin akan berakibat hanya pada satu server saja. Berbeda dengan beberapa server yang menempati sebuah mesin, kesalahan pada mesin akan mengakibatkan kesalahan pada seluruh server virtual.

Untuk menangani hal ini maka ada langkah dan rencana khusus, yang diantaranya adalah:

- a. Set up perangkat keras cadangan seperti network interface cards pada sistem host, dan satukan seluruhnya sehingga kesalahan pada sebuah kartu akan terlihat oleh mesin virtual.
  - b. Beli dan pelihara perangkat keras duplikat untuk sistem fisik yang ditempati oleh mesin virtual yang penting.
  - c. Replikasikan mesin virtual yang ditempati oleh layanan yang amat penting ke seluruh perangkat keras, sehingga kesalahan pada perangkat keras yang satu dapat diback up perangkat keras yang lain.
  - d. Jalankan perangkat lunak sistem monitoring terpusat untuk memberi tahu bila ada kesalahan perangkat keras atau perangkat lunak sebelum kesalahan itu menjadi kritis. Hal ini memberi kesempatan untuk memindahkan layanan yang terpengaruh ke mesin fisik yang lain
2. Kepadatan Saluran Jaringan

Sebagian besar sistem virtualisasi penuh menggunakan kartu jaringan virtual, subnet virtual dan menjembatani paket untuk dipetakan ke perangkat keras fisik. Jika host fisik hanya menyediakan sebuah kartu jaringan, dan menjalankan beberapa mesin virtual yang mengeksekusi network intensive task, maka permintaan layanan ke sebuah kartu jaringan menjadi sangat padat. Untuk menangani hal ini, adalah dengan menginstal beberapa kartu jaringan pada host fisik dan menghubungkan masing-masing kartu ke mesin virtual. Sayangnya dengan menerapkan hal ini akan menambah kesulitan dalam memigrasi sebuah mesin virtual dari mesin fisik yang satu ke mesin fisik yang lain.

### 3. Menaikkan Kompleksitas Jaringan dan Waktu Debug

Penggunaan virtual network interfaces dan mesin virtual membuat manajemen jaringan menjadi lebih rumit, sehingga desain dan perancangan infrastruktur mesin virtual harus sangat cermat dan memakan banyak waktu.

### 4. Menaikkan kompleksitas Administrasi

Sebelumnya telah disebutkan tentang menyederhanakan sistem administrasi. Hal ini tidak berlaku bila menggunakan sistem manajemen terdistribusi yang tidak mengenal mesin virtual. Untuk itu berhati-hatilah saat membeli virtual mesin, yaitu virtual mesin yang dapat berkomunikasi dengan sistem manajemen terdistribusi.

## 8.13 Dari Virtualisasi Ke Cloud Computing

Banyak pengguna solusi TI saat ini menganggap teknologi virtualisasi dan komputasi awan sebagai hal yang sama. Namun kedua teknologi tersebut sebenarnya berbeda, atau dengan kata lain virtualisasi bukanlah cloud computing.

Kami dapat membuktikan klaim ini dengan parameter berikut (Santoso, 2023):

1. Jenis layanan: Umumnya, virtualisasi menawarkan lebih banyak layanan infrastruktur daripada layanan platform dan aplikasi. Tetapi komputasi awan menawarkan semua layanan infrastruktur (IaaS), platform (PaaS), dan perangkat lunak (SaaS).
2. Pengiriman layanan: Pengiriman layanan dalam komputasi awan sesuai permintaan dan memungkinkan pengguna akhir untuk

menggunakan layanan awan sesuai kebutuhan. Tetapi virtualisasi tidak dibuat untuk layanan sesuai permintaan.

3. Penyediaan layanan: Dalam komputasi awan, penyediaan otomatis dan swalayan dimungkinkan untuk pengguna akhir, sedangkan dalam virtualisasi, tidak mungkin dan banyak pekerjaan manual diperlukan dari penyedia atau administrator sistem untuk menyediakan layanan kepada pengguna akhir.
4. Orkestrasi layanan: Cloud computing memungkinkan orkestrasi layanan dan komposisi layanan untuk memenuhi kebutuhan pengguna akhir. Beberapa penyedia juga menyediakan orkestrasi layanan otomatis kepada pengguna akhir. Namun dalam virtualisasi, mengatur layanan yang berbeda untuk mendapatkan layanan komposit tidak dimungkinkan.
5. Elastisitas: Salah satu karakteristik penting yang membedakan komputasi awan dari virtualisasi adalah elastisitas. Dalam cloud computing, kita dapat menambah atau menghapus infrastruktur secara dinamis sesuai dengan kebutuhan, dan menambah atau menghapus infrastruktur secara otomatis. Tetapi virtualisasi gagal memberikan elastisitas karena menghentikan dan memulai VM bersifat manual dan juga sulit.
6. Pemirsanya yang ditargetkan: Pemirsanya yang ditargetkan dari kedua teknologi ini juga berbeda. Komputasi awan menargetkan penyedia layanan untuk pemanfaatan sumber daya yang tinggi dan ROI yang lebih baik. Pada saat yang sama, ini juga memfasilitasi pengguna akhir untuk menghemat uang dengan menggunakan layanan sesuai permintaan. Dalam kasus virtualisasi, audiens yang ditargetkan hanyalah penyedia layanan atau pemilik TI, bukan pengguna akhir.

Dengan pembahasan singkat ini, dapat disimpulkan bahwa cloud computing dan virtualisasi itu berbeda. Karena cloud computing menggunakan virtualisasi untuk penyampaian layanannya. Komputasi awan dapat berjalan di lingkungan virtual apa pun karena virtualisasi adalah salah satu teknologi yang memungkinkan untuk komputasi awan.

Tentu saja, tanpa virtualisasi, komputasi awan mungkin tidak ada. Komputasi awan menggunakan virtualisasi untuk pemanfaatan sumber daya yang lebih baik dan digabungkan dengan komputasi utilitas untuk menguntungkan penyedia layanan, pengembang, dan pengguna akhir. Dengan kata lain, kita dapat mengatakan bahwa komputasi awan membawa virtualisasi ke langkah selanjutnya. Komputasi awan dan virtualisasi menyatu dalam pemanfaatan sumber daya yang lebih baik, dan virtualisasi berhenti di sana sedangkan komputasi awan bergerak selangkah lebih maju dan bergabung dengan komputasi utilitas untuk menyediakan TI sebagai layanan.

Virtualisasi digunakan sebagai teknologi yang memungkinkan untuk menyediakan infrastruktur multitenant, platform pengembangan, dan SaaS. Selain itu, ada layanan cloud lain yang menggunakan virtualisasi seperti Network as a Service menggunakan virtualisasi jaringan, Penyimpanan sebagai Layanan menggunakan virtualisasi penyimpanan, dan Database sebagai Layanan menggunakan virtualisasi basis data.

# Bab 9

## Manajemen Proyek Sistem Informasi Berbasis Cloud

### 9.1 Pengantar Manajemen Proyek Sistem Informasi

#### 9.1.1 Definisi Manajemen Proyek dalam Konteks Sistem Informasi

Manajemen proyek adalah penerapan pengetahuan, keterampilan, alat, dan teknik untuk mengarahkan aktivitas proyek agar memenuhi persyaratan proyek (Project Management Institute, 2017). Dalam konteks sistem informasi (SI), manajemen proyek mencakup perencanaan, pengorganisasian, pengendalian, dan pengawasan terhadap pembangunan atau pengembangan sistem informasi, baik berupa perangkat lunak, infrastruktur IT, maupun integrasi teknologi (Schwalbe, 2021).

Proyek sistem informasi sering kali bersifat kompleks karena melibatkan berbagai aspek seperti teknologi, proses bisnis, sumber daya manusia, dan aspek keamanan informasi (MarnewickErasmus and Nazeer, 2018). Oleh karena itu, manajemen proyek dalam bidang ini harus mampu menyelaraskan antara kebutuhan bisnis dan kemampuan teknis untuk memastikan keberhasilan implementasi sistem informasi.

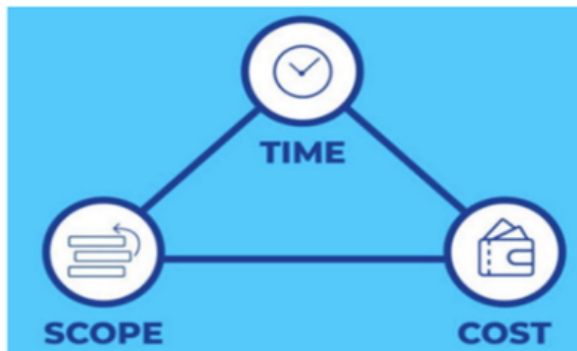
### 9.1.2 Peran Penting Manajemen Proyek dalam Keberhasilan Sistem Informasi

Manajemen proyek berperan krusial dalam menentukan apakah sebuah sistem informasi dapat berhasil diimplementasikan dan memberikan nilai tambah kepada organisasi (SilvaPereira and Magano, 2021).

Beberapa peran pentingnya antara lain:

1. **Mengelola Keterbatasan Proyek (Triple Constraint):** Menyeimbangkan antara cakupan proyek (scope), waktu (time), dan biaya (cost) agar tetap sesuai dengan tujuan.
2. **Memastikan Kualitas:** Menjaga kualitas hasil akhir sesuai standar yang ditentukan.
3. **Mengelola Risiko:** Mengidentifikasi dan memitigasi potensi risiko yang bisa menghambat proyek.
4. **Koordinasi Tim Multidisiplin:** Mengelola komunikasi dan kolaborasi antara tim teknis, pengguna, manajemen, dan pemangku kepentingan lainnya.
5. **Dokumentasi dan Pelaporan:** Menyediakan laporan kemajuan dan dokumentasi penting untuk pertanggungjawaban dan evaluasi proyek.
6. **Meningkatkan Kepuasan Pengguna:** Dengan memastikan bahwa sistem informasi yang dikembangkan sesuai dengan kebutuhan dan harapan pengguna akhir.

Tanpa manajemen proyek yang baik, sistem informasi berbasis cloud mengalami kegagalan baik dari segi waktu, anggaran, maupun fungsionalitas.



**Gambar 9.1:** Triple Constraint (Panchal and Khokrale, 2024)

Gambar 9.1 di atas menunjukkan tiga hal terkait dengan keterbatasan proyek antara lain: waktu, biaya, dan cakupan proyek.

### 9.1.3 Perbedaan Manajemen Proyek Tradisional vs Berbasis Cloud

Berikut ini merupakan perbedaan antara manajemen proyek tradisional dengan manajemen proyek berbasis Cloud.

**Tabel 9.1:** Proyek Tradisional vs Proyek Berbasis Cloud

Aspek	Proyek Tradisional	Proyek Berbasis Cloud
Infrastruktur	Infrastruktur dikelola internal (on-premise)	Infrastruktur disediakan pihak ketiga (cloud provider)
Fleksibilitas	Terbatas, sering memerlukan investasi awal besar	Lebih fleksibel, bisa skalabel sesuai kebutuhan
Tim Proyek	Sering berada dalam satu	Tim dapat tersebar secara geografis

Aspek	Proyek Tradisional	Proyek Berbasis Cloud
	lokasi	(remote/collab online)
Pendekatan Pengembangan	Cenderung menggunakan model waterfall	Lebih adaptif terhadap Agile, DevOps, CI/CD
Manajemen Risiko	Fokus pada risiko teknis internal	Risiko meluas ke keamanan data, ketergantungan vendor, SLA
Biaya dan Anggaran	Investasi awal tinggi (CapEx)	Lebih banyak menggunakan biaya operasional (OpEx)

Manajemen proyek berbasis cloud menuntut pendekatan baru yang lebih dinamis, kolaboratif, dan berorientasi pada layanan. Perubahan cepat dalam teknologi cloud juga mengharuskan manajer proyek untuk terus memperbarui pengetahuan dan keterampilannya.

## 9.2 Ruang Lingkup Proyek Sistem Informasi Berbasis Cloud

### 9.2.1 Jenis-jenis Proyek SI yang Umum Berbasis Cloud

Dalam era transformasi digital, organisasi semakin mengandalkan cloud computing sebagai fondasi utama dalam pengembangan dan pengelolaan sistem informasi (SI) (Bibi et al., 2024).

Berikut ini adalah jenis-jenis proyek SI yang umum berbasis cloud:

1. Migrasi ke Cloud (Cloud Migration Projects)
  - a. Proyek ini bertujuan untuk memindahkan aplikasi, data, dan infrastruktur TI dari lingkungan lokal (on-premise) ke lingkungan cloud.
  - b. Contoh: Migrasi email perusahaan dari server lokal ke Microsoft 365 atau Google Workspace.
  - c. Fokus utama: kelayakan migrasi, pemilihan penyedia layanan cloud, pemindahan data yang aman, dan validasi pasca-migrasi.
2. Pengembangan Aplikasi Cloud-Native
  - a. Merancang dan membangun aplikasi dari awal agar memanfaatkan sepenuhnya kapabilitas cloud, seperti container, microservices, dan serverless architecture.
  - b. Contoh: Aplikasi layanan pelanggan yang dibangun dengan teknologi Kubernetes dan dijalankan di AWS Lambda.
  - c. Kelebihan: Skalabilitas otomatis, ketersediaan tinggi, dan efisiensi biaya.
3. Integrasi Layanan SaaS (Software as a Service)
  - a. Integrasi aplikasi pihak ketiga berbasis cloud ke dalam sistem internal organisasi.
  - b. Contoh: Integrasi Salesforce (CRM) dengan ERP internal organisasi.
  - c. Fokus pada kompatibilitas API, keamanan data antar sistem, dan orkestrasi proses bisnis.
4. Automasi dan Orkestrasi Cloud
  - a. Proyek ini mencakup penggunaan alat manajemen cloud (seperti Terraform, Ansible) untuk otomatisasi deployment dan pengelolaan infrastruktur.

- b. Tujuannya adalah meningkatkan efisiensi dan mengurangi kesalahan manual.
5. Penguatan Infrastruktur dan Keamanan Cloud  
Menangani proyek untuk meningkatkan kontrol akses, audit log, enkripsi, serta penerapan kebijakan keamanan cloud.

Catatan: Proyek-proyek ini sering kali tumpang tindih dan bersifat iteratif, menuntut pendekatan manajemen proyek yang fleksibel dan adaptif seperti Agile atau DevOps.

### 9.2.2 Kebutuhan dan Tantangan Unik dalam Proyek Cloud

Setiap proyek sistem informasi memiliki karakteristik yang berbeda tergantung pada teknologi yang digunakan. Dalam konteks cloud computing, proyek memiliki kebutuhan khusus yang tidak selalu ditemukan dalam proyek TI konvensional. Misalnya, ketergantungan terhadap penyedia layanan pihak ketiga, kebutuhan integrasi lintas platform, serta kepatuhan terhadap regulasi data menjadi faktor penting yang harus diperhitungkan sejak awal.

Di sisi lain, tantangan seperti perubahan teknologi yang cepat, pengelolaan tim virtual, hingga kontrol biaya berbasis konsumsi menjadikan proyek cloud lebih kompleks (J and M, 2024). Oleh karena itu, memahami kebutuhan dan tantangan unik ini sangat penting untuk memastikan perencanaan dan pelaksanaan proyek berjalan sukses dan berkelanjutan.

Kebutuhan dalam Proyek Cloud:

1. Pemilihan Arsitektur dan Model Layanan Cloud yang Tepat  
Pemahaman yang kuat terhadap kebutuhan bisnis untuk memilih antara IaaS, PaaS, atau SaaS.
2. Pemahaman Regulasi dan Kepatuhan  
Kebutuhan akan kepatuhan terhadap peraturan data lokal (misal: GDPR, UU Perlindungan Data Pribadi).

### 3. Monitoring dan SLA

Harus ada mekanisme pemantauan performa dan kesesuaian terhadap SLA yang disepakati.

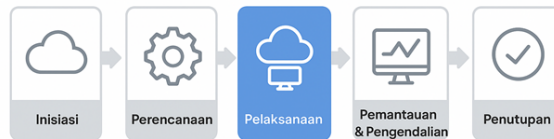
Tantangan Unik Proyek Cloud:

1. Ketergantungan terhadap Vendor Cloud (Vendor Lock-in)  
Sulitnya berpindah layanan karena perbedaan standar dan arsitektur antar penyedia.
2. Manajemen Biaya Dinamis  
Biaya cloud berbasis konsumsi (pay-as-you-go) memerlukan pengendalian dan optimalisasi yang cermat.
3. Kompleksitas Integrasi  
Integrasi dengan sistem lama (legacy systems) sering memerlukan rekayasa tambahan.
4. Keamanan dan Privasi Data  
Perlu perhatian lebih pada autentikasi, otorisasi, enkripsi, serta audit akses pengguna.
5. Perubahan Kultural dan Organisasional  
Perlu adopsi keterampilan baru dan pendekatan kerja lintas fungsi (DevOps, tim lintas lokasi).

## 9.3 Siklus Hidup Proyek Cloud

Manajemen proyek sistem informasi berbasis cloud tetap mengikuti siklus hidup proyek secara umum, sebagaimana dijelaskan dalam PMBOK® Guide (Project Management Institute, 2021). Namun, ada karakteristik khusus yang perlu diperhatikan karena keterlibatan teknologi cloud yang dinamis, skalabel, dan tergantung pada penyedia layanan eksternal.

Tahapan Proyek terlihat pada Gambar 9.2, yang terdiri dari lima tahapan besar dari Inisiasi, Perencanaan, Pelaksanaan, Pemantauan & Pengendalian, dan Penutupan Proyek.



**Gambar 9.2:** Tahapan Proyek

Gambar 9.2 di atas menunjukkan tahapan proyek dari Inisiasi hingga Penutupan Proyek, akan di jabarkan lebih detil pada penjelasan berikut ini.

Tahapan Proyek:

#### 1. Inisiasi (Initiation)

Tahap awal untuk mendefinisikan tujuan, ruang lingkup awal, dan kelayakan proyek. Melibatkan identifikasi kebutuhan bisnis, pemilihan model cloud yang sesuai, serta penyusunan dokumen inisiasi proyek (project charter). Tujuannya adalah untuk mendapatkan persetujuan manajemen agar proyek dapat dilanjutkan ke tahap berikutnya.

Penekanan Cloud:

- Evaluasi opsi cloud (public, private, hybrid).
- Analisis vendor cloud dan pemilihan model layanan (IaaS, PaaS, SaaS).
- Identifikasi risiko awal seperti lokasi data dan kepatuhan hukum (regulasi data lokal).

#### 2. Perencanaan (Planning)

Pada tahap ini dilakukan perumusan rencana terperinci terkait jadwal, anggaran, sumber daya, pengelolaan risiko, komunikasi, serta pemilihan vendor cloud. Perencanaan juga mencakup pemetaan arsitektur cloud, strategi keamanan, dan penetapan

indikator kinerja (KPI & SLA) untuk memastikan proyek berjalan sesuai target.

Penekanan Cloud:

- a. Perencanaan arsitektur cloud (misalnya *microservices*, *multi-cloud*).
- b. Estimasi biaya berbasis konsumsi (*usage-based pricing*).
- c. Perencanaan keamanan cloud (*access control*, enkripsi, *backup*).

### 3. Pelaksanaan (Execution)

Tahap di mana rencana proyek diimplementasikan secara nyata. Aktivitas mencakup *deployment* layanan cloud, migrasi data, pengembangan aplikasi *cloud-native* (jika ada), pelatihan pengguna, dan integrasi sistem. Proses ini membutuhkan kolaborasi lintas tim dan penggunaan tools cloud yang mendukung otomatisasi dan efisiensi kerja.

Implementasi dari rencana proyek, termasuk pembangunan atau integrasi sistem cloud.

Aktivitas utama:

- a. Pengembangan atau konfigurasi layanan cloud.
- b. Integrasi dengan sistem eksisting.
- c. Pelatihan pengguna dan pengujian sistem.

Penekanan Cloud:

- a. Otomatisasi *deployment* (menggunakan tools seperti *Terraform*, *Jenkins*).
- b. *Provisioning* layanan cloud melalui panel atau API.
- c. *Monitoring* performa awal dan penggunaan sumber daya.

#### 4. Pemantauan & Pengendalian (Monitoring & Controlling)

Tahap pengawasan proyek agar tetap berjalan sesuai rencana. Dilakukan melalui pelacakan progres, pemantauan performa sistem, pengukuran terhadap KPI dan SLA, serta penanganan deviasi atau risiko yang muncul. Tools monitoring cloud seperti AWS CloudWatch atau Azure Monitor biasanya digunakan dalam fase ini.

Melakukan pengawasan terhadap kinerja proyek, mencocokkan antara rencana dengan realisasi.

Aktivitas utama:

- a. Pelacakan jadwal, biaya, dan kualitas.
- b. Pengelolaan perubahan dan isu.
- c. Evaluasi risiko yang sedang berlangsung.

Penekanan Cloud:

- a. Pemantauan SLA dari penyedia cloud.
- b. Pemantauan metrik real-time (latensi, throughput, pemakaian CPU/RAM).
- c. Penggunaan cloud-native monitoring tools (misal: AWS CloudWatch, Azure Monitor).

#### 5. Penutupan (Closing)

Tahap akhir untuk menyelesaikan semua aspek proyek, termasuk serah terima sistem kepada pengguna, dokumentasi akhir, evaluasi keberhasilan proyek, dan pembelajaran untuk proyek mendatang. Penutupan juga melibatkan validasi SLA, audit keamanan akhir, dan rencana operasional jangka panjang.

Penekanan Cloud:

- a. Validasi akses, pemisahan peran (role separation), dan audit konfigurasi akhir.

- b. Transfer knowledge terkait pengelolaan cloud.
- c. Evaluasi performa cloud dan optimalisasi untuk pasca proyek.

## 9.4 Metodologi dan Kerangka Kerja dalam Proyek Cloud

Dalam proyek sistem informasi berbasis cloud, penggunaan metodologi manajemen proyek tidak hanya penting untuk pengendalian proses, tetapi juga harus mampu mengakomodasi dinamika, skalabilitas, dan kompleksitas teknologi cloud (AlabiMustapha and Akinade, 2025). Pendekatan seperti Agile, DevOps, dan Hybrid menjadi semakin relevan dibandingkan model tradisional seperti waterfall.

### 9.4.1 Agile dalam Proyek Cloud

Agile adalah pendekatan iteratif dan inkremental yang berfokus pada kolaborasi, fleksibilitas, pengiriman produk yang cepat, dan respon terhadap perubahan.

Ciri Khas:

1. Pendekatan berbasis sprint (iterasi waktu singkat)
2. Fokus pada kolaborasi tim dan keterlibatan pengguna
3. Cocok untuk proyek cloud-native dan pengembangan aplikasi SaaS

Kelebihan dalam konteks cloud:

1. Cocok dengan dinamika cloud: Agile mendukung perubahan cepat dalam kebutuhan bisnis dan teknologi cloud.
2. Mudah diintegrasikan dengan CI/CD: Penyedia layanan cloud mendukung pipeline otomatisasi untuk pengujian dan deployment.

## 9.4.2 DevOps dalam Proyek Cloud

DevOps adalah pendekatan yang menggabungkan pengembangan (development) dan operasional (operations) untuk mempercepat siklus rilis dan meningkatkan kualitas aplikasi.

Prinsip DevOps:

1. Automasi: Continuous Integration/Continuous Deployment (CI/CD)
2. Kolaborasi: Penghapusan sekat antara tim pengembang dan operasional
3. Monitoring: Pemantauan real-time sistem dan performa

Manfaat DevOps dalam cloud:

1. Sangat cocok untuk cloud-native apps yang sering berubah dan berskala tinggi.
2. Cloud-friendly tools seperti Jenkins, Docker, Kubernetes, GitLab CI/CD, dan cloud CLI/API memudahkan orkestrasi dan deployment.

## 9.4.3 Pendekatan Hybrid dalam Proyek Cloud

Hybrid methodology menggabungkan elemen dari Agile, DevOps, dan metode tradisional sesuai dengan konteks proyek.

Contoh hybrid:

1. Agile untuk fase pengembangan aplikasi (iteratif)
2. Waterfall untuk aspek regulasi dan kepatuhan (yang memerlukan dokumentasi formal)
3. DevOps untuk fase deployment dan monitoring berkelanjutan

Kapan menggunakan pendekatan hybrid?:

1. Saat proyek mencakup sistem legacy dan cloud secara bersamaan

2. Dalam organisasi dengan kebutuhan kepatuhan formal (misalnya sektor finansial atau pemerintahan)
3. Ketika transisi dari infrastruktur lokal ke cloud memerlukan tahapan bertahap

Kesesuaian Metodologi dengan Jenis Layanan Cloud

**Tabel 9.2:** Kesesuaian Metodologi dengan Jenis Layanan Cloud

Jenis Layanan Cloud	Metodologi yang Cocok	Penjelasan
<b>IaaS</b> (Infrastructure as a Service)	DevOps, Hybrid	Karena pengelolaan infrastruktur penting, DevOps mendukung provisioning otomatis dan monitoring.
<b>PaaS</b> (Platform as a Service)	Agile, DevOps	Mendukung pengembangan cepat berbasis platform, cocok untuk iterasi aplikasi.
<b>SaaS</b> (Software as a Service)	Agile, DevOps	Cocok untuk pengembangan aplikasi yang berfokus pada kebutuhan pengguna dan fitur cepat rilis.

## 9.5 Perencanaan Proyek Sistem Informasi Cloud

Tahap perencanaan adalah fondasi keberhasilan proyek sistem informasi berbasis cloud. Pada tahap ini, semua aspek teknis, bisnis, operasional, serta risiko harus dipertimbangkan dan direncanakan secara terstruktur agar proyek berjalan dengan efisien dan memberikan nilai bisnis yang maksimal (Ayele, 2023).

### 9.5.1 Identifikasi Kebutuhan Cloud dan Pemilihan Vendor

#### 1. Identifikasi Kebutuhan Cloud:

Perencanaan dimulai dari pemahaman menyeluruh terhadap kebutuhan bisnis dan teknis yang akan dipenuhi oleh cloud, antara lain:

- a. Skalabilitas: Apakah solusi perlu berkembang sesuai volume pengguna?
- b. Fleksibilitas: Apakah memerlukan arsitektur modular atau cloud-native?
- c. Kepatuhan: Apakah data harus disimpan di wilayah hukum tertentu?
- d. Keamanan: Tingkat perlindungan data dan privasi yang dibutuhkan.

#### 2. Pemilihan Vendor Cloud:

Proses seleksi vendor perlu mempertimbangkan:

- a. Model layanan: IaaS, PaaS, atau SaaS.
- b. Biaya dan struktur harga: Pay-as-you-go, reserved instance, dll.
- c. SLA dan uptime: Jaminan ketersediaan sistem (misal: 99.99% uptime).
- d. Kompatibilitas dan integrasi: Dukungan terhadap sistem lama (legacy).
- e. Dukungan teknis dan dokumentasi: Ketersediaan support 24/7, dokumentasi API.
- f. Reputasi dan compliance: Sertifikasi keamanan (ISO 27001, SOC 2, dll).

### 9.5.2 Estimasi Biaya, Waktu, dan Sumber Daya

1. Estimasi Biaya:
  - a. Biaya penggunaan layanan (storage, compute, bandwidth).
  - b. Biaya setup awal (migrasi, konfigurasi).
  - c. Biaya lisensi, pelatihan, dan manajemen proyek.
  - d. Tools bantu estimasi biaya:
    - 1) AWS Pricing Calculator
    - 2) Azure Pricing Tool
    - 3) Google Cloud Cost Estimator
2. Estimasi Waktu:
  - a. Waktu konfigurasi dan provisioning infrastruktur cloud.
  - b. Waktu migrasi data dan sistem lama.
  - c. Siklus sprint (jika menggunakan Agile).
  - d. Buffer untuk testing, debugging, dan approval.
3. Estimasi Sumber Daya:
  - a. Manusia: Project manager, cloud architect, devops engineer, QA tester.
  - b. Teknologi: Tools CI/CD, platform monitoring, backup system.
  - c. Organisasi: Dukungan dari manajemen dan pengguna akhir.

### 9.5.3 Penentuan Parameter Keberhasilan Proyek Cloud

Untuk menilai keberhasilan proyek cloud, perlu ditetapkan indikator atau parameter keberhasilan yang objektif dan terukur:

**Tabel 9.3:** Parameter Keberhasilan Proyek Cloud

Kategori	Parameter
Teknis	<ul style="list-style-type: none"> <li>• Uptime dan reliabilitas sistem</li> <li>• Performa sistem (response time, throughput)</li> </ul>

Operasional	<ul style="list-style-type: none"> <li>• Waktu delivery sesuai rencana</li> <li>• Efisiensi penggunaan sumber daya</li> </ul>
Ekonomi	<ul style="list-style-type: none"> <li>• Biaya aktual vs. anggaran</li> <li>• ROI dan TCO (Total Cost of Ownership)</li> </ul>
Pengguna	<ul style="list-style-type: none"> <li>• Kepuasan pengguna (survei NPS/CSAT)</li> <li>• Tingkat adopsi sistem</li> </ul>
Keamanan dan Kepatuhan	<ul style="list-style-type: none"> <li>• Tidak ada pelanggaran keamanan</li> <li>• Audit lulus dengan baik</li> </ul>

Tabel 9.3 Parameter Keberhasilan Proyek Cloud ini merangkum indikator yang digunakan untuk menilai efektivitas dan dampak dari implementasi proyek cloud, mencakup aspek teknis (seperti uptime dan performa sistem), operasional (ketepatan waktu dan efisiensi sumber daya), ekonomi (kesesuaian anggaran dan ROI), kepuasan pengguna (melalui CSAT atau NPS), serta keamanan dan kepatuhan terhadap regulasi. Dengan indikator ini, keberhasilan proyek dapat diukur secara objektif dan komprehensif.

## 9.6 Pengelolaan Risiko dalam Proyek Cloud

Pengelolaan risiko (risk management) merupakan aspek penting dalam manajemen proyek sistem informasi berbasis cloud karena lingkungan cloud bersifat dinamis, bergantung pada pihak ketiga, dan terhubung dengan berbagai sistem serta data sensitif (Kim, 2022). Risiko yang tidak ditangani dapat menyebabkan kerugian finansial, reputasi, bahkan pelanggaran hukum.

### 9.6.1 Risiko Umum dalam Proyek Cloud

1. Downtime dan Gangguan Layanan
  - a. Ketergantungan pada penyedia layanan cloud membuat organisasi rentan terhadap gangguan layanan atau kegagalan sistem di sisi penyedia.
  - b. Dampak: Menurunnya produktivitas, kehilangan data transaksi, gangguan operasional kritikal.
  - c. Contoh nyata: AWS outage pada 2021 yang berdampak global.
2. Vendor Lock-in
  - a. Ketika organisasi terlalu bergantung pada layanan, teknologi, atau arsitektur milik satu penyedia cloud, sehingga sulit melakukan migrasi ke penyedia lain.
  - b. Dampak: Ketergantungan tinggi, biaya migrasi mahal, sulit menegosiasikan SLA atau harga.
3. Isu Keamanan dan Privasi Data
  - a. Ancaman terhadap data melalui serangan eksternal, pelanggaran akses internal, atau kesalahan konfigurasi.
  - b. Dampak: Kebocoran data, sanksi hukum (misalnya melanggar GDPR, UU PDP), kerugian reputasi.
  - c. Jenis serangan umum: DDoS, man-in-the-middle, data breach, insecure API.
4. Kesalahan Konfigurasi dan Otomasi
  - a. Karena banyak proses cloud berjalan otomatis, kesalahan dalam scripting (infrastructure-as-code) dapat menyebabkan gangguan luas.
  - b. Dampak: Kehilangan data, akses tidak sah, gangguan operasional.

5. Kepatuhan terhadap Regulasi
  - a. Ketidakmampuan memenuhi persyaratan regulasi seperti ISO, SOC, HIPAA, GDPR, UU PDP, dll.
  - b. Dampak: Sanksi hukum, kerugian finansial, hilangnya kepercayaan publik.

### 9.6.2 Strategi Mitigasi Risiko

Pengelolaan risiko tidak hanya menanggapi kejadian, tetapi harus dimulai sejak tahap perencanaan dengan pendekatan proaktif (Lirko, 2024).

Strategi mitigasi meliputi:

1. Multi-Zone dan Multi-Region Deployment
  - a. Menyebarkan sistem ke beberapa wilayah dan zona ketersediaan cloud.
  - b. Mengurangi risiko downtime lokal.
2. Penerapan Arsitektur Cloud yang Portabel dan Terstandarisasi
  - a. Gunakan teknologi terbuka (open standards) dan arsitektur microservices.
  - b. Gunakan container (Docker) dan orchestrator (Kubernetes) untuk mempermudah migrasi antar cloud (mengurangi vendor lock-in).
3. Enkripsi Data dan Manajemen Akses Ketat
  - a. Terapkan enkripsi end-to-end (at rest & in transit).
  - b. Gunakan prinsip least privilege access, autentikasi multi-faktor (MFA), dan kontrol berbasis peran (RBAC).
4. Audit dan Monitoring Berkelanjutan
  - a. Gunakan tools seperti AWS CloudTrail, Azure Monitor, GCP Operations Suite.
  - b. Lakukan audit berkala dan simulasikan insiden keamanan (penetration testing).

5. SLA yang Kuat dan Evaluasi Vendor Berkala
  - a. Negosiasikan SLA yang mencakup ketersediaan layanan, waktu tanggap support, dan kompensasi bila terjadi pelanggaran.
  - b. Tinjau ulang performa dan kepatuhan vendor secara rutin.
6. Dokumentasi dan Uji Pemulihan Bencana (Disaster Recovery Testing)
  - a. Siapkan dokumen BCP (Business Continuity Plan) dan DRP (Disaster Recovery Plan).
  - b. Lakukan uji coba pemulihan secara berkala.
7. Pelatihan dan Kesadaran Tim

Tingkatkan kompetensi tim TI dan pengguna akhir melalui pelatihan keamanan cloud, pengelolaan akses, dan penggunaan layanan cloud secara aman.

## 9.7 Pemantauan dan Evaluasi Proyek Cloud

Tahap pemantauan dan evaluasi merupakan komponen penting dalam siklus hidup proyek cloud untuk memastikan bahwa proyek berjalan sesuai rencana, memenuhi standar kinerja, dan memberikan nilai yang diharapkan. Pada proyek berbasis cloud, evaluasi dilakukan tidak hanya terhadap deliverables proyek, tetapi juga terhadap layanan cloud yang digunakan (Correia and Martens, 2022).

### 9.7.1 Indikator Kinerja Utama (KPI) dan Service Level Agreement (SLA)

#### 1. Indikator Kinerja Utama (KPI – Key Performance Indicators)

KPI digunakan untuk mengukur keberhasilan proyek cloud dari berbagai aspek, baik teknis, operasional, maupun kepuasan pengguna (Bakhrom, 2024).

**Tabel 9.4:** Kategori KPI

Kategori KPI	Contoh KPI
Teknis	<ul style="list-style-type: none"> <li>• Response time aplikasi</li> <li>• Availability sistem (% uptime)</li> <li>• Latency dan throughput jaringan</li> </ul>
Proyek	<ul style="list-style-type: none"> <li>• Kesesuaian waktu pelaksanaan terhadap rencana (on-time delivery)</li> <li>• Kesesuaian anggaran dengan realisasi</li> <li>• Jumlah issue/bug yang ditemukan dan terselesaikan</li> </ul>
Kepuasan Pengguna	<ul style="list-style-type: none"> <li>• Skor CSAT (<i>Customer Satisfaction Score</i>)</li> <li>• Net Promoter Score (NPS)</li> </ul>
Keamanan & Kepatuhan	<ul style="list-style-type: none"> <li>• Jumlah insiden keamanan</li> <li>• Tingkat kepatuhan terhadap audit (ISO 27001, GDPR, dll)</li> </ul>

#### 2. Service Level Agreement (SLA)

SLA adalah kontrak antara organisasi dengan penyedia layanan cloud yang menjelaskan standar minimum layanan (Mo and Xing, 2022), termasuk: Availability/Uptime: Biasanya ditargetkan 99.9% hingga 99.999% (five nines).

- a. Response Time: Waktu maksimal untuk merespons dan menyelesaikan masalah.

- b. Support Time: Ketersediaan dukungan teknis (misal: 24/7, business hours).
- c. Data Durability: Misalnya, AWS S3 menjamin 99.999999999% durability.
- d. Penalty & Credit: Kompensasi bila SLA tidak terpenuhi.

SLA harus dikaji dan disesuaikan dengan kebutuhan bisnis agar tidak sekadar formalitas, tapi menjadi alat kontrol yang nyata.

## 9.7.2 Tools Monitoring dan Pengelolaan Proyek Berbasis Cloud

Monitoring dan pengelolaan proyek cloud memerlukan kombinasi antara alat manajemen proyek dan alat pemantauan infrastruktur atau aplikasi (Wang et al., 2024).

Berikut adalah kategorinya:

1. Tools Manajemen Proyek Cloud
  - a. Jira: Manajemen backlog, sprint, dan pelacakan isu.
  - b. Trello / Asana: Visualisasi tugas dengan metode Kanban.
  - c. Microsoft Project / ClickUp: Perencanaan proyek yang kompleks dan pelacakan kinerja.
  - d. Monday.com: Dasbor proyek kolaboratif dengan automasi dan integrasi cloud.
2. Tools Monitoring Infrastruktur dan Aplikasi
  - a. AWS CloudWatch: Memantau sumber daya AWS (EC2, Lambda, RDS) dan metrik custom.
  - b. Azure Monitor: Pemantauan layanan Azure dan integrasi dengan Log Analytics.
  - c. Google Cloud Operations (Stackdriver): Logging, monitoring, dan alerting di Google Cloud.

- d. Datadog: Observabilitas cloud dan aplikasi, termasuk tracing & dashboard.
  - e. Prometheus + Grafana: Monitoring berbasis open-source dengan visualisasi real-time.
  - f. New Relic / AppDynamics: Pemantauan performa aplikasi (APM), analisis bottleneck.
3. Tools Khusus Keamanan dan Audit
- a. AWS Config / Security Hub: Audit konfigurasi keamanan cloud.
  - b. Qualys / Nessus: Scanner kerentanan di lingkungan cloud.
  - c. Splunk: Analitik log dan peringatan dini atas anomali sistem.

# Bab 10

## Cloud Computing Dalam Pendidikan

### 9.1 Manfaat Cloud Computing dalam Dunia Pendidikan

Transformasi digital di sektor pendidikan merupakan bagian dari perkembangan teknologi yang semakin pesat di berbagai aspek kehidupan. Pendidikan sebagai fondasi utama pembangunan manusia tidak luput dari pengaruh teknologi informasi yang terus berkembang. Berbagai inovasi diterapkan untuk meningkatkan kualitas proses belajar-mengajar, baik dari sisi metode, media, maupun pengelolaan data pendidikan.

Salah satu teknologi yang kini menjadi kunci dalam mendukung transformasi digital tersebut adalah Cloud Computing. Teknologi ini telah membuka jalan bagi lembaga pendidikan untuk mengakses dan mengelola layanan teknologi informasi secara lebih mudah, fleksibel, dan efisien.

Tidak lagi diperlukan perangkat keras yang kompleks dan mahal untuk menjalankan sistem pendidikan berbasis digital.

Cloud computing memberikan kemudahan dalam penyimpanan, pemrosesan, dan distribusi data secara daring. Melalui koneksi internet, guru dan siswa dapat terhubung ke berbagai layanan pendidikan yang disediakan dalam bentuk platform, aplikasi, hingga sistem manajemen pembelajaran. Ini memungkinkan pelaksanaan pendidikan yang lebih terbuka dan tidak terbatas ruang dan waktu (Kurniawan et al., 2023).

Dengan model layanan yang dapat disesuaikan dengan kebutuhan (on-demand), cloud computing membantu lembaga pendidikan untuk mengatur sumber daya teknologi informasi sesuai kapasitas dan anggaran. Hal ini sangat penting, terutama bagi institusi pendidikan yang memiliki keterbatasan dana namun ingin tetap mengembangkan sistem digitalnya secara optimal.

Secara keseluruhan, kehadiran cloud computing dalam dunia pendidikan memberikan peluang besar untuk memperluas jangkauan pendidikan, meningkatkan efisiensi administrasi, serta memperkaya pengalaman belajar mengajar. Inilah alasan mengapa teknologi ini semakin menjadi bagian integral dalam pengembangan sistem pendidikan modern.

Cloud computing merupakan paradigma teknologi yang memungkinkan akses sumber daya komputasi secara fleksibel melalui jaringan internet. Dalam konteks pendidikan, cloud computing tidak hanya merevolusi cara penyampaian materi ajar, tetapi juga berperan strategis dalam manajemen pendidikan secara keseluruhan. Penerapan teknologi ini mendorong sistem pendidikan yang lebih terbuka, efisien, dan adaptif terhadap perkembangan zaman.

Secara teknis, cloud computing menawarkan model layanan seperti Infrastructure as a Service (IaaS), Platform as a Service (PaaS), dan Software as a Service (SaaS) yang dapat disesuaikan dengan kebutuhan lembaga pendidikan. Penggunaan layanan ini berkontribusi pada optimalisasi

infrastruktur teknologi informasi, peningkatan kapasitas manajerial, serta percepatan transformasi digital.

Manfaat Cloud Computing bagi Pendidikan (Abidah et al., 2020):

### 1. Menyelenggarakan Kelas Online

Cloud computing telah merevolusi cara dunia pendidikan menyelenggarakan kelas, terutama melalui platform berbasis cloud yang mendukung pembelajaran daring. Sebelum teknologi ini berkembang pesat, kegiatan belajar-mengajar secara daring menghadapi banyak hambatan, mulai dari keterbatasan infrastruktur hingga sulitnya menyampaikan materi secara interaktif. Namun, dengan hadirnya cloud computing, berbagai aplikasi dan layanan seperti Zoom, Google Classroom, Microsoft Teams, dan Moodle dapat digunakan secara luas untuk memfasilitasi interaksi antara guru dan siswa tanpa harus berada dalam satu ruang fisik.

Peran cloud computing menjadi sangat penting saat dunia dihadapkan pada pandemi COVID-19. Ketika pembelajaran tatap muka dihentikan untuk mencegah penyebaran virus, sekolah dan perguruan tinggi harus beradaptasi secara cepat. Dalam situasi ini, teknologi cloud terbukti menjadi solusi yang andal. Kelas-kelas yang sebelumnya hanya dapat berlangsung secara langsung kini dapat dialihkan ke format daring tanpa mengorbankan kontinuitas proses pembelajaran. Transisi ini tidak hanya bersifat sementara, tetapi juga menjadi titik balik dalam cara institusi pendidikan mendesain sistem pengajaran ke depan.

Platform Learning Management System (LMS) yang berbasis cloud seperti Google Classroom, Moodle, dan Canvas telah menjadi alat utama dalam pelaksanaan kelas online. Melalui LMS, guru dapat mengunggah materi ajar, memberikan tugas, mengatur jadwal ujian, hingga memantau perkembangan belajar siswa secara real-time. Semua aktivitas ini tersimpan secara otomatis di cloud, sehingga siswa dan guru dapat mengaksesnya kapan saja dan dari perangkat mana pun yang terhubung ke internet. Kemudahan ini secara signifikan meningkatkan fleksibilitas dan efektivitas pembelajaran.

Tak hanya memudahkan akses dan distribusi materi, cloud computing juga memungkinkan kolaborasi yang lebih dinamis dalam kelas online. Siswa dapat bekerja sama dalam proyek kelompok menggunakan dokumen bersama seperti Google Docs atau Microsoft 365 yang tersimpan di cloud. Mereka juga dapat berdiskusi melalui forum daring atau video call secara langsung. Semua interaksi ini memperkaya pengalaman belajar, serta membiasakan siswa dengan keterampilan kolaborasi digital yang semakin dibutuhkan di era kerja modern.

Seiring dengan meningkatnya adopsi teknologi ini, institusi pendidikan mulai menyadari pentingnya integrasi cloud computing dalam sistem mereka, tidak hanya sebagai alat darurat, tetapi sebagai bagian dari strategi jangka panjang. Dengan investasi yang tepat dan pelatihan yang memadai bagi tenaga pengajar, penyelenggaraan kelas online berbasis cloud dapat menjadi solusi berkelanjutan untuk menciptakan pendidikan yang inklusif, fleksibel, dan adaptif terhadap perubahan zaman.



**Gambar 10.1:** Kelas Online Berbasis Cloud Computing

Gambar di atas menekankan bagaimana cloud computing memungkinkan kegiatan belajar mengajar dilakukan secara daring. Melalui layanan cloud, pengajar dapat menyampaikan materi dari mana saja, dan siswa dapat

mengakses pembelajaran menggunakan berbagai perangkat, menunjukkan fleksibilitas dan inklusivitas yang ditawarkan oleh teknologi cloud dalam dunia pendidikan modern.

## 2. Mendukung Metode Belajar Modern

Cloud computing telah menjadi fondasi penting dalam penerapan metode pembelajaran modern seperti hybrid learning, blended learning, dan flipped classroom. Ketiga pendekatan ini menekankan fleksibilitas waktu dan tempat dalam belajar, serta pemanfaatan teknologi digital untuk mendukung proses pembelajaran yang lebih mandiri dan kolaboratif. Tanpa infrastruktur cloud yang andal, penerapan metode-metode ini akan sangat terbatas karena tergantung pada akses data dan koneksi real-time yang konsisten.

Dalam model blended learning, siswa menggabungkan pembelajaran tatap muka dengan materi yang dipelajari secara daring. Cloud computing memfasilitasi hal ini dengan menyediakan penyimpanan data yang besar untuk video, e-book, modul interaktif, serta kuis daring. Guru dapat mengunggah materi secara terstruktur ke platform Learning Management System (LMS), sementara siswa bisa mengaksesnya kapan saja sesuai kebutuhan mereka. Hal ini mendukung gaya belajar yang lebih personal, memungkinkan siswa untuk mengulang materi atau mempercepat proses belajar sesuai kecepatan masing-masing.

Sementara itu, dalam pendekatan flipped classroom, siswa mempelajari materi terlebih dahulu di rumah melalui sumber daya daring, lalu menggunakan waktu kelas untuk diskusi, analisis kasus, atau aktivitas kelompok. Cloud computing memungkinkan penyebaran konten digital seperti video penjelasan, simulasi interaktif, dan forum diskusi yang dapat diakses sebelum kegiatan tatap muka berlangsung. Model ini mendorong keterlibatan aktif siswa di kelas dan memberikan ruang lebih bagi guru untuk membimbing secara individual atau kelompok kecil.

Metode hybrid learning, yang menggabungkan pembelajaran daring dan luring secara bersamaan, juga sangat bergantung pada teknologi cloud.

Guru dapat mengajar secara langsung di kelas fisik sambil terhubung dengan siswa lain yang mengikuti dari rumah melalui platform video conference. Materi yang sama dapat diakses oleh semua siswa, baik yang hadir langsung maupun secara daring. Dengan cloud computing, integrasi data dari dua lingkungan belajar ini menjadi lebih mudah dan efisien, menciptakan pengalaman belajar yang setara dan berkualitas tinggi bagi seluruh peserta didik (Zhou et al., 2024)



**Gambar 10.2:** Metode Pembelajaran Modern

Gambar 10.2 memvisualisasikan bagaimana cloud computing menjadi penghubung utama dalam metode belajar modern. Guru dapat menyusun dan menyebarkan materi pelajaran secara daring melalui layanan cloud, memungkinkan siswa belajar sebelum kelas (flipped classroom), secara campuran daring dan luring (blended learning), atau hadir langsung dan virtual secara bersamaan (hybrid learning). Semua aktivitas ini terintegrasi dalam satu sistem berbasis cloud, menciptakan pengalaman belajar yang fleksibel, kolaboratif, dan terpersonalisasi (Suryawijaya & Praptodiyono, 2024)

### 3. Mengurangi Ketergantungan pada Perangkat Keras

Perkembangan teknologi cloud computing, ketergantungan pada perangkat keras fisik, seperti hard drive eksternal, semakin berkurang. Sebelumnya,

untuk menyimpan data pembelajaran, siswa dan pendidik harus menggunakan perangkat keras eksternal yang harus dipasang pada komputer atau perangkat lain. Namun, dengan adanya cloud computing, kebutuhan tersebut dapat diminimalisir karena data tidak lagi perlu disimpan secara fisik di perangkat keras lokal (Barus et al., 2024).

Cloud computing memungkinkan pengguna untuk menyimpan file secara online, yang dapat diakses kapan saja dan di mana saja selama terhubung dengan internet. Hal ini memberikan kemudahan bagi siswa dan pendidik untuk mengakses materi pembelajaran, tugas, atau sumber daya lainnya tanpa harus bergantung pada perangkat keras tertentu. Penyimpanan berbasis cloud menjadi solusi praktis yang memungkinkan aksesibilitas yang lebih tinggi.

Selain itu, penyimpanan cloud juga memungkinkan fleksibilitas dalam hal perangkat yang digunakan. Siswa dan pendidik tidak lagi terbatas pada satu perangkat, seperti komputer atau laptop tertentu, untuk mengakses file pembelajaran. Mereka dapat mengakses file melalui berbagai perangkat, termasuk ponsel pintar atau tablet, yang semakin mendukung mobilitas dan efisiensi dalam kegiatan belajar-mengajar.

Pengurangan ketergantungan pada perangkat keras ini juga membawa dampak positif dari segi penghematan biaya dan perawatan perangkat. Pengguna tidak perlu lagi membeli perangkat keras yang mahal atau khawatir dengan kerusakan perangkat penyimpanan eksternal. Semua data penting dapat disimpan dengan aman dan mudah diakses melalui penyedia layanan cloud, yang mengurangi kebutuhan akan perangkat keras tambahan.

## 9.2 Implementasi Cloud Computing dalam Pendidikan di Indonesia

Di Indonesia, implementasi cloud computing dalam sektor pendidikan telah memasuki tahap yang signifikan melalui kerja sama antara Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi dengan berbagai penyedia layanan cloud, termasuk Elitery. Kolaborasi ini bertujuan untuk memberikan akses yang lebih luas dan merata terhadap aplikasi pendidikan berbasis cloud yang dapat diakses oleh pelajar di seluruh Indonesia. Dengan pendekatan ini, pemerintah berharap dapat mengatasi kesenjangan pendidikan yang ada di berbagai daerah, terutama di daerah terpencil yang memiliki keterbatasan infrastruktur teknologi.

Program yang digagas oleh Kementerian Pendidikan ini melibatkan penyedia layanan cloud untuk memastikan penyediaan berbagai aplikasi pendidikan, mulai dari perangkat lunak pembelajaran hingga sistem manajemen pembelajaran online. Aplikasi-aplikasi tersebut memungkinkan siswa dan guru untuk terhubung dengan mudah, berbagi materi pelajaran, dan melakukan interaksi dalam lingkungan digital yang aman dan terstruktur. Dengan menggunakan cloud computing, seluruh data dan materi pembelajaran dapat disimpan dan diakses secara efisien tanpa harus bergantung pada perangkat keras lokal.

Salah satu manfaat utama dari implementasi cloud computing ini adalah peningkatan aksesibilitas pendidikan. Pelajar di daerah-daerah terpencil yang sebelumnya kesulitan dalam mengakses materi pembelajaran kini dapat mengunduh atau mengaksesnya langsung melalui cloud. Hal ini membantu mengurangi hambatan geografis dan ekonomi, yang sering kali menjadi tantangan dalam sistem pendidikan tradisional. Dengan adanya koneksi internet, mereka dapat belajar dari berbagai sumber tanpa terbatas oleh lokasi atau perangkat yang digunakan (Afzaal & Ul Haq, 2025).

Selain itu, cloud computing juga memudahkan kolaborasi antara siswa dan guru. Dengan sistem berbasis cloud, guru dapat memberikan tugas,

memberikan umpan balik secara langsung, serta memantau perkembangan belajar siswa dengan lebih efektif. Siswa juga dapat berdiskusi dan bekerja sama dalam grup virtual, yang mendukung pembelajaran kolaboratif. Hal ini menciptakan lingkungan yang lebih dinamis dan mendukung perkembangan keterampilan digital yang sangat dibutuhkan di era modern ini (Barus et al., 2024).



# Bab 11

## Tantangan dalam Penggunaan Cloud Computing

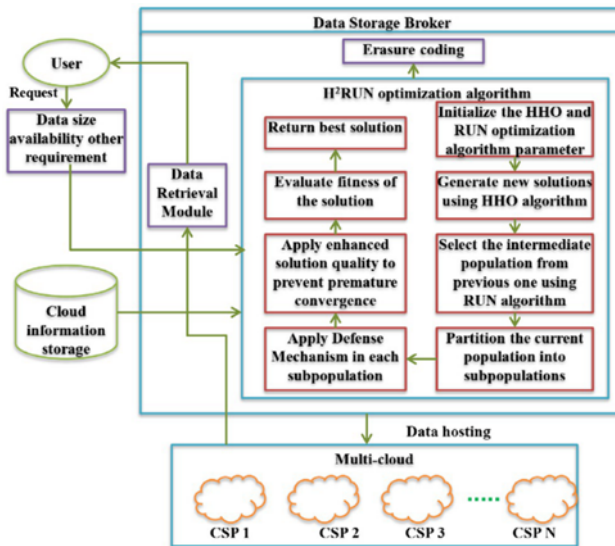
### 11.1 Ketergantungan pada Penyedia Layanan Cloud

Cloud software service adalah cara penyediaan fasilitas komputer dan penyebaran perangkat lunak melalui Internet dengan menggabungkan Cloud Computing dan Software-as-a-Service (SaaS) (Katzan, 2009). Cloud computing mengubah bagaimana cara komputer mengakses ataupun menyediakan data, sementara SaaS memungkinkan akses yang lebih merata terhadap perangkat lunak dan data melalui jaringan. Satu karakteristik cloud software service adalah transfer kontrol dari domain klien ke penyedia layanan, serta manfaat ekonomi yang dimiliki penyedia.

Tantangan utama dalam penggunaan layanan cloud adalah vendor lock-in, yaitu situasi di mana biaya untuk beralih ke penyedia lain sangat tinggi sehingga perusahaan cenderung terjebak dengan satu penyedia layanan

cloud. Dalam upaya mengurangi risiko ini, banyak perusahaan mengadopsi strategi multi-cloud, meskipun strategi tersebut memiliki kelemahan seperti biaya tinggi dan kompleksitas dalam pengelolaan. Kumar & Mala (2022) mengenalkan algoritma H2RUN (Horse Herd Runge Kutta) untuk mengoptimalkan keseimbangan antara biaya dan ketersediaan layanan cloud dengan teknik erasure coding.

Hal ini terbukti mampu mengurangi biaya hingga 48% dan meningkatkan ketersediaan hingga 58%. Tantangan berikutnya adalah downtime dan gangguan layanan. Bahkan downtime yang singkat dapat menyebabkan kerugian finansial signifikan dan gangguan operasional (Fahira dkk., 2024).



**Gambar 11.1:** Metode Horse Red Runge Kutta (Sumber: Kumar & Mala, 2022)

Sementara itu, Leesatapornwongsa & Gunawi (2014) mencatat bahwa 568 jam downtime di 13 layanan cloud sejak 2007 menyebabkan kerugian ekonomi lebih dari \$70 juta, dan setiap jam downtime dapat menyebabkan kerugian antara \$1 hingga \$5 juta. Untuk mengatasi risiko ini, strategi seperti optimisasi multi-server, deteksi dini risiko, dan manajemen sumber daya yang efisien perlu diterapkan.

Mekanisme seperti HMGOWM (Hybrid Migration Optimization with Monitoring) dapat mengotomatisasi migrasi virtual machine mengurangi dampak downtime dan meningkatkan pemulihan layanan secara signifikan (Cao dkk., 2021). Keamanan dan privasi data juga merupakan tantangan yang signifikan dalam layanan cloud. Menyimpan data di cloud berarti mempercayakan informasi sensitif kepada pihak ketiga, tentunya meningkatkan risiko kebocoran atau penyalahgunaan data. Zhang dkk. (2020) menggunakan teknik Ciphertext-Policy Attribute-Based Encryption (CP-ABE), yang memungkinkan perlindungan data dengan kebijakan akses tersembunyi untuk menjaga privasi pengguna. Namun, banyak skema CP-ABE yang ada masih menghadapi tantangan dalam hal efisiensi komunikasi dan biaya komputasi.

Oleh karena itu, pengembangan skema yang lebih efisien dalam verifikasi otoritas dapat membantu mengurangi risiko kebocoran privasi dan meningkatkan keamanan data. Dalam menghadapi berbagai tantangan tersebut, perusahaan perlu menerapkan pendekatan yang proaktif dan terukur dalam pengelolaan layanan cloud.

Mengadopsi strategi seperti multi-cloud, peningkatan keamanan data, serta mekanisme pemulihan downtime yang efektif dapat membantu perusahaan mengurangi risiko dan meningkatkan fleksibilitas operasional. Dengan demikian, perusahaan dapat memanfaatkan potensi penuh dari layanan cloud sambil tetap menjaga stabilitas, keamanan, dan efisiensi biaya.

## 11.2 Latensi Jaringan dan Keandalan

Latensi jaringan merupakan waktu yang diperlukan agar data berpindah dari satu titik ke titik lainnya dalam sebuah jaringan. Prasad dkk. (2014) mendefinisikan latensi sebagai durasi yang dibutuhkan untuk mengirimkan satu unit data dalam sistem. Jaringan dengan latensi rendah dirancang menggunakan arsitektur, perangkat keras, dan protokol yang bertujuan untuk meminimalkan latensi. Aplikasi interaktif seperti transmisi suara,

gaming, dan video sangat bergantung pada latensi jaringan. Oleh karena itu, pengelolaan latensi yang optimal serta peningkatan keandalan jaringan menjadi aspek krusial dalam layanan cloud.

Tantangan utama dalam mengelola latensi jaringan dan keandalan meliputi berbagai faktor teknis. Briscoe dkk. (2016) menyebutkan bahwa struktur jaringan yang kurang optimal, seperti penempatan server yang tidak efisien, dapat meningkatkan latensi secara signifikan. Setiap interaksi antara endpoint komunikasi menambah Round Trip Time (RTT) yang berpengaruh besar pada latensi, terutama dalam aliran data pendek. Selain itu, berbagai sumber penundaan lain seperti buffering sistem operasi, antrean dalam jaringan, serta keterbatasan perangkat keras dapat menyebabkan akumulasi latensi yang tinggi.

Latensi jaringan yang tinggi berdampak langsung pada keandalan layanan cloud. Edquist (2024) dalam penelitiannya menemukan korelasi negatif yang kuat antara pertumbuhan latensi dan produktivitas total faktor di negara-negara OECD. Penurunan 10% dalam pertumbuhan latensi pada periode sebelumnya dikaitkan dengan peningkatan 0,3% dalam pertumbuhan produktivitas total faktor. Bartlette (2006) juga menunjukkan bahwa latensi tinggi (lebih dari 100 ms) dapat mengganggu koordinasi, ritme, dan interaktivitas dalam aplikasi yang membutuhkan sinkronisasi real-time, seperti pertunjukan musik jarak jauh.

Dengan demikian, latensi jaringan yang tidak terkelola dengan baik dapat menurunkan performa bisnis serta menimbulkan kerugian finansial yang signifikan. Untuk mengatasi tantangan tersebut, berbagai solusi dapat diterapkan guna mengoptimalkan kinerja jaringan. Salah satu strategi yang efektif adalah pengaturan struktur jaringan yang lebih efisien, termasuk optimalisasi lokasi server (Briscoe dkk., 2016). Selain itu, pendekatan seperti edge computing memungkinkan pemrosesan data lebih dekat dengan pengguna, sehingga mengurangi latensi. Teknik lain, seperti penggunaan paket data pendek juga dapat meningkatkan efisiensi transmisi dan pemrosesan data secara simultan (Lai dkk., 2024).

Seiring berkembangnya teknologi, jaringan nirkabel generasi kelima (5G) semakin difokuskan pada pengurangan latensi dengan penerapan teknologi seperti Software Defined Network (SDN), Network Function Virtualization (NFV), caching, dan mobile edge computing (Parvez, 2017). Pada dasarnya, dengan mengelola latensi dan keandalan jaringan secara efektif, sesungguhnya perusahaan dapat meningkatkan performa layanan cloud, menjaga kepuasan pelanggan, serta memastikan stabilitas operasional dalam jangka panjang. Optimalisasi ini juga berkontribusi terhadap daya saing bisnis di era digital yang semakin menuntut konektivitas tinggi dan respons cepat.

## 11.3 Pengelolaan Identitas dan Akses

Dalam era digital yang semakin berkembang, pengelolaan Identity and Access Management (IAM) menjadi semakin krusial yang tidak hanya berfungsi sebagai sistem keamanan tetapi juga sebagai kerangka kerja yang mencakup aturan, prosedur, dan alat untuk mengelola serta mengontrol akses pengguna terhadap data sensitif dan identitas digital. Implementasi yang tepat memungkinkan peningkatan keamanan, pengalaman pengguna yang lebih baik, serta memastikan bahwa hanya individu yang memiliki hak akses yang dapat mengakses sumber daya penting dalam jaringan perusahaan.

Namun, Pratiksha dkk. (2018) menjelaskan bahwa penerapan IAM di berbagai aplikasi berbasis hak digital menghadapi tantangan yang kompleks. Solusi manajemen data perlu mengadopsi teknik kontrol akses yang efisien dan menyesuaikan pengaturan secara optimal di antara berbagai pendekatan untuk memastikan sistem yang aman dan terintegrasi. Sejumlah teknologi telah dikembangkan untuk mengatasi tantangan IAM, termasuk Web Single Sign-on (SSO), federated identity (identitas federasi), sinkronisasi kata sandi, dan granularitas layanan.

Identitas federasi memungkinkan pengguna menggunakan satu kredensial untuk mengakses berbagai layanan atau sistem tanpa harus masuk ulang, sehingga meningkatkan kenyamanan pengguna sekaligus mengurangi risiko penggunaan kata sandi yang lemah. Sementara itu, granularitas layanan mengacu pada kontrol akses yang lebih spesifik, di mana sistem dapat mengatur izin pengguna berdasarkan kebutuhan mereka, seperti membatasi akses hanya ke bagian tertentu dari suatu sistem untuk meningkatkan keamanan.

Namun, implementasi solusi ini dalam skala besar sering kali menghadapi berbagai kendala teknis dan operasional. Menurut Pratiksha dkk. (2018) salah satu pendekatan yang semakin populer adalah sistem berbasis kebijakan, yang memungkinkan integrasi identitas, autentikasi, peran pengguna, otorisasi akses, dan validasi aturan pada berbagai level. Dengan pendekatan ini, organisasi dapat mengotomatiskan kontrol akses secara lebih efisien, meningkatkan keamanan, serta menyederhanakan pengelolaan hak akses pengguna.

Di balik berbagai solusi yang tersedia, keamanan dalam IAM tetap menjadi tantangan utama. Laporan Verizon 'Data Breach Investigations Report' tahun 2017 dalam Furnell (2019) mengungkapkan bahwa 81% pelanggaran terkait peretasan memanfaatkan kata sandi yang dicuri atau tidak aman, dengan 62% dari total pelanggaran melibatkan metode peretasan. Selain itu, ancaman internal dari individu dengan hak akses luas juga berpotensi menjadi risiko keamanan yang signifikan, baik melalui kesalahan manusia maupun penyalahgunaan akses.

Dalam upaya meningkatkan keamanan, penggunaan Multi-Factor Authentication (MFA) telah terbukti menjadi metode perlindungan yang efektif terhadap akses tidak sah. Meyer (2023) menemukan bahwa lebih dari 99,99% akun yang menggunakan MFA tetap aman dalam periode investigasi, dengan pengurangan risiko kompromi sebesar 99,22% secara keseluruhan dan 98,56% dalam spesifik kasus kebocoran kredensial. Selain itu, aplikasi autentikasi khusus seperti Microsoft Authenticator lebih

unggul dibandingkan metode berbasis SMS dalam menjaga keamanan akun pengguna.

Selain teknologi autentikasi, kepatuhan terhadap regulasi juga menjadi faktor penting dalam pengelolaan IAM. Van Ooijen & Vrabec (2018) menyoroti bahwa GDPR (General Data Protection Regulation) memberikan perhatian besar terhadap kontrol individu atas data pribadi mereka dengan berbagai prinsip yang dirancang untuk meningkatkan perlindungan data. Namun, implementasi regulasi ini masih menghadapi tantangan, terutama karena asumsi yang digunakan dalam perumusan kebijakan sering kali tidak sejalan dengan cara individu mengambil keputusan terkait data pribadi mereka.

Sementara itu, di Amerika Serikat, Shah (2023) menjelaskan bahwa Health Insurance Portability and Accountability Act (HIPAA) berperan penting dalam menjaga keamanan informasi kesehatan elektronik dengan fokus utama pada kerahasiaan, integritas, dan ketersediaan data medis. Untuk mengatasi tantangan ini, pendekatan Attribute-Based Access Control (ABAC) mulai banyak diterapkan sebagai solusi yang lebih fleksibel dan otomatis. Kunz (2019) menjelaskan bahwa ABAC memungkinkan sistem untuk menentukan izin akses secara otomatis berdasarkan atribut pengguna yang telah ditetapkan.

Namun, keberhasilan metode ini sangat bergantung pada kualitas definisi dan nilai atribut yang digunakan. Oleh karena itu, sistem seperti TAQM (Tool-Assisted Quality Management) telah dikembangkan untuk meningkatkan kualitas data IAM dan memastikan pengelolaan akses yang lebih efisien.

Pendekatan Zero Trust Security Model juga semakin banyak diadopsi untuk meningkatkan keamanan dalam pengelolaan akses digital. Menurut Habash & Khalel (2023), Zero Trust mengikuti prinsip “never trust, always verify,” mengharuskan verifikasi ketat terhadap setiap perangkat dan pengguna sebelum diberikan akses ke sistem. Tidak seperti model keamanan tradisional yang menganggap entitas internal sebagai pihak yang dapat dipercaya, Zero Trust memastikan bahwa setiap akses diawasi secara

ketat. Model ini terbukti efektif dalam mencegah serangan dari dalam maupun luar jaringan perusahaan dengan menerapkan kebijakan akses yang lebih ketat dan kontrol terhadap manipulasi data.

Oleh karena itu, tantangan dalam pengelolaan identitas dan akses merupakan isu yang terus berkembang seiring dengan kemajuan teknologi dan peningkatan ancaman keamanan siber. Dengan menerapkan kombinasi teknologi terbaru, kepatuhan terhadap regulasi yang ketat, serta pendekatan keamanan yang adaptif, organisasi dapat membangun sistem IAM yang lebih tangguh dalam menghadapi berbagai tantangan di masa depan.

## 11.4 Migrasi Data

Dalam era digital yang terus berkembang, migrasi data menjadi tantangan utama bagi banyak organisasi yang ingin beralih ke sistem baru. Anderson dkk. (2010) menjelaskan bahwa masalah utama dalam migrasi data adalah menentukan rencana pemindahan objek data dalam jaringan dari satu konfigurasi ke konfigurasi lain. Proses ini sering kali diperlukan untuk menyeimbangkan beban atau menyesuaikan pola penggunaan data. Selain memindahkan informasi, migrasi data juga harus memastikan keakuratan, keamanan, dan kegunaannya di lingkungan baru. Salah satu tantangan terbesar adalah kompleksitas data.

Ramzan dkk. (2018) menyatakan bahwa basis data relasional memiliki keterbatasan dalam menangani data modern yang beragam dan heterogen. Organisasi yang masih menggunakan sistem lama berbasis relasional sering mengalami kesulitan dalam mengelola data semacam ini. Oleh karena itu, banyak yang beralih ke solusi big data yang lebih fleksibel dan mampu menangani data dalam berbagai bentuk, serta mendukung skala besar dan interaksi waktu nyata. Namun, migrasi ke sistem big data bukan tanpa hambatan. Proses transformasi data dari sistem lama ke sistem baru

membutuhkan strategi yang matang agar tidak terjadi inkonsistensi atau kehilangan data.

Migrasi data bukan hanya prosedur yang mahal, tetapi juga memiliki risiko keamanan yang signifikan. Beberapa perusahaan lebih menitikberatkan pada efisiensi biaya, terutama dalam pengujian aplikasi selama migrasi, sementara yang lain lebih fokus pada minimisasi risiko keamanan, terutama jika data yang dipindahkan bersifat sensitif. Salah satu pendekatan untuk mengurangi risiko ini adalah meminimalkan jumlah pergeseran data selama migrasi, karena semakin sedikit pergeseran yang terjadi, semakin kecil kemungkinan data terekspos.

Hasil dari Subramani dkk. (2019) menunjukkan bahwa pendekatan pengurangan pergeseran ini dapat mengoptimalkan keamanan migrasi dan menghasilkan solusi yang mendekati optimal dalam lebih dari 85% kasus. Oleh karena itu, strategi enkripsi dan kontrol akses yang ketat sangat diperlukan untuk menjaga keamanan data selama proses ini berlangsung. Sementara itu, Shi dkk. (2022) mengungkapkan bahwa downtime selama migrasi juga dapat berdampak besar pada bisnis. Teknik migrasi mesin virtual secara langsung memungkinkan pemindahan sistem operasi dan aplikasi yang sedang berjalan dari satu host fisik ke host lain tanpa mengganggu layanan.

Teknologi ini memberikan fleksibilitas dalam menyeimbangkan beban sistem, menghemat daya, serta meningkatkan toleransi kesalahan dalam pusat data. Namun, masih terdapat tantangan dalam migrasi lintas pusat data, terutama dalam hal latensi dan skalabilitas, yang dapat menyebabkan waktu henti yang lama serta degradasi kinerja. Solusi seperti Memory/Disk Operation Aware Lightweight VM Live Migration telah dikembangkan untuk mengurangi jumlah data yang harus dipindahkan selama proses migrasi, sehingga mampu mengurangi rata-rata 62,9% dari total waktu migrasi dan 36,0% downtime dibandingkan metode konvensional.

Kompatibilitas antara sistem lama dan baru sering kali menjadi tantangan dalam proses migrasi. Migrasi dari satu sistem perusahaan ke sistem lain memiliki tantangan tersendiri, terutama jika sistem lama telah digunakan

dalam jangka waktu yang lama dan menyimpan sejumlah besar data. Terkadang, format data antara kedua sistem tidak sepenuhnya kompatibel, yang dapat menyebabkan kesulitan dalam transfer data. Dalam kebanyakan kasus, migrasi tetap dapat dilakukan, tetapi tidak selalu memungkinkan untuk memindahkan data sepenuhnya ke sistem baru (Mikhail, 2010).

Dalam proses transisi, organisasi dapat memilih pendekatan seperti menjalankan kedua sistem secara paralel atau melakukan konversi data secara bertahap untuk memastikan semua data dapat disimpan dengan aman di sistem baru. Dengan strategi yang matang, seperti pembersihan dan pemetaan data serta pemanfaatan alat bantu migrasi, organisasi dapat mengatasi berbagai tantangan dalam proses ini. Secara keseluruhan, migrasi data bukan sekadar aspek teknis, tetapi juga bagian dari strategi transformasi bisnis yang lebih luas. Dengan perencanaan yang baik, metode yang tepat, dan pemanfaatan teknologi yang mendukung, organisasi dapat memastikan proses migrasi berjalan sukses tanpa mengganggu operasional bisnis secara signifikan.

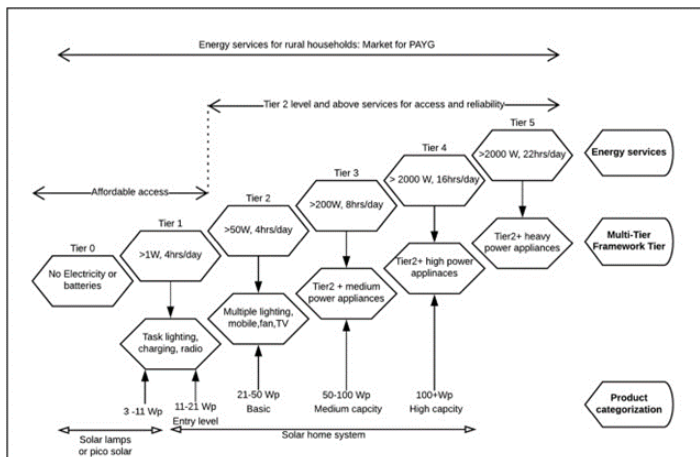
## 11.5 Skalabilitas dan Kapasitas

Salah satu keunggulan utama cloud computing adalah skalabilitas yang fleksibel. Perusahaan bisa menyesuaikan kapasitas komputasi sesuai kebutuhan, baik itu memperbesar (scaling up) saat ada lonjakan trafik maupun mengurangi (scaling down) saat beban menurun. Namun, fleksibilitas ini juga membawa tantangan tersendiri, terutama dalam hal biaya. Sistem pay-as-you-go yang memungkinkan pengguna membayar sesuai pemakaian, sering menjadi pilihan utama dalam model cloud publik.

Dalam skema ini, pemilik data hanya membayar layanan yang benar-benar dikonsumsi oleh pengguna. Namun, model ini juga menghadirkan tantangan signifikan, terutama dalam aspek keamanan dan efisiensi. Wang dkk. (2021) menyoroti bahwa dalam model pay-as-you-go, ada beberapa permasalahan serius seperti tingginya biaya dekripsi dalam attribute-based

encryption (ABE), potensi serangan DDoS terhadap ciphertext, serta kurangnya transparansi dalam audit konsumsi sumber daya. Untuk mengatasi hal ini, solusi seperti Fully Accountable ABE (FA-ABE) dikembangkan agar keamanan dan efisiensi dalam skema pay-as-you-go dapat ditingkatkan.

Selain biaya, latensi dan performa juga menjadi tantangan dalam skalabilitas cloud. Infrastruktur cloud berbasis pusat data memungkinkan perusahaan untuk menyewa sumber daya tanpa harus membangun sendiri. Namun, performa aplikasi di cloud sangat dipengaruhi oleh kondisi jaringan dan lokasi penyimpanan data. Popescu & Moore (2022) menjelaskan bahwa variasi latensi dalam pusat data dapat berdampak langsung pada performa aplikasi.



**Gambar 11.2:** Pay-As-You-Go Model (Sumber: Yadav dkk., 2019)

Mereka memperkenalkan NoMora, sebuah arsitektur yang mengoptimalkan penempatan aplikasi dalam pusat data untuk mengurangi dampak latensi. Eksperimen yang dilakukan menunjukkan bahwa pendekatan ini dapat meningkatkan performa aplikasi hingga 42% dalam simulasi dan 32,5% pada uji coba langsung. Dengan kata lain, perusahaan yang tidak mempertimbangkan latensi dalam penempatan data dan aplikasi di cloud dapat mengalami penurunan efisiensi operasional.

Di sisi biaya operasional, komputasi cloud memang menawarkan fleksibilitas, tetapi pengelolaannya menjadi tantangan tersendiri. Osypanka & Nawrocki (2023) menyoroti bahwa pengeluaran cloud kini menjadi salah satu komponen anggaran terbesar bagi perusahaan dari berbagai skala. Untuk mengoptimalkan biaya tanpa mengorbankan kualitas layanan, diperlukan pendekatan berbasis machine learning yang bisa memprediksi beban kerja dan merencanakan penggunaan sumber daya secara lebih efisien.

Hasil pengujian pada Microsoft Azure menunjukkan penghematan biaya operasional antara 31% hingga 89%, tergantung pada skenario yang digunakan. Ini membuktikan bahwa tanpa strategi yang jelas, perusahaan bisa dengan mudah mengalami pembengkakan biaya akibat penggunaan cloud yang tidak terkendali. Di sisi pengelolaan data, data sprawl menjadi tantangan besar yang sering kali luput dari perhatian. Michener (2015) menjelaskan bahwa semakin banyak organisasi yang dituntut untuk memiliki data management plan (DMP) sebagai bagian dari regulasi dan efisiensi dalam pengelolaan data.

DMP mencakup seluruh siklus hidup data, dari penemuan, pengumpulan, penyimpanan, hingga distribusi dan pengarsipan. Tanpa strategi yang jelas, data bisa tersebar tanpa kendali, menghambat efisiensi operasional dan meningkatkan risiko keamanan. Oleh karena itu, banyak organisasi kini mulai menerapkan sistem yang lebih ketat dalam dokumentasi dan pengelolaan metadata untuk mencegah data sprawl yang tidak terkendali.

Meskipun cloud dikenal dengan uptime yang tinggi, gangguan teknis tetap bisa terjadi dan berdampak besar bagi bisnis. Bieser & Menzel (2019) melaporkan bahwa rata-rata biaya downtime per menit untuk peralatan IT mencapai \$7.900, dengan durasi insiden rata-rata 86 menit, yang berarti satu kali gangguan bisa menyebabkan kerugian hingga \$690.200 per kejadian. Hal ini menegaskan bahwa meskipun penyedia cloud menjanjikan ketersediaan tinggi, kegagalan dalam operasional pusat data tetap menjadi ancaman yang signifikan.

Oleh karena itu, perusahaan perlu mengadopsi strategi redundansi dan pemantauan yang lebih ketat untuk mengurangi risiko downtime yang merugikan. Di luar tantangan teknis dan biaya, perusahaan juga menghadapi tantangan dalam fleksibilitas migrasi antar layanan cloud. Banyak organisasi yang awalnya memilih satu penyedia cloud karena kemudahan integrasi, tetapi seiring waktu, mereka menyadari bahwa ketergantungan pada satu vendor bisa membatasi inovasi dan efisiensi biaya. Oleh karena itu, semakin banyak perusahaan yang mulai menerapkan multi-cloud strategy, di mana mereka menggunakan layanan dari beberapa penyedia cloud untuk menghindari risiko keterikatan dengan satu vendor.

Salah satu pendekatan yang kini berkembang adalah serverless computing, yang menawarkan layanan cloud lebih terjangkau dan berbasis kebutuhan tanpa harus mengelola infrastruktur server secara langsung. Abed dkk. (2021) menjelaskan bahwa serverless computing mengalami adopsi yang pesat karena memungkinkan akses lebih fleksibel terhadap sumber daya cloud. Namun, teknologi ini juga menghadapi berbagai tantangan, seperti keberagaman teknologi tanpa pendekatan desain yang terpadu, kompleksitas dalam mengelola sumber daya dari pusat data hingga edge computing, serta kebutuhan kolaborasi lintas bidang untuk membangun fondasi yang lebih kuat.

Dalam beberapa tahun ke depan, kerja sama antara software engineering, sistem paralel dan terdistribusi, serta analisis performa dan modeling sistem akan menjadi faktor kunci dalam menjadikan serverless computing sebagai teknologi yang matang dan berkelanjutan. Cloud computing menawarkan skalabilitas tinggi yang memungkinkan perusahaan untuk menyesuaikan sumber daya sesuai kebutuhan.

Namun, tantangan seperti biaya yang sulit dikendalikan, latensi, pengelolaan data, risiko downtime, dan fleksibilitas migrasi layanan tetap harus diperhitungkan dalam strategi jangka panjang. Dengan penerapan strategi yang tepat, seperti optimasi berbasis machine learning, arsitektur penyimpanan yang lebih efisien, dan pendekatan multi-cloud, perusahaan

dapat memaksimalkan keuntungan dari cloud computing tanpa harus terjebak dalam masalah-masalah yang ada.

## 11.6 Manajemen Versi Layanan

Cloud computing telah menjadi bagian penting dalam operasional bisnis modern dengan menawarkan fleksibilitas, skalabilitas, dan efisiensi yang sulit dicapai dengan infrastruktur tradisional. Namun, seiring dengan meningkatnya adopsi teknologi ini, muncul berbagai tantangan yang harus dikelola dengan baik agar layanan cloud tetap optimal. Salah satu tantangan utama adalah keamanan dan privasi data, yang menjadi perhatian bagi banyak organisasi yang menyimpan informasi sensitif di lingkungan.

Ancaman siber seperti ransomware, phishing, dan insider threats terus berkembang seiring dengan meningkatnya ketergantungan perusahaan pada layanan cloud. Menurut Abdi dkk. (2024), regulasi seperti GDPR, HIPAA, dan ISO 27001 semakin menuntut perusahaan untuk menerapkan standar keamanan yang ketat dalam pengelolaan data mereka. Laporan IBM menunjukkan bahwa rata-rata biaya kebocoran data di seluruh dunia mencapai \$4,5 juta per insiden, angka yang menegaskan betapa seriusnya risiko yang dihadapi oleh organisasi yang tidak memiliki sistem keamanan yang kuat.

Salah satu faktor utama yang memperburuk situasi adalah kesalahan konfigurasi (misconfiguration) dalam sistem cloud. Bulut & Hwang (2021) mencatat bahwa lebih dari 144.000 celah keamanan telah terdaftar dalam National Vulnerability Database (NVD) pada akhir 2020 dengan banyak di antaranya berasal dari pengaturan akses yang salah, kurangnya enkripsi, atau kegagalan memperbarui sistem keamanan. Penggunaan perangkat lunak open-source juga berkontribusi terhadap tantangan ini karena banyak proyek open-source yang tidak selalu mengikuti standar keamanan global yang ketat.

Untuk mengatasi tantangan ini, penerapan Cloud Security Posture Management (CSPM) menjadi semakin penting dalam mendukung otomatisasi pemantauan keamanan cloud. Dengan adanya CSPM, organisasi dapat lebih mudah mendeteksi dan mengatasi celah keamanan sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab (Bulut & Hwang, 2021). Selain itu, pendekatan berbasis deep learning mulai diterapkan untuk mengidentifikasi dan memitigasi ancaman secara proaktif sehingga mempercepat respons terhadap risiko keamanan tanpa harus mengandalkan pemantauan manual yang rentan terhadap keterlambatan.

Di luar tantangan keamanan, biaya layanan cloud juga menjadi perhatian bagi banyak perusahaan. Wu dkk. (2021) menyatakan bahwa model pay-as-you-go memungkinkan organisasi membayar hanya berdasarkan penggunaan sumber daya cloud mereka. Namun, sistem ini memiliki tantangan tersendiri dalam hal transparansi biaya dan jaminan integritas data. Dalam beberapa kasus, perusahaan kesulitan memastikan bahwa data mereka benar-benar tersimpan dengan baik oleh penyedia layanan cloud.

Untuk mengatasi masalah ini, Wu dkk. (2021) menjelaskan bahwa mekanisme Proof of Storage (PoS) dikembangkan untuk memungkinkan penyedia layanan cloud membuktikan bahwa data pelanggan tetap utuh dan dapat diakses kapan saja. Dengan menggunakan protokol Proof of Retrievability (PoR), organisasi dapat mengaudit data mereka secara berkala untuk memastikan integritasnya.

Lebih lanjut, sistem auditing publik berbasis privacy-preserving PoS memungkinkan pihak ketiga melakukan verifikasi tanpa mengorbankan privasi pengguna atau mengungkap informasi sensitif terkait waktu penyimpanan. Selain keamanan dan biaya, kinerja dan ketersediaan layanan menjadi tantangan lain yang tidak kalah penting.

Mohan dkk. (2021) menyoroti bahwa gangguan layanan dapat berdampak besar bagi bisnis, terutama dalam industri yang sangat bergantung pada rantai pasokan yang presisi. Jika perusahaan dapat memprediksi potensi gangguan lebih awal, mereka dapat menghindari downtime yang merugikan dan menjaga keberlanjutan operasional mereka.

Salah satu pendekatan yang mulai diterapkan dalam mengelola kinerja cloud adalah model Adaptive ARIMA berbasis machine learning. Model ini memungkinkan sistem untuk menganalisis berbagai parameter operasional guna mengidentifikasi potensi gangguan sebelum terjadi (Mohan dkk., 2021). Dalam beberapa kasus, penerapan teknologi ini telah terbukti mampu meningkatkan Mean Time Between Failure (MTBF) secara signifikan, sehingga mengurangi frekuensi gangguan dan meningkatkan keandalan sistem cloud yang digunakan oleh perusahaan.

Dengan mempertimbangkan berbagai tantangan ini, organisasi perlu menerapkan strategi yang tepat untuk memastikan layanan cloud mereka tetap efisien dan aman. Mengadopsi pendekatan keamanan berbasis Zero Trust, mengoptimalkan sistem auditing PoS untuk meningkatkan transparansi model pay-as-you-go, serta menggunakan machine learning untuk memprediksi dan mencegah kegagalan layanan dapat membantu perusahaan dalam mengelola infrastruktur cloud mereka dengan lebih baik.

Kesuksesan manajemen versi layanan sangat bergantung pada kemampuan organisasi dalam memilih model layanan yang tepat, seperti Infrastructure as a Service (IaaS), Platform as a Service (PaaS), atau Software as a Service (SaaS), sesuai dengan kebutuhan bisnis dan teknisnya. Organisasi juga perlu memperhatikan aspek skalabilitas dan fleksibilitas layanan, sehingga mampu beradaptasi dengan perubahan kebutuhan bisnis secara cepat dan efisien.

Penggunaan Service Level Agreement (SLA) yang jelas dan terukur dapat membantu menjamin kualitas layanan yang diterima. Keamanan data dan kepatuhan terhadap regulasi juga merupakan aspek krusial, mengingat layanan cloud seringkali menyangkut data sensitif yang harus dilindungi. Terakhir, keberhasilan juga ditentukan oleh kesiapan sumber daya manusia dalam memahami dan mengelola layanan cloud secara efektif melalui pelatihan dan pengembangan kompetensi yang berkelanjutan.

# Bab 12

## Tren Masa Depan Cloud Computing

### 12.1 Edge Computing dan Cloud Hybrid

Cloud computing telah berkembang pesat dalam beberapa tahun terakhir, dan masa depannya tampak semakin cerah. Teknologi ini terus mengalami inovasi dan perubahan yang dapat meningkatkan efisiensi operasional, menurunkan biaya, serta memungkinkan perusahaan dan individu untuk memanfaatkan sumber daya komputasi yang lebih fleksibel dan skalabel.

Edge computing adalah model komputasi yang memindahkan pemrosesan data lebih dekat ke sumber data atau perangkat pengguna, seperti perangkat Internet of Things (IoT), daripada mengirimkan data ke pusat data cloud yang terpusat. Dengan pendekatan ini, data dapat diproses dan dianalisis di "edge" jaringan, yaitu di lokasi yang lebih dekat dengan perangkat yang

menghasilkan data, seperti pabrik, kendaraan otonom, atau perangkat medis.

Hal ini mengurangi latensi, menghemat bandwidth, serta meningkatkan efisiensi dan kecepatan respons. Edge computing sangat berguna untuk aplikasi yang memerlukan waktu respons rendah atau pengolahan data secara real-time, seperti dalam kasus kendaraan otonom yang membutuhkan pemrosesan cepat untuk menentukan tindakan berdasarkan informasi yang dikumpulkan secara langsung dari sensor-sensor mereka (Shi et al., 2016).

Cloud Hybrid, di sisi lain, adalah model infrastruktur yang menggabungkan penggunaan cloud publik dan cloud pribadi dalam satu sistem yang saling terintegrasi. Pendekatan ini memungkinkan organisasi untuk memanfaatkan fleksibilitas dan skalabilitas cloud publik untuk beban kerja yang lebih dinamis, sementara tetap menjaga kontrol dan keamanan data dengan menggunakan cloud pribadi untuk aplikasi atau data yang sensitif.

Cloud hybrid memungkinkan organisasi untuk mengoptimalkan penggunaan sumber daya mereka, mengurangi biaya operasional, serta tetap mematuhi regulasi dan kebijakan keamanan data yang ketat. Organisasi dapat memilih untuk menyimpan data atau aplikasi tertentu di cloud pribadi, sementara aplikasi lain yang tidak terlalu sensitif dapat dipindahkan ke cloud publik (Zhang et al., 2010).

Kedua teknologi ini, edge computing dan cloud hybrid, saling melengkapi dalam menghadapi tantangan modern seperti kebutuhan untuk mengelola data besar dengan efisien, menurunkan latensi, dan mempertahankan kontrol terhadap data sensitif. Dengan cloud hybrid, organisasi bisa mendapatkan manfaat dari skalabilitas cloud publik sambil tetap mempertahankan keamanan dan kontrol data melalui cloud pribadi.

Sementara itu, edge computing membantu mempercepat pengolahan data di lokasi yang lebih dekat dengan sumber data, yang sangat penting untuk aplikasi yang memerlukan analisis cepat dan real-time. Keduanya mewakili masa depan infrastruktur teknologi yang lebih terdistribusi dan fleksibel.

## 12.2 Kecerdasan Buatan (AI) dan Pembelajaran Mesin (Machine Learning) di Cloud

Kecerdasan Buatan (AI) dan Pembelajaran Mesin (Machine Learning) adalah dua bidang teknologi yang semakin berkembang dan menjadi semakin penting dalam dunia komputasi modern, khususnya dalam konteks cloud computing. AI merujuk pada simulasi kecerdasan manusia dalam mesin yang dapat menjalankan tugas-tugas yang biasanya memerlukan kecerdasan manusia, seperti pengambilan keputusan, pengenalan suara, dan analisis data kompleks. Sedangkan machine learning (ML) adalah cabang dari AI yang memungkinkan komputer untuk belajar dari data tanpa diprogram secara eksplisit.

Dalam konteks cloud, AI dan ML mengandalkan sumber daya komputasi besar yang disediakan oleh penyedia layanan cloud untuk menjalankan model-model algoritma yang memerlukan kapasitas pemrosesan tinggi dan penyimpanan data besar. Cloud menyediakan platform yang skalabel dan fleksibel untuk mengembangkan, melatih, dan menerapkan model AI dan ML dengan lebih efisien.

Misalnya, penyedia cloud seperti Amazon Web Services (AWS), Google Cloud, dan Microsoft Azure menawarkan layanan berbasis cloud untuk AI dan ML, yang memungkinkan pengembang dan perusahaan untuk mengakses infrastruktur yang diperlukan tanpa investasi besar dalam perangkat keras fisik (Chen et al., 2019).

Cloud computing juga memfasilitasi pemrosesan data besar (big data) yang penting dalam melatih model ML, karena akses yang mudah ke data dari berbagai sumber, serta kapasitas pemrosesan yang tinggi memungkinkan analisis yang lebih mendalam dan cepat. Dengan memanfaatkan cloud, perusahaan tidak hanya mengurangi biaya dan waktu yang diperlukan untuk pengolahan data besar, tetapi juga memperoleh keuntungan dari

kemudahan skalabilitas dan integrasi berbagai aplikasi dan layanan berbasis AI dan ML.

Seiring dengan perkembangan AI dan ML, integrasi dengan cloud akan semakin mempercepat adopsi teknologi ini di berbagai sektor industri, termasuk kesehatan, keuangan, dan e-commerce, dengan manfaat yang mencakup otomatisasi proses, prediksi yang lebih akurat, dan peningkatan pengambilan keputusan berbasis data (Zikopoulos et al., 2017). Oleh karena itu, peran cloud computing dalam mempercepat perkembangan AI dan ML sangat penting, menciptakan ekosistem teknologi yang lebih terhubung dan efisien.

## 12.3 Keamanan dan Privasi Data yang Lebih Baik

Keamanan dan privasi data menjadi perhatian utama dalam era digital, terutama dengan semakin meluasnya adopsi cloud computing oleh perusahaan dan individu. Cloud computing memungkinkan pengguna untuk menyimpan, mengelola, dan memproses data melalui internet, yang memberi banyak keuntungan seperti akses yang fleksibel, efisiensi biaya, dan skalabilitas. Namun, dengan manfaat ini, muncul pula tantangan besar terkait keamanan dan privasi data.

Keamanan data di cloud merujuk pada perlindungan data dari ancaman seperti pencurian, perusakan, atau akses tidak sah, sedangkan privasi data berkaitan dengan pengelolaan dan perlindungan informasi pribadi agar tidak disalahgunakan. Keamanan cloud mencakup beberapa aspek, seperti enkripsi data, kontrol akses, serta perlindungan terhadap serangan siber dan ancaman malware.

Penyedia layanan cloud terkemuka seperti Amazon Web Services (AWS), Google Cloud, dan Microsoft Azure menawarkan berbagai fitur keamanan untuk membantu melindungi data pelanggan, seperti enkripsi end-to-end,

yang memastikan bahwa data hanya dapat diakses oleh pihak yang berwenang (Zhou et al., 2020).

Privasi data di cloud juga menjadi perhatian utama, terutama dengan adanya regulasi global seperti General Data Protection Regulation (GDPR) di Uni Eropa, yang memberikan perlindungan hukum terhadap informasi pribadi. Pengguna dan organisasi yang mengadopsi cloud computing perlu memastikan bahwa data pribadi dikelola dengan hati-hati, dengan mematuhi kebijakan privasi yang ketat dan melibatkan audit keamanan yang terus-menerus.

Cloud computing menawarkan manfaat besar dalam hal keamanan data, tetapi juga memerlukan langkah-langkah yang lebih lanjut untuk mengurangi risiko terkait kebocoran data atau akses yang tidak sah. Penggunaan teknologi multi-factor authentication (MFA) dan identitas berbasis peran (role-based access control, RBAC) semakin penting dalam mengelola siapa yang dapat mengakses data di cloud dan bagaimana data tersebut dapat diproses atau dibagikan (Mell et al., 2011).

Untuk mengatasi masalah keamanan dan privasi, cloud computing juga memanfaatkan model keamanan berbasis kebijakan yang memungkinkan perusahaan untuk menetapkan dan mengontrol bagaimana data mereka disimpan, diproses, dan diakses oleh pihak ketiga. Misalnya, perusahaan dapat memilih untuk menggunakan cloud pribadi untuk data yang sangat sensitif, sementara cloud publik digunakan untuk data yang tidak terlalu penting.

Model hybrid cloud ini memungkinkan perusahaan untuk menyeimbangkan keuntungan skalabilitas dan fleksibilitas cloud publik dengan kontrol yang lebih ketat terhadap data sensitif menggunakan cloud pribadi. Seiring dengan terus berkembangnya ancaman terhadap data, penting bagi penyedia layanan cloud dan pengguna untuk terus berinovasi dan mengimplementasikan protokol keamanan terbaru untuk melindungi data dan menjaga privasi pengguna.

## 12.4 Cloud-Native dan Microservices

Cloud-native adalah pendekatan dalam pengembangan aplikasi yang dirancang untuk berjalan di lingkungan cloud secara optimal. Aplikasi yang dibangun dengan prinsip cloud-native memanfaatkan sepenuhnya karakteristik cloud seperti skalabilitas, elastisitas, dan ketahanan yang tinggi. Cloud-native tidak hanya mengacu pada penggunaan cloud untuk hosting, tetapi juga pada cara aplikasi dibangun, dikelola, dan dioperasikan di cloud.

Salah satu ciri utama dari aplikasi cloud-native adalah kemampuannya untuk menggunakan microservices. Aplikasi cloud-native dipecah menjadi layanan-layanan kecil yang disebut microservices, yang masing-masing dapat dikembangkan, diuji, dan diterapkan secara independen. Pendekatan ini memungkinkan pengembang untuk membangun dan merilis aplikasi dengan kecepatan yang lebih tinggi, serta memperbaiki dan memperbarui komponen aplikasi tanpa memengaruhi keseluruhan sistem (Fowler, 2012).

Microservices adalah pendekatan arsitektur perangkat lunak di mana aplikasi dibangun dari serangkaian layanan kecil yang dapat berdiri sendiri dan berfungsi secara independen. Setiap microservice biasanya menjalankan satu fungsi tertentu atau bagian dari aplikasi dan berkomunikasi dengan microservices lainnya melalui API atau protokol komunikasi yang standar. Keuntungan utama dari microservices adalah kebebasan dalam pengembangan dan penerapan. Setiap tim dapat bekerja pada bagian-bagian aplikasi yang berbeda, menggunakan bahasa pemrograman atau teknologi yang paling sesuai dengan kebutuhan mereka.

Selain itu, microservices memfasilitasi penerapan continuous integration/continuous deployment (CI/CD), yang memungkinkan pembaruan dan perbaikan dilakukan secara berkelanjutan tanpa mengganggu keseluruhan aplikasi. Dengan cara ini, microservices mendukung pengembangan aplikasi yang lebih cepat, lebih fleksibel, dan lebih mudah untuk diskalakan, karena layanan dapat diperbarui atau diganti tanpa memengaruhi sistem secara keseluruhan (Newman, 2015).

Cloud-native dan microservices bekerja sama untuk menciptakan aplikasi yang lebih efisien, mudah dipelihara, dan lebih cepat dalam merespons perubahan kebutuhan pasar. Dalam konteks cloud computing, aplikasi cloud-native yang berbasis microservices dapat dengan mudah disebar dan dipantau di berbagai lingkungan cloud, seperti public cloud, private cloud, atau hybrid cloud. Microservices yang berjalan dalam lingkungan cloud dapat memanfaatkan auto-scaling dan load balancing untuk memastikan aplikasi tetap tersedia dan responsif meskipun ada lonjakan permintaan.

Selain itu, cloud-native apps juga sering memanfaatkan containerization (misalnya, Docker) dan orchestration (misalnya, Kubernetes) untuk mengelola dan menyebarkan aplikasi secara lebih efisien. Containerization memungkinkan setiap microservice dijalankan dalam kontainer yang terisolasi, memudahkan pengembangan dan penerapan aplikasi secara konsisten di berbagai platform cloud (Turner et al., 2017).

Dengan semakin meningkatnya kebutuhan untuk aplikasi yang cepat, skalabel, dan dapat beradaptasi dengan perubahan teknologi dan pasar, cloud-native dan microservices menjadi pendekatan yang sangat relevan dalam pengembangan perangkat lunak modern. Penggunaan arsitektur ini membantu perusahaan untuk mencapai waktu pemasaran yang lebih cepat, fleksibilitas yang lebih besar dalam pengembangan dan pemeliharaan, serta kemampuan untuk memanfaatkan teknologi cloud secara maksimal.

## 12.5 5G dan Cloud

5G adalah generasi kelima dari teknologi jaringan seluler yang dirancang untuk menggantikan 4G (LTE) dan menawarkan kecepatan internet yang jauh lebih tinggi, latensi yang lebih rendah, serta kemampuan konektivitas yang lebih luas dan lebih stabil. Salah satu fitur utama dari 5G adalah kemampuannya untuk mendukung Internet of Things (IoT) dalam skala

yang jauh lebih besar, memungkinkan jutaan perangkat untuk terhubung secara simultan dengan kinerja yang tetap stabil.

Kecepatan unduh dan unggah 5G dapat mencapai lebih dari 10 gigabit per detik, jauh lebih cepat dibandingkan dengan 4G, yang memungkinkannya untuk mendukung aplikasi yang lebih kompleks dan membutuhkan bandwidth besar, seperti real-time video streaming dengan kualitas 4K/8K, augmented reality (AR), dan kendaraan otonom (Zhao et al., 2019).

Selain itu, 5G juga menjanjikan latensi yang lebih rendah, yang sangat penting untuk aplikasi real-time yang sensitif terhadap waktu, seperti telemedicine, kontrol industri otomatis, dan aplikasi kecerdasan buatan (AI) yang memerlukan respon cepat. Dengan kapasitas lebih besar dan kecepatan yang lebih cepat, 5G memungkinkan terciptanya ekosistem digital yang lebih terhubung dan responsif, yang dapat mengubah berbagai sektor industri, mulai dari kesehatan, manufaktur, transportasi, hingga hiburan.

Sementara itu, cloud computing adalah model layanan teknologi yang memungkinkan penyimpanan, pengolahan, dan akses data melalui internet, tanpa memerlukan infrastruktur perangkat keras lokal. Cloud computing menyediakan fleksibilitas dan skalabilitas untuk pengguna, memungkinkan mereka untuk menyewa sumber daya komputasi sesuai kebutuhan tanpa perlu mengelola infrastruktur fisik.

Cloud memungkinkan pengguna untuk menjalankan aplikasi dan mengakses data dari mana saja di dunia, selama terhubung dengan internet. Keunggulan utama dari cloud computing adalah kemampuannya untuk meningkatkan efisiensi dan menurunkan biaya operasional, memberikan organisasi dan individu akses ke kapasitas komputasi yang besar dan penyimpanan data tanpa harus berinvestasi besar dalam perangkat keras fisik (Armbrust et al., 2010).

Gabungan antara 5G dan cloud computing membuka potensi besar untuk inovasi digital di masa depan. Kecepatan tinggi dan latensi rendah yang ditawarkan oleh 5G akan memperkuat kinerja layanan cloud, dengan

memberikan konektivitas yang lebih cepat dan lebih andal antara perangkat pengguna dan server cloud. Hal ini sangat bermanfaat untuk aplikasi cloud yang memerlukan pemrosesan data secara real-time, seperti big data analytics, AI, dan machine learning.

Cloud computing akan mendukung penyimpanan dan pengolahan data dalam skala besar, sementara 5G akan memastikan bahwa data tersebut dapat dipindahkan dengan cepat dan tanpa hambatan, memberikan kinerja yang optimal untuk aplikasi berbasis cloud (Zhang et al., 2020). Misalnya, dalam konteks kendaraan otonom, data yang dikumpulkan oleh kendaraan akan diproses di cloud dengan cepat dan dikirimkan melalui jaringan 5G untuk memberikan perintah secara real-time, memungkinkan kendaraan tersebut untuk merespons secara otomatis terhadap situasi yang berkembang.

Selain itu, kombinasi antara 5G dan cloud computing juga mempercepat adopsi teknologi edge computing, yang menggabungkan pemrosesan data yang lebih dekat dengan sumber data untuk mengurangi latensi dan meningkatkan efisiensi, sambil memanfaatkan cloud untuk pengolahan data yang lebih berat dan komprehensif.

Dengan kata lain, 5G tidak hanya meningkatkan kinerja cloud computing, tetapi juga memperluas jangkauan dan fungsionalitasnya, membuka berbagai peluang baru untuk aplikasi digital yang lebih cepat, lebih aman, dan lebih responsif. Kolaborasi antara keduanya akan menjadi pendorong utama bagi transformasi digital di berbagai sektor, memacu perkembangan smart cities, industri 4.0, serta mempercepat adopsi teknologi canggih lainnya yang bergantung pada pemrosesan data besar dan konektivitas yang stabil.

## 12.6 Cloud untuk Industri Spesifik

Cloud untuk industri spesifik merujuk pada solusi cloud computing yang dirancang dan dioptimalkan untuk memenuhi kebutuhan unik dan tantangan yang dihadapi oleh sektor-sektor tertentu, seperti kesehatan, keuangan, manufaktur, pendidikan, dan lain-lain. Setiap industri memiliki persyaratan fungsional, regulasi, dan operasional yang berbeda, sehingga cloud untuk industri spesifik menyediakan platform, aplikasi, dan layanan yang disesuaikan untuk mendukung kebutuhan tersebut.

Layanan cloud ini menggabungkan fleksibilitas dan skalabilitas dari komputasi awan dengan alat dan fitur yang relevan untuk sektor tersebut, memungkinkan organisasi untuk memperoleh manfaat dari teknologi cloud tanpa mengorbankan kepatuhan terhadap regulasi industri atau kebutuhan teknis yang sangat spesifik (Bucchiarone et al., 2020).

Dalam sektor kesehatan, misalnya, cloud untuk industri ini menyediakan penyimpanan data yang aman dan skalabel untuk catatan medis elektronik (EMR), gambar medis (seperti radiologi), dan data pasien lainnya. Platform cloud khusus untuk kesehatan memastikan bahwa data pasien disimpan dengan aman dan mematuhi standar regulasi seperti Health Insurance Portability and Accountability Act (HIPAA) di AS atau General Data Protection Regulation (GDPR) di Eropa.

Penyedia cloud untuk industri kesehatan juga menyediakan aplikasi untuk telemedicine, manajemen rumah sakit, dan alat analitik kesehatan berbasis data besar yang dapat membantu dalam pengambilan keputusan medis (Hassani et al., 2021). Dengan menggunakan cloud computing, rumah sakit dan penyedia layanan kesehatan lainnya dapat mengakses data secara cepat dan aman dari berbagai lokasi, yang sangat penting dalam perawatan pasien dan manajemen fasilitas kesehatan.

Sektor keuangan juga banyak diuntungkan dengan adanya cloud untuk industri spesifik. Bank dan lembaga keuangan menggunakan platform cloud untuk mengelola data transaksi dalam skala besar, menjaga keamanan informasi pelanggan, serta mengembangkan aplikasi untuk analisis risiko,

fraud detection, dan manajemen portofolio. Cloud memungkinkan lembaga keuangan untuk meningkatkan efisiensi operasional, mengurangi biaya infrastruktur TI, dan mempercepat waktu pengembangan aplikasi yang dapat menyesuaikan diri dengan regulasi yang ketat, seperti yang diterapkan oleh Financial Conduct Authority (FCA) di Inggris atau Securities and Exchange Commission (SEC) di AS.

Dengan adanya cloud, lembaga keuangan juga dapat memanfaatkan kecerdasan buatan (AI) dan pembelajaran mesin (ML) untuk meningkatkan prediksi dan analisis pasar secara real-time, serta meningkatkan pengalaman pengguna dalam layanan perbankan digital (Gai et al., 2018).

Cloud untuk industri spesifik juga mencakup sektor manufaktur, di mana perusahaan dapat memanfaatkan cloud computing untuk Internet of Things (IoT) dan analitik data besar (big data). Dengan menghubungkan mesin dan perangkat di pabrik ke cloud, perusahaan manufaktur dapat memantau dan menganalisis kinerja mesin secara real-time, mendeteksi potensi kerusakan sebelum terjadi, serta meningkatkan efisiensi operasional. Platform cloud dalam industri ini mendukung integrasi dengan sistem Enterprise Resource

Planning (ERP) dan Supply Chain Management (SCM) untuk meningkatkan koordinasi antar bagian dan pengelolaan sumber daya yang lebih baik. Selain itu, cloud memberikan skalabilitas untuk mendukung berbagai inisiatif baru seperti produksi berbasis data, otomatisasi industri, dan smart factories (Mell & Grance, 2011).

## 12.7 Sustainability dan Green Cloud

Sustainability atau keberlanjutan, dalam konteks teknologi informasi dan komunikasi (TIK), mengacu pada kemampuan sistem untuk memenuhi kebutuhan saat ini tanpa mengorbankan kemampuan generasi mendatang untuk memenuhi kebutuhan mereka sendiri. Dalam dunia teknologi, keberlanjutan mengacu pada penggunaan sumber daya alam, energi, dan

bahan secara efisien, dengan mengurangi dampak negatif terhadap lingkungan. Salah satu cara untuk mencapai keberlanjutan adalah melalui adopsi teknologi yang ramah lingkungan, yang dapat mengurangi emisi karbon, penggunaan energi, dan limbah elektronik.

Dalam konteks cloud computing, keberlanjutan ini merujuk pada penerapan teknologi yang mengoptimalkan penggunaan energi dan meminimalkan jejak karbon pusat data serta memastikan bahwa teknologi tersebut dapat didaur ulang dan digunakan kembali (Koller et al., 2017). Selain itu, banyak penyedia layanan cloud kini berusaha untuk mencapai net-zero carbon emissions, yang berarti mereka mengimbangi emisi karbon yang mereka hasilkan dengan langkah-langkah untuk mengurangi atau mengimbangi dampak lingkungannya.

Green Cloud atau cloud ramah lingkungan adalah konsep yang berkaitan dengan penyediaan layanan cloud computing dengan cara yang meminimalkan dampak lingkungan. Penyedia layanan green cloud berfokus pada pengurangan konsumsi energi yang digunakan dalam operasional pusat data mereka, serta mengadopsi sumber energi terbarukan untuk mengurangi jejak karbon mereka. Konsep ini tidak hanya mencakup penggunaan teknologi yang lebih efisien dalam hal konsumsi energi, tetapi juga mencakup desain pusat data yang menggunakan peralatan dan infrastruktur yang lebih hemat energi dan lebih ramah lingkungan.

Penyedia cloud seperti Google, Amazon Web Services (AWS), dan Microsoft Azure telah mengimplementasikan kebijakan green data centers, yang menggunakan energi terbarukan, pendinginan efisien, dan desain bangunan yang mengurangi dampak lingkungan secara keseluruhan. Mereka juga mengoptimalkan penggunaan sumber daya melalui teknologi seperti virtualisasi dan komputasi berbasis container yang dapat mengurangi jumlah perangkat keras fisik yang diperlukan, serta mengurangi pemborosan energi (Sheldon & Tan, 2012).

Salah satu aspek penting dari green cloud adalah pengelolaan energi yang efisien. Cloud computing memungkinkan penggunaan sumber daya secara lebih efisien karena pengelolaan yang lebih baik terhadap kapasitas

komputasi dan penyimpanan melalui mekanisme on-demand scaling. Penyedia layanan cloud dapat memanfaatkan infrastruktur bersama, yang memungkinkan mereka untuk mengalokasikan sumber daya sesuai permintaan dan mengurangi pemborosan sumber daya yang biasa terjadi pada pusat data yang dikelola secara tradisional.

Dengan menggunakan pusat data berbasis cloud, perusahaan dapat mengurangi kebutuhan mereka untuk memiliki dan mengelola infrastruktur fisik yang besar, yang berpotensi mengurangi penggunaan energi dan emisi karbon. Selain itu, cloud computing memungkinkan pengelolaan sumber daya secara dinamis, yang berarti bahwa pusat data dapat menyesuaikan penggunaan energi mereka berdasarkan beban yang ada, meningkatkan efisiensi dan mengurangi konsumsi energi secara keseluruhan.

Dengan meningkatnya kesadaran akan perubahan iklim dan dampak lingkungan dari teknologi informasi, green cloud dan sustainability menjadi prioritas utama bagi penyedia layanan cloud dan organisasi yang bergantung pada cloud. Di masa depan, perusahaan diharapkan akan semakin berfokus pada praktik ramah lingkungan dalam operasional teknologi mereka, mulai dari penggunaan energi terbarukan untuk pusat data hingga pengurangan emisi dan daur ulang perangkat keras.

Keberlanjutan dalam cloud computing juga sejalan dengan tren global untuk mengurangi dampak lingkungan industri teknologi secara keseluruhan, dengan tujuan untuk menciptakan ekosistem digital yang lebih hijau dan lebih efisien (Hawkins et al., 2021).



# Daftar Pustaka

- Abdi, A., Bennouri, H., & Keane, A. (2024). Cyber Resilience, Risk Management, and Security Challenges in Enterprise-Scale Cloud Systems: Comprehensive Review. 2024 13th Mediterranean Conference on Embedded Computing (MECO), 1-8.
- Abidah, I. N., Hamdani, M. A., & Amrozi, Y. (2020). Implementasi Sistem Basis Data Cloud Computing pada Sektor Pendidikan. *KELUWIH: Jurnal Sains Dan Teknologi*, 1(2), 77–84. <https://doi.org/10.24123/saintek.v1i2.2868>
- ACHAR, S. (2020). Cloud and HPC headway for next-generation management of projects and technologies. *Asian Business Review*.
- Achar, S. (2021). AN OVERVIEW OF ENVIRONMENTAL SCALABILITY AND SECURITY IN HYBRID CLOUD INFRASTRUCTURE DESIGNS. *I-Proclaim*, 8(2), 2021.
- Afzaal, R. and Ul Haq, H.B. (2025) 'A Review and Comparative Study of Cloud Computing and the Internet of Things', *Spectrum of Engineering and Management Sciences*, 3(1), pp. 18–27. Available at: <https://doi.org/10.31181/sems31202534a>.
- ALABI, A. A., MUSTAPHA, S. D., & AKINADE, A. O. (2025). Leveraging advanced technologies for efficient project management in telecommunications. *International Journal of Multidisciplinary Research and Growth Evaluation*.

- Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*, 305, 357–383. <https://doi.org/10.1016/j.ins.2015.01.025>
- Almorsy, M., Grundy, J., & Müller, I. (2016). An Analysis of the Cloud Computing Security Problem (arXiv:1609.01107). arXiv. <https://doi.org/10.48550/arXiv.1609.01107>
- Alshazly, A. A., ElNainay, M. Y., El-Zoghabi, A. A., & Abougabal, M. S. (2021). A cloud software life cycle process (CSLCP) model. *Ain Shams Engineering Journal*, 12(2), 1809–1822. <https://doi.org/10.1016/j.asej.2020.11.004>
- Amazon Web Services. (2021). Overview of Amazon Web Services. AWS Whitepapers.
- Anderson, E., dkk. (2010). Algorithms for Data Migration. *Algorithmica*, 57, 349–380.
- Ang, P. L., Rana, M. E., & Hameed, V. A. (2023). Revolutionizing Finance: The Transformative Impact of Cloud Computing in Finance Shared Service Center (FSSC). 2023 IEEE 21st Student Conference on Research and Development (SCOREd), 482–488. <https://doi.org/10.1109/SCOREd60679.2023.10563756>
- Armbrust, M., et al. (2010). "A View of Cloud Computing." *Communications of the ACM*, 53(4), 50–58.
- Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50–58. <https://doi.org/10.1145/1721654.1721672>
- Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50–58.
- AYELE, Y. G. (2023). The significance of planning and scheduling on the success of projects. *Economics & Management Information*.

- BAKHROM, U. M. (2024). Key performance indicators in service organizations: Global practices in KPI application. *International Journal of Advance Scientific Research*.
- Bartlette, C., Headlam, D., Bocko, M., & Velikic, G. (2006). Effect of Network Latency on Interactive Musical Performance. *Music Perception*, 24, 49-62.
- Barus, E., Pardede, K. M., & Putri Br. Manjorang, J. A. (2024). Transformasi Digital: Teknologi Cloud Computing dalam Efisiensi Akuntansi. *Jurnal Sains Dan Teknologi*, 5(3), 904-911. <https://doi.org/10.55338/saintek.v5i3.2862>
- Barus, E., Pardede, K.M. and Putri Br. Manjorang, J.A. (2024) 'Transformasi Digital: Teknologi Cloud Computing dalam Efisiensi Akuntansi', *Jurnal Sains dan Teknologi*, 5(3), pp. 904-911. Available at: <https://doi.org/10.55338/saintek.v5i3.2862>.
- Bhowmik, Sandeep. (2017). "Cloud Computing". Cambridge University Press, India.
- BIBI, J., KAMATH, K. S., MADHESH, K., & VISHAL, S. (2024). Comprehensive study of cloud computing. *International Journal of Engineering and Computer Science*.
- Bieser, J., & Menzel, K. (2019). Assessing Facility Maintenance Models for Data Centres: Status and Deficits of Current Facility Management and Maintenance Concepts. *Applied Mechanics and Materials*, 887, 255 - 263.
- Briscoe, B., dkk. (2016). Reducing Internet Latency: A Survey of Techniques and Their Merits. *IEEE Communications Surveys & Tutorials*, 18, 2149-2196.
- Bucchiarone, A., Delling, D., & Küster, J. (2020). Cloud Computing for Industry 4.0: Applications, Opportunities, and Challenges. *Journal of Cloud Computing: Advances, Systems and Applications*, 9(1), 1-17.

- Bulut, M., & Hwang, J. (2021). NL2Vul: Natural Language to Standard Vulnerability Score for Cloud Security Posture Management. 2021 IEEE 14th International Conference on Cloud Computing (CLOUD), 566-571.
- Buyya, R., Broberg, J., & Goscinski, A. (2011). *Cloud Computing: Principles and Paradigms*. Wiley.
- Cantika Humendru, D. (2025). *Konsep Dasar Dan Perkembangan Terbaru Dalam Organisasi Dan Arsitektur Komputer*.
- Cao, R., Tang, Z., Li, K., & Li, K. (2021). HMGOWM: A Hybrid Decision Mechanism for Automating Migration of Virtual Machines. *IEEE Transactions on Services Computing*, 14, 1397-1410.
- Celesti, A., Tusa, F., Villari, M., & Puliafito, A. (2010). How to Enhance Cloud Architectures to Enable Cross-Federation. 3rd Int. Conf. on Cloud Computing.
- Chauhan, M., & Shiaeles, S. (2023). An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. In *Network* (Vol. 3, Issue 3, pp. 422–450). Multidisciplinary Digital Publishing Institute (MDPI). <https://doi.org/10.3390/network3030018>
- Chen, L., Xie, L., & Xie, L. (2019). Artificial intelligence and cloud computing: Applications, challenges, and future directions. *Journal of Cloud Computing: Advances, Systems and Applications*, 8(1), 1-16.
- Cisco Systems. (2020). *Networking Basics: What You Need To Know*. Cisco Networking Academy.
- Computing Infrastructure. (2023) Moratuwa Engineering Research Conference (MERCon), 473-478.
- CORREIA, S. R. V., & MARTENS, C. (2022). Cloud computing projects: Critical success factors. *RAUSP Management Journal*.
- Denny, M., Pujangga, C., Hidayat, N., & Bakhtiar, F. A. (2021). Implementasi Load Balancing pada Cloud Computing dengan Algoritme Improved Weighted Least Connection (Vol. 5, Issue 10). <http://j-ptiik.ub.ac.id>

- Edquist, H. (2024). How Important is Mobile Broadband Latency for Total Factor Productivity Growth? *Journal of Telecommunications and the Digital Economy* 12(1), 305-327.
- Erl, T., Puttini, R., & Mahmood, Z. (2013). *Cloud Computing: Concepts, Technology & Architecture*. Prentice Hall
- Fahira, S., Priambodo, A., Artikel, I., Syarifah, N., & Sulaiman, F. (2024). Downtime Data Center: Memahami Penyebab, Dampak, dan Solusi Efektif. *Sanskara Manajemen Dan Bisnis* 2(2), 67-78.
- Firdha Aisyah, N., Arif, M., & Ridha, F. (2022). High Availability Service dengan Multiple Master pada Kubernetes Cluster Menggunakan Virtualisasi Kernel Based Virtual Machine (KVM). 17–19.
- Forouzan, B. A. (2012). *Data Communications and Networking* (5th ed.). McGraw-Hill.
- Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008). Cloud computing and grid computing 360-degree compared. In *Proceedings of the Grid Computing Environments Workshop* (pp. 1-10). IEEE.
- Fowler, M. (2014). *Microservices: A definition of the architecture*. MartinFowler.com.
- Furnell, S. (2019). Password meters: inaccurate advice offered inconsistently? *Computer Fraud & Security* 11.
- Gai, K., Qiu, M., & Zhao, L. (2018). Cloud computing for financial services: Architectures, applications, and future directions. *Future Generation Computer Systems*, 86, 301-312.
- Gaianu, M. (2023). On Premise Data Center vs CLOUD. 2023 International Conference on Computational Science and Computational Intelligence (CSCI), 1068–1071. <https://doi.org/10.1109/CSCI62032.2023.00176>
- Gallico, D., Biancani, M., Blanchet, C., Bedri, M., Gibrat, J.-F., Baranda, J. I. A., Hacker, D., & Kourkouli, M. (2016). CYCLONE: A Multi-cloud

- Federation Platform for Complex Bioinformatics and Energy Applications. 5th IEEE International Conference on Cloud Networking (Cloudnet), 146–149.
- Garg, M. Y., Bhavana Gupta, M., & Tech Scholar, M. (2022). A COMPREHENSIVE SURVEY OF INFRASTRUCTURE AS A SERVICE BY TOP PUBLIC CLOUD VENDORS. [www.ijcrt.org](http://www.ijcrt.org)
- Gholami, A., & Laure, E. (2015). Security and Privacy of Sensitive Data in Cloud Computing: A Survey of Recent Developments. *Computer Science & Information Technology ( CS & IT )*, 131–150. <https://doi.org/10.5121/csit.2015.51611>
- Giap, Y. C. et al. (2020) *Cloud Computing: Teori dan Implementasi*. Yayasan Kita Menulis.
- Golightly, Lewis, Chang, Victor, Xu, Qianwen Ariel, Gao, Xianghua, & Liu, Ben S C. (2022). Adoption of cloud computing as innovation in the organization. *International Journal of Engineering Business Management*, 14, 18479790221093990. <https://doi.org/10.1177/18479790221093992>
- Habash, R., & Khalel, M. (2023). Zero trust security model for enterprise networks. *Iraqi Journal of Information and Communication Technology* 6(2).
- Hajare, R., Hodage, R., Wangwad, O., Mali, Y., & Bagwan, F. (2021). Data Security in Cloud. In *International Journal of Scientific Research in Computer Science, Engineering and Information Technology: Vol. ISSN (Issue 3)*. <http://ijsrcseit.com>
- Haryadi (2024) *Cloud Computing*. 1st edn, Pamulang: Penatamuda Media. [https://en.wikipedia.org/wiki/Cloud\\_computing#/media/File:Cloud\\_computing.svg%0Ahttps://www.it24hrs.com/2015/cloud-computing-and-cloud-definition/](https://en.wikipedia.org/wiki/Cloud_computing#/media/File:Cloud_computing.svg%0Ahttps://www.it24hrs.com/2015/cloud-computing-and-cloud-definition/).
- Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing.

- Hassani, H., Ghodsi, M., & Heidari, A. (2021). Cloud computing and healthcare: A comprehensive survey. *International Journal of Cloud Computing and Services Science*, 10(3), 145-159.
- Hawkins, D., M. Brown, & M. Wang. (2021). The Future of Green Cloud Computing: Sustainability and Energy Efficiency in the Digital Age. *Environmental Management and Sustainability*, 16(2), 125-139.
- Huawei Technologies Co., L. (2023) *Network Basics in Cloud Computing*. 1st edn, Cloud Computing Technology. 1st edn. Hangzhou, Zhejiang, China: Huawei Technologies Co., Ltd.
- Hurwitz, J., et al. (2012). *Cloud Computing For Dummies*. Wiley Publishing.
- Ilahi, E. N., Saripudin, M., Nugraha<sup>3</sup>, M. A., Dwight, G., Cardinsyah<sup>4</sup>, A., Hikmatulloh<sup>5</sup>, F., & Encep<sup>6</sup>, M. (2024). Mengungkap Potensi Luar Biasa dan Tantangan Menantang Cloud Computing di Era Digital (Vol. 3).
- J, Q. M., & M, H. I. (2024). An overview of cloud computing systems. *International Journal for Multidisciplinary Research*.
- Juliansyah, L., & Afrianto, I. (2023). *Tinjauan Literatur : Ancaman Keamanan pada Teknologi Cloud Computing dan Penanggulangannya*.
- Jumarlis, M. and Mirfan (2022) 'Detecting Diseases on Clove Leaves Using GLCM and Clustering K-Means', *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 6(4), pp. 624-631. Available at: <https://doi.org/10.29207/resti.v6i4.4033>.
- Junaedy, F. Z., Surapati, U., Studi, P., Informatika, T., Tinggi, S., Komputer, I., Karya Informatika, C., Kota, J., Timur, D., Khusus, I., & Jakarta, I. (2024). Optimisasi Web Service REST API Menggunakan Load Balancer dan Cache dengan Algoritma Round Robin (Studi Kasus: Madani Infosphere). In *Jurnal Indonesia : Manajemen Informatika dan Komunikasi (JIMIK)* (Vol. 5, Issue 3). <https://journal.stmiki.ac.id>
- kacha, L., & Zitouni, A. (2018). An Overview on Data Security in Cloud Computing. [https://doi.org/10.1007/978-3-319-67618-0\\_23](https://doi.org/10.1007/978-3-319-67618-0_23)

- Kahn, M. G., Mui, J. Y., Ames, M. J., Yamsani, A. K., Pozdeyev, N., Rafaels, N., & Brooks, I. M. (2022). Migrating a research data warehouse to a public cloud: Challenges and opportunities. *Journal of the American Medical Informatics Association*, 29(4), 592–600. <https://doi.org/10.1093/jamia/ocab278>
- Kaliappan, M., Augustine, S., & Paramasivan, B. (2016). Enhancing energy efficiency and load balancing in mobile ad hoc network using dynamic genetic algorithms. *Journal of Network and Computer Applications*, 73, 35–43. <https://doi.org/10.1016/j.jnca.2016.07.003>
- Katzan, J. (2009). Cloud Software Service: Concepts, Technology, Economics. *Service science* 1, 256-269.
- Khia, A., Tari, A., & Guérout, T. (2020). MFHS: A modular scheduling framework for heterogeneous system. *Software: Practice and Experience*, 50(8), 1463–1497. <https://doi.org/10.1002/spe.2827>
- Khoer, M. F., & Heryana, N. (2024). TINJAUAN SISTEMATIK LITERATUR TENTANG CLOUD COMPUTING DAN ANALISIS DATA: ARSITEKTUR DAN METODOLOGI. *Jurnal Informatika Dan Teknik Elektro Terapan*, 12(3). <https://doi.org/10.23960/jitet.v12i3.4989>
- KIM, H.-J. (2022). Three approaches to risk management in the cloud. *Information Resources Management Journal*, 35, 1-12.
- Koller, C., L. Diaz, & R. Cook. (2017). Sustainability and Green IT: A Global Perspective on Environmental Impact. *Journal of Cloud Computing: Advances, Systems and Applications*, 6(4), 85-98.
- Kumar, H., & Mala, G. (2022). H2RUN: An efficient vendor lock-in solution for multi-cloud environment using horse herd Runge Kutta based data placement optimization. *Transactions on Emerging Telecommunications Technologies*, 33.
- Kundu, A. (2024). AI/ML, Graphs and Access Control: Towards Holistic Identity and Access Management. *Proceedings of the 29th ACM Symposium on Access Control Models and Technologies*.

- Kunz, M., Puchta, A., Groll, S., Fuchs, L., & Pernul, G. (2019). Attribute quality management for dynamic identity and access management. *J. Inf. Secur. Appl.*, 44, 64-79.
- Kurniawan, S., Wiranata, W., Kusnan, K., Ma'muriyah, N., & Ting, V. V. (2023). Pemanfaatan Komputasi Awan (Cloud Computing) Pada Bidang Pendidikan. *Journal of Information System and Technology*, 4(2), 403-405. <https://doi.org/10.37253/joint.v4i2.6243>
- Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson.
- Kusuma, S.F., Pawening, R.E. and Dijaya, R. (2017) 'Otomatisasi klasifikasi kematangan buah mengkudu berdasarkan warna dan tekstur', *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, 3(1). Available at: <https://doi.org/10.26594/r.v3i1.576>.
- Lai, X., Jiang, H., Bhunia, S., & Tran, H. (2024). Reducing Latency in MEC Networks with Short-Packet Communications. *IEEE Transactions on Vehicular Technology*, 73, 3000-3004.
- Leesatapornwongsa, T., & Gunawi, H. (2014). The Case for Drill-Ready Cloud Computing. *Proceedings of the ACM Symposium on Cloud Computing*.
- LIRKO, T. (2024). Integration of risk-oriented project management into modern business models. *Business Inform.*
- Lubis, M., dkk. (2024). Analisis Risiko Keamanan Produk. Yayasan Kita Menulis. ISBN: 978-623-113-498-1.
- Lubis, M., dkk. (2024). Pengantar Sistem Informasi Organisasi. Yayasan Kita Menulis. ISBN: 978-623-113-431-8.
- Lubis, M., dkk. (2024). Pengantar Sistem Kesehatan Pintar. Yayasan Kita Menulis. ISBN: 978-623-113-465-3.
- Lubis, M., dkk. (2024). Pengelolaan Sistem Informasi Organisasi. Yayasan Kita Menulis. ISBN: 978-623-113-565-0.

- Lubis, M., dkk. (2025). Penerapan Sistem Informasi Organisasi. Yayasan Kita Menulis. ISBN: 978-623-113-765-4.
- Lubis, M., Fauzi, R., & Zamzami, I.F. (2018). The Development of Radical Innovation with the Digital Gift. IEEE ICOSNIKOM 2018.
- Lubis, M., Fauzi, R., Sutoyo, E., & Abdulmana, S. (2019). Responsive innovation through perceived shared values and preferences of customers. *J. of Physics: Con. S.* 1361(1) 012075. IOP Publishing.
- Lubis, M., Lubis, A.R., & Ernovianti, E. (2018). Disruptive innovation service oriented framework: a case study of transportation in Indonesia. *Proc. of 7th ICMR*.
- Lubis, M., Lubis, A.R., Lubis, B., & Lubis, A. (2018). Incremental innovation towards business performance: data management challenges in healthcare industry in Indonesia. *MATEC web of conferences* 218, 04015. EDP Sciences.
- Lubis, M., Lumingkewas, L.W., & Lubis, A.R. (2022). Business Process Re-Engineering: Strategies for Health Management Services in Puskesmas. *Lecture Notes in Networks and Systems* 217, 175-184.
- Mai, V., & Khalil, I. (2017). Design and implementation of a secure cloud-based billing model for smart meters as an Internet of things using homomorphic cryptography. *Future Generation Computer Systems*, 72, 327–338. <https://doi.org/10.1016/j.future.2016.06.003>
- Marinescu, D. C. (2013). *Cloud Computing: Theory and Practice*. Morgan Kaufmann.
- MARNEWICK, C., ERASMUS, W., & NAZEER, J. (2018). The symbiosis between information system project complexity and information system project success.
- Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing (Special Publication 800-145)*. National Institute of Standards and Technology.

- Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*. National Institute of Standards and Technology.
- Mell, P., & Grance, T. (n.d.). *The NIST Definition of Cloud Computing*.
- Mell, P., Grance, T., & Marshall, W. (2011). *The NIST Definition of Cloud Computing*. National Institute of Standards and Technology.
- Meyer, L., Romero, S., Bertoli, G., Burt, T., Weinert, A., & Ferres, J. (2023). How effective is multifactor authentication at deterring cyberattacks? *ArXiv*, abs/2305.00945.
- Michener, W. (2015). Ten Simple Rules for Creating a Good Data Management Plan. *PLoS Computational Biology*, 11.
- Mikhail, B. (2010). Optimizing the process of implementing a new corporate system to the end user. 6th Central and Eastern European Software Engineering Con. (CEE-SECR), 170-174.
- MO, Y.-C., & XING, L. (2022). Efficient analysis of resource availability for cloud computing systems to reduce SLA violations. *IEEE Transactions on Dependable and Secure Computing*, 19, 3699-3710. <https://doi.org/10.1109/TDSC.2021.3070957>
- Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in Cloud. *Journal of Network and Computer Applications*, 36(1), 42-57. <https://doi.org/10.1016/j.jnca.2012.05.003>
- Mohan, T., Roselyn, J., Uthra, R., Devaraj, D., & Umachandran, K. (2021). Intelligent machine learning based total productive maintenance approach for achieving zero downtime in industrial machinery. *Comput. Ind. Eng.*, 157, 107267.
- Muttaqin, M. et al. (2023) *Cloud Computing: Konsep dan Implementasi*. Yayasan Kita Menulis.
- Muttaqin, M. et al. (2024) *Data Cloud: Masa Depan Teknologi Penyimpanan dan Pengelolaan Data*. Yayasan Kita Menulis.

- N'Goran, K. R., Tetchueng, J.-L., Kermarrec, Y., Brou, A. P. B., & Asseu, O. (2023). Blockchain-based Identity and Access Management in a Community Cloud. 2023 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 1–6. <https://doi.org/10.23919/SoftCOM58365.2023.10271602>
- Namruddin, R., Sam, R. M. I. S., Syamsuddin, R. W., A, A., & Kunaefi, A. (2025). Performance Analysis of API in Google Cloud Storage Service Integration. *Journal of System and Computer Engineering (JSCE)*, 6(1), 161–169. <https://doi.org/10.61628/jsce.v6i1.1637>
- Newman, S. (2015). *Building Microservices: Designing Fine-Grained Systems*. O'Reilly Media.
- Osypanka, P., & Nbiawrocki, P. (2023). QoS-Aware Cloud Resource Prediction for Computing Services. *IEEE Transactions on Services Computing*, 16, 1346–1357.
- PANCHAL, F., & KHOKRALE, S. (2024). Effective project management with SAP project system (PS): Balancing scope, time and budget constraints.
- Parvez, I., Rahmati, A., Guvenc, I., Sarwat, A., & Dai, H. (2017). A Survey on Low Latency Towards 5G: RAN, Core Network and Caching Solutions. *IEEE Comm. Surveys & Tutorials*, 20, 3098–3130.
- Popescu, D., & Moore, A. (2022). Network Latency and Application Performance Aware Cluster Scheduling in Data Centers. *IEEE Network* 36, 58–65.
- Prasad, C., G.S, V., Agrawal, C., & Srivastava, R. (2014). Achieving low latency networks through high performance computing. *Int. Journal of Advanced Research in Computer and Communication Engineering*, 8753–8756.
- Pratiksha, N., Prasad, S., & Mungara, J. (2018). Identity and Access Management. *CompTIA® Security+® Practice Tests*.

- PROJECT MANAGEMENT INSTITUTE, P. (2021). A guide to the project management body of knowledge (PMBOK® Guide)—Seventh edition and the standard for project management. Project Management Institute.
- Raj, P., & Raman, A. C. (2017). *Big Data Analytics and Cloud Computing: Theory, Algorithms and Applications*. Springer
- Ramsari, N., & Ginanjar, A. (2022). Implementasi Infrastruktur Server Berbasis Cloud Computing Untuk Web Service Berbasis Teknologi Google Cloud Platform. SENATIK. <https://doi.org/10.28989/senatik.v7i1.472>
- Ramzan, S., Bajwa, I., & Kazmi, R. (2018). An Intelligent Approach for Handling Complexity by Migrating from Conventional Databases to Big Data. *Symmetry*, 10, 698.
- Rezki, M. (2014) 'Cloud Computing', in *Cloud Computing*, pp. 1–36.
- Rizal, M., Kusnanto, E., & Kasih Bangsa, S. (2022). Peran Regulasi dalam Mendorong Adopsi Cloud Computing UMKM DKI Jakarta. 3(1). <https://journal.univetbantara.ac.id/index.php/jbfe>
- Safitra, M.F., dkk. (2018). Cyber Resilience: Research Opportunities. *Proc. of ICECCE* 99-104.
- Safitra, M.F., dkk. (2023). Green Networking: Challenges, Opportunities, and Future Trends for Sustainable Development. *Proc. of 11th ACM ICCCM*.
- Safitra, M.F., dkk. (2023). Intelligent Computing in Communication Networks: Challenges, Solutions, and Research Prospects. *Proc. of IEEE ICOCO* 306-310.
- Safitra, M.F., dkk. (2023). Leveraging Digital Intelligence for Network Economy and Knowledge Management in Technology-Focused Firms. *Proc. of ACM ICIBE*.

- Safitra, M.F., dkk. (2023). Metaverse Trend: Definition, Application, Opportunities, Law, and Ethics. *Proc. of IEEE ICOCO*, 160-165.
- Safitra, M.F., dkk. (2024). The State of Cyber Resilience: Advancements and Future Directions. *Intelligent Sustainable Systems: Selected Papers of WorldS4 2*(817).
- Safitra, M.F., Lubis, M., Kurniawan, M.T., Saedudin, R.R., & Alhari, M.I. (2023). Beyond Efficiency: Advancing Sustainability in Data Centers through TIA-942 Guidelines and Case Studies. *Proc. ACM ICCCM*.
- Safitra, M.F., Lubis, M., Kusumasari, T.F., & Putri, D.P. (2024). Advancements in Artificial Intelligence and Data Science: Models, Applications, and Challenges. *Procedia Computer Science* 234, 381-388.
- Safitra, M.F., Lubis, M., Lubis, A.R., & Alhari, M.I. (2023). The Need for Energy-Efficient Networks: A Review of Green Communication Systems and Network Architectures. *Proc of Int. Con. on WorldS4* 127-136.
- Salem, H. S., Hodhod, R., El-Tawel, G. S., & Elyamany, H. F. (2020). Service-based Architecture for SLA Management in Cloud Computing. In *International Journal of Computer Applications* (Vol. 175, Issue 26).
- Santoso, J.T. (2023) *Komputasi awan*. 1st edn, Computing. 1st edn. Semarang: YPAT.
- SCHWALBE, K. (2021). *An introduction to project management (7th ed.): Predictive, agile, and hybrid approaches*.
- Setiawan, W., Fajriyah, N. , & Duha, T. (2022). *Analisa Layanan Cloud Computing Di Era Digital*.
- Shah, W. (2023). Preserving Privacy and Security: A Comparative Study of Health Data Regulations - GDPR vs. HIPAA. *International Journal for Research in Applied Science and Engineering Technology* 11.

- Sheldon, F., & Tan, S. (2014). The Role of Cloud Computing in Sustainability: A Green Approach. *Journal of Computing and Sustainable Development*, 21(3), 99-112.
- Shi, B., Shen, H., Dong, B., & Zheng, Q. (2022). Memory/Disk Operation Aware Lightweight VM Live Migration. *IEEE/ACM Transactions on Networking*, 30, 1895-1910.
- Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, 3(5), 637-646.
- SILVA, C., PEREIRA, C., & MAGANO, J. (2021). The value of project management to competitiveness: Key factors from a holistic and practical perspective. *International Journal of Managing Projects in Business*.
- Singh, A., Kuzminykh, I., & Ghita, B. (2024). Industry Perception of Security Challenges with Identity Access Management Solutions. 2024 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), 312-315.
- Singh, S., Jeong, Y.-S., & Park, J. H. (2016). A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications*, 75, 200-222. <https://doi.org/10.1016/j.jnca.2016.09.002>
- Smith, J. (2020, August 10). What is cloud computing and how does it work? TechRadar. <https://www.techradar.com/news/what-is-cloudcomputing>.
- Sofana, I. (2012). *Cloud Computing: Teori dan Praktik* (OpenNebula, VMware, dan Amazon AWS). Informatika.
- Soundararajan Guru, S. (2024). Cost-Effective Payment Processing Solutions in The Public Cloud: Strategies for Optimizing Infrastructure and Maximizing Efficiency. In *Journal of Advanced Research Engineering and Technology (JARET)* (Vol. 3, Issue 1).

<https://iaeme.com/Home/journal/JARET45editor@iaeme.comhttps://iaeme.com/Home/issue/JARET?Volume=3&Issue=1>

- Soundararajan Guru, S. (2024). Cost-Effective Payment Processing Solutions in The Public Cloud: Strategies for Optimizing Infrastructure and Maximizing Efficiency. In *Journal of Advanced Research Engineering and Technology (JARET)* (Vol. 3, Issue 1). <https://iaeme.com/Home/journal/JARET45editor@iaeme.comhttps://iaeme.com/Home/issue/JARET?Volume=3&Issue=1>
- Soveizi, N., Turkmen, F., & Karastoyanova, D. (2022). Security and Privacy Concerns in Cloud-based Scientific and Business Workflows: A Systematic Review (arXiv:2210.02161). arXiv. <https://doi.org/10.48550/arXiv.2210.02161>
- Stallings, W. (2016). *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud*. Pearson Education.
- Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), 1–11. <https://doi.org/10.1016/j.jnca.2010.07.006>
- Subramani, K., Çaskurlu, B., & Acikalın, U. (2019). Security-Aware Database Migration Planning. *Algorithm Aspects of Cloud* 103-121.
- Sunyaev, A. (2020). *Cloud Computing*. Springer International Publishing.
- Suryawijaya, M. R., & Praptodiyono, S. (2024). Pemanfaatan Komputasi Awan untuk Pengarsipan Digital di Indonesia. *Jurnal Ilmu Komputer Dan Teknologi*, 5(3), 1–7. <https://doi.org/10.35960/ikomti.v5i3.1479>
- Suryawijaya, M.R. and Praptodiyono, S. (2024) 'Pemanfaatan Komputasi Awan untuk Pengarsipan Digital di Indonesia', *Jurnal Ilmu Komputer dan Teknologi*, 5(3), pp. 1–7. Available at: <https://doi.org/10.35960/ikomti.v5i3.1479>.
- Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks* (5th ed.). Prentice Hall.

- Teo, M., Mahdin, H., Hwee, L. J., Dicken, H. A., Hui, T. X., Ling, T. M., & Azmi, M. S. (2018). A Review on Cloud Computing Security. *JOIV : International Journal on Informatics Visualization*, 2(4-2), 293-298. <https://doi.org/10.30630/joiv.2.4-2.171>
- Turner, M., Budgen, D., & Brereton, P. (2017). Microservices: A systematic review. *Software: Practice and Experience*, 47(12), 1611-1634.
- Umar, R. (2013) 'Review Tentang Virtualisasi', *Jurnal Informatika*, 7(2), pp. 775-794.
- Van Ooijen, I., & Vrabec, H. (2018). Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioral Perspective. *Journal of Consumer Policy*, 42, 91-107.
- Velte, A. T., Velte, T. J., & Elsenpeter, R. (2010). *Cloud Computing: A Practical Approach*. McGraw-Hill.
- WANG, F., WANG, J., CAI, H., & YANG, G. (2024). Research on the design and application of integrated monitoring and visualization systems in intelligent project management. In *2024 IEEE 16th International Conference on Computational Intelligence and Communication Networks (CICN)* (pp. 1141-1145). IEEE. <https://doi.org/10.1109/CICN52025.2024.10123924>
- Wang, T., H., Zhou, Y., Zhang, R., & Song, Z. (2021). Fully Accountable Data Sharing for Pay-as-You-Go Cloud Scenes. *IEEE Transactions on Dependable and Secure Computing*, 18, 2005-2016.
- Wu, T., Yang, G., Mu, Y., Guo, F., & Deng, R. (2021). Privacy-Preserving Proof of Storage for the Pay-As-You-Go Business Model. *IEEE Transactions on Dependable and Secure Computing*, 18, 563-575.
- Xu, X., Zang, S., Bilal, M., Xu, X., & Dou, W. (2024). Intelligent architecture and platforms for private edge cloud systems: A review. *Future Generation Computer Systems*, 160, 457-471. <https://doi.org/10.1016/j.future.2024.06.024>

- Yadav, P., Heynen, A. P., & Palit, D. (2019). Pay-As-You-Go financing: A model for viable and widespread deployment of solar home systems in rural India. *Energy for Sustainable Development*, 48, 139–153.
- Yunie Cancer, Z.A. (2016) 'Platform as a service (PaaS)', *Business and Information Systems Engineering*, 3(6), pp. 381–384. Available at: <https://doi.org/10.1007/s12599-011-0183-3>.
- Zhang, L., Cui, Y., & Mu, Y. (2020). Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing. *IEEE Systems Journal*, 14, 387-397.
- Zhang, L., Zhou, W., & Chen, X. (2020). 5G and cloud computing: A comprehensive review. *Journal of Cloud Computing: Advances, Systems and Applications*, 9(1), 1-17.
- Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, 1(1), 7–18. <https://doi.org/10.1007/s13174-010-0007-6>
- Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, 1(1), 7-18.
- Zhao, N., Xu, X., & Zhang, Y. (2019). 5G mobile networks: Technology overview and challenges. *IEEE Access*, 7, 100562-100576.
- Zhou, M., Zhang, C., & Xu, H. (2020). Cloud computing security issues and challenges: A survey. *International Journal of Computer Applications*, 49(16), 23-30.
- Zhou, S. et al. (2024) 'THE IMPACT OF PRICING SCHEMES ON CLOUD COMPUTING AND DISTRIBUTED SYSTEMS', *Journal of Knowledge Learning and Science Technology* ISSN: 2959-6386 (online), 3(3), pp. 193–205. Available at: <https://doi.org/10.60087/jklst.v3.n3.p206-224>.
- Zhou, S., Yuan, B., Xu, K., Zhang, M., & Zheng, W. (2024). THE IMPACT OF PRICING SCHEMES ON CLOUD COMPUTING AND

DISTRIBUTED SYSTEMS. *Journal of Knowledge Learning and Science Technology* ISSN: 2959-6386 (Online), 3(3), 193–205.  
<https://doi.org/10.60087/jklst.v3.n3.p206-224>

Zikopoulos, P., Eaton, C., & Deroos, D. (2017). *Cloud Computing: A Practical Approach for Learning and Implementation*. McGraw-Hill Education.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3), 583–592.  
<https://doi.org/10.1016/j.future.2010.12.006>



# Biodata Penulis



**Ir. Mila Jumarlis, S.Pt., S.Kom., M.Kom., IPP.**

Lulus S-1 di program Studi Sosial Ekonomi Peternakan Universitas Hasanuddin tahun 2009, S-1 Teknik Informatika Universitas pejuang Republik Indonesia Tahun 2016, S-2 Sistem Komputer STMIK Handayani Tahun 2015, Program Profesi Insinyur Universitas Muslim Indonesia tahun 2021. Saat ini adalah Dosen Tetap di STAIN Majene. Aktif di beberapa organisasi yaitu Asosiasi Pendidikan Tinggi Informatika dan Komputer (APTIKOM), Ikatan Ahli Informatika Indonesia (IAII),

Perkumpulan Dosen Indonesia Semesta (DIS) dan Persatuan Insinyur Indonesia (PII) pemberdayaan Perempuan.



**Indah Purnama Sari, S.T., M.Kom.** Lahir di Medan pada tanggal 18 April 1990. Lulus S1 di Program Studi Teknik Informatika Fakultas Teknik Informatika Universitas Islam Sumatera Utara (UISU) tahun 2012, lulus S2 di Program Magister Teknik Informatika Universitas Sumatera Utara (USU) tahun 2019. Saat ini adalah dosen tetap Program Studi Teknologi Informasi Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara.

Mengampu mata kuliah Algoritma dan Pemrograman, Rekayasa Perangkat Lunak, Pemrograman Internet Dasar, Pengolahan Citra Digital, Pemrograman Berorientasi Objek, Logika Informatika, Penulisan Proposal, Aplikasi Komputer dan Teknologi Informasi. Pernah menjadi dosen tamu di Program Studi D-3 Manajemen Informatika, Politeknik Ganesa, Universitas Prima Indonesia. Aktif menulis artikel di Jurnal Nasional Informatika dan Teknologi Jaringan (InfoTekjar), Hello Word, Blend Sains, Sudo dan Journal of Computer Science, Information Technology and

Telecommunication Engineering (JCoSITTE) dan menjadi pemateri dalam seminar konferensi Internasional dan Nasional.

Dan juga menjadi Editor In Chief pada Jurnal Hanif Journal of Information Systems, Tsabit Journal of Computer Science, dan IjatCoss.

Selama ini terlibat aktif dalam kegiatan MSIB Studi Independent dan terlibat aktif dalam pengelolaan jurnal.

Telah menulis 4 Buku ajar, yakni Rekayasa Perangkat Lunak, Pemrograman Internet Dasar, Algoritma dan Pemrograman dan Buku Aplikasi Komputer. Dan menjadi Editor Buku Artificial Intelligence dan Kalkulus Integral.

E-mail: indahpurnama@umsu.ac.id



**Heru Saputra** adalah seorang dosen tetap di salah satu universitas swasta di Kota Padang, Sumatera Barat. Ia menyelesaikan pendidikan S1-nya di Jurusan Sistem Informasi dan melanjutkan studi S2 pada jurusan yang sama di Universitas UPI YPTK Padang. Dengan latar belakang akademik yang kuat dalam bidang sistem informasi, Heru Saputra memiliki keahlian mendalam di berbagai disiplin ilmu modern, seperti Blockchain, Machine Learning, Virtual Reality/Augmented Reality (VR/AR), serta Artificial Intelligence (AI).

Selain aktif mengajar dan melakukan penelitian, ia juga berkontribusi secara signifikan dalam dunia akademik sebagai editor di Indonesian Journal of Computer Science (IJCS). Tidak hanya itu, Heru Saputra juga dipercaya menjadi reviewer dalam seminar nasional bergengsi, seperti SENATIKA 3 dan SENATIKA 4. Kiprahnya sebagai narasumber dalam berbagai seminar nasional juga semakin memperkuat reputasinya sebagai ahli di bidang sistem informasi. Hingga saat ini, Heru Saputra telah menulis 15 buku referensi yang banyak digunakan sebagai sumber belajar di perguruan tinggi maupun kalangan profesional. Beberapa judul buku: Teknologi Cloud Computing, Sistem Multimedia, Perancangan Basis Data, Pembelajaran Berbasis Multimedia, Teknologi Jaringan Nirkabel, Transformasi Digital: Memahami Internet of Things, Sistem Basis Data: Konsep, Desain, dan Implementasi, Teknologi Finansial, E-commerce, dan Blockchain. Buku-buku tersebut mencerminkan dedikasinya untuk berbagi pengetahuan dan pengalaman kepada generasi muda

serta masyarakat luas tentang perkembangan teknologi terkini. Heru Saputra dapat dihubungi melalui email: [h3ru.saputra@gmail.com](mailto:h3ru.saputra@gmail.com). Dengan segala kontribusinya dalam dunia pendidikan dan teknologi, Heru Saputra terus menginspirasi banyak orang melalui tulisan-tulisannya yang inovatif dan relevan dengan kebutuhan zaman.



**Suhardi Aras**, merupakan lulusan dari program S1 Universitas Dipanegara Makassar dan program S2 pada Universitas Amikom Yogyakarta. Ia adalah dosen tetap Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Sorong

Mengampu mata kuliah Kecerdasan Buatan dan Deep Learning.

Merupakan Founder dari Rumah Kata Sorong @rumahkatasorong yang merupakan ruang baca publik dan komunitas sastra di Kota Sorong. Mengelola juga Rumah Koding Sorong sebagai ruang belajar Computational Thinking for Kid.

E-mail: [suhardi.aras@gmail.com](mailto:suhardi.aras@gmail.com) [suhardi.aras@um-sorong.ac.id](mailto:suhardi.aras@um-sorong.ac.id)



**Sitti Suhada** Penulis lahir di Kota Makassar Provinsi Sulawesi Selatan tepatnya tanggal 28 Mei 1978. Sejak tahun 2003 penulis merupakan salah satu dosen tetap di Jurusan Teknik Informatika, Fakultas Teknik, Universitas Negeri Gorontalo. Penulis menyelesaikan Program Sarjana (S1) Jurusan Teknik Informatika di STMIK Dipanegara Makassar tahun 2003, Program Magister(S2)

Konsentrasi Teknik Informatika di Universitas Hasanuddin Makassar tahun 2013 dan saat ini melanjutkan studi Program Doktor di Program Studi Pendidikan Vokasi Keteknikan Program Pascasarjana Universitas Negeri Makassar. Penulis bisa dihubungi via nomor 081355514142 atau melalui E-mail [sittisuhada@ung.ac.id](mailto:sittisuhada@ung.ac.id)



**Andi Ikmal Rachman** lahir di Kabupaten Wajo, pada 27 November 1991. Merupakan anak bungsu 3 (tiga) bersaudara dari pasangan H. A. Rachman Guna (ayah) dan Hj Hasriana Hasyim (ibu). Lulus sarjana pada Program Studi Teknik Informatika STMIK Dipanegara pada tahun 2013 dan menyelesaikan studi Pasca Sarjana pada Program Studi Manajemen Informatika di Universitas Muslim Indonesia tahun 2016. Memulai karir sebagai civitas akademika sejak tahun 2021. Saat ini menjadi dosen tetap yayasan di Universitas Almarisah Madani. Saat penulisan buku ini, berhomebase pada Universitas Almarisah Madani Makassar Program Studi Sistem Informasi.

E-mail: [andiikmalrachman01@gmail.com](mailto:andiikmalrachman01@gmail.com)



**Dr. Ir. Adam M. Tanniewa, S.Kom.,SE.,MM.,MT.,IPM.,Asean Eng.** Telah mengenyam pendidikan S1 di Fakultas Ilmu Komputer Universitas Indonesia Timur tahun 2005, Makassar, melanjutkan pendidikan Magister Teknik pada Universitas Hasanuddin, Makassar Tahun 2008 dan Telah menyelesaikan Pendidikan S3 pada Universitas Muslim Indonesia Tahun 2022. Bekerja Sebagai Dosen sejak tahun 2005 sampai saat ini di Universitas Sulawesi Barat.

Mengampu mata kuliah Sistem Informasi Manajemen, Metodologi Penelitian, Manajemen Proyek Perangkat Lunak, Proyek Perangkat Lunak, Kewirausahaan. Aktif di dalam berbagai Organisasi di antaranya APTIKOM, PII, IAI dan Organisasi lainnya. Telah menulis beberapa Buku referensi dan Aktif dalam melakukan penelitian publikasi jurnal nasional dan Internasional

E-mail: [adamtanniewa76@gmail.com](mailto:adamtanniewa76@gmail.com)



**Defiariany** lahir di Padang Panjang, pada 12 Maret 1968. Pendidikan Sarjana (S1) diselesaikan STMIK YPTK Padang (UPI Padang) lulus tahun 1993. Pendidikan Program Pascasarjana (S2) Komputer dengan konsentrasi Sistem Informasi diselesaikan Universitas Putra Indonesia Padang (UPI Padang) lulus tahun 2009 Berprofesi sebagai Dosen sejak tahun 2003, pernah mengajar di beberapa PTS di Sumatera Barat, dan menjadi dosen tetap di Universitas Metamedia di Padang, Program Studi Sistem Informasi sampai sekarang. Pernah menjabat sebagai Ketua Program Studi Sistem Informasi tahun 2014, sebagai pengurus bidang penelitian Asosiasi Pendidikan Tinggi Informatika dan Komputer (APTIKOM) Provinsi Sumatera Barat periode tahun 2018-2022. Mengampu beragam matakuliah, dan sudah menyelesaikan 8 buku referensi.



Penulis merupakan lulusan sarjana Teknik Informatika dari Universitas Bina Nusantara, Jakarta. Magister Komputer dari STMIK Eresha, Jakarta, jurusan Teknik Informatika dan sedang melanjutkan pendidikan doctoral pada Asia eUniversity, Kuala Lumpur Malaysia. Selain sebagai dosen di Universitas Mercu Buana Jakarta pada Fakultas Ilmu Komputer, jurusan Sistem Informasi, penulis juga aktif terlibat bekerja sebagai Konsultan pada berbagai proyek TI sejak tahun 2010. Pengalaman terlibat dalam berbagai proyek TI tersebut memberikan banyak manfaat untuk bisa berbagi pengetahuan dan pengalaman saat di kelas maupun sebagai bahan penelitian ataupun saat melakukan pengabdian masyarakat, sebagai bagian dari Tri Dharma Pendidikan.

Bidang spesialisasi yang penulis tekuni antara lain Project Management, IT Governance, dan Software Engineering. Penulis juga aktif berorganisasi pada Project Management Institute (PMI) Indonesia Chapter. Selain itu penulis sering kali memberikan pelatihan profesional untuk pelatihan sertifikasi internasional seperti: ITIL 4 Foundation, COBIT 2019 Foundation, serta PRINCE2 Foundation. Penulis menyadari teknologi selalu berkembang setiap saat oleh sebab itu penulis senantiasa untuk selalu belajar dan membagi pengetahuan serta pengalamannya baik saat di kelas ataupun melalui media buku ini, semoga

pengetahuan yang sedikit ini bisa memberikan manfaat bagi pembaca. Semua ini hanya karena Allah SWT semata yang telah memberikan karuniaNya.

Email Penulis: bayu.waseso@mercubuana.ac.id, bwaseso@gmail.com

**Ir. Mirfan.,S.Kom., M.T., M.Kom., IPM., ASEAN Eng.** Lulus S-1 di



Program Studi Teknik Informatika STMIK Handayani Tahun 2005, S-2 Teknik Elektro Universitas Hasanuddin Tahun 2015, S-2 Sistem Komputer STMIK Handayani Tahun 2016, Program Profesi Insinyur UMI Tahun 2021, saat ini adalah Dosen tetap Pada Universitas Handayani Makassar, Aktif di beberapa organisasi yaitu Asosiasi Pendidikan Tinggi Informatika dan Komputer (APTIKOM), IKatan Ahli Informatika Indonesia, Forum Dosen Indonesia. Pengurus Badan Kejuruan

Informatika PII & Majelis Uji Kompetensi Badan Kejuruan Informatika PII



**Muharman Lubis** telah meraih gelar Doctor of Philosophy untuk program Information Technology dari International Islamic University Malaysia. Menyelesaikan pendidikan Master di Universitas yang sama dan program Bachelor di Universiti Utara Malaysia dengan kekhususan pada Jaringan Komputer. Saat ini sedang menempuh pendidikan Magister Manajemen di Universitas Widyatama, Sarjana Hukum di Universitas Terbuka, dan Double Degree pada International Open University untuk Bachelor of Art (Islamic Studies) dan Bachelor of

Science (Psychology). Mampu beragam mata kuliah dari Tata Kelola Data dan Teknologi Informasi, Analisa Data dan Bisnis Perusahaan, Transformasi dan Strategi Digital, Inovasi dan Kewirausahaan Teknologi, Manajemen Pengetahuan dan Sumber Daya, Metodologi Penelitian, Hukum dan Etika Siber. Menulis beberapa jurnal ilmiah dan seminar internasional terkait Perlindungan Data Pribadi, Strategi Sistem Informasi Organisasi, dan Ketangguhan dan Jaminan Siber.

E-mail: muharmanlubis@telkomuniversity.ac.id



**Dr. Ir. Janner Simarmata, S.T., M.Kom. (C.SP., C.BMC., C.DMP., C.PI., C.PKIR., C.SF., C.PDM., C.SEM., C.COM., C.SI., C.SY., C.STMI INT'L, CBPA., C.WI.)** Sarjana Teknik Informatika dari STMIK Bandung, Magister Ilmu Komputer dari Universitas Gadjah Mada (UGM) dan Doktor Pendidikan Teknologi Kejuruan (PTK) diperoleh dari Universitas Pendidikan Indonesia (UPI) Bandung bidang kajian Blended Learning. Program Profesi Insinyur (PPI) dari Institut Teknologi Indonesia (ITI).

Alumni Tapla II 2004 Lemhannas RI . Menulis buku sejak tahun 2005 dan telah menulis 315 buku dan 200 HKI. Dosen di Pendidikan Teknologi Informatika dan Komputer (PTIK) Fakultas Teknik Universitas Negeri Medan.



# Dasar Dasar **CLOUD COMPUTING & SISTEM INFORMASI**

Seiring dengan perkembangan teknologi yang begitu pesat, kebutuhan akan layanan komputasi awan (cloud computing) menjadi semakin mendesak, baik di sektor bisnis, pemerintahan, maupun pendidikan. Melalui buku ini, pembaca akan dibimbing untuk memahami fondasi dasar cloud computing, mulai dari karakteristik, model layanan, jenis-jenis cloud, hingga arsitektur dan isu-isu keamanan yang melekat di dalamnya. Tak hanya itu, buku ini juga mengulas berbagai aspek penting seperti virtualisasi, manajemen sumber daya, serta penerapannya dalam sistem informasi dan dunia pendidikan.

Buku ini membahas:

- Bab 1 Dasar-Dasar Cloud Computing
- Bab 2 Karakteristik Cloud Computing
- Bab 3 Model Layanan Cloud Computing
- Bab 4 Jenis - Jenis Cloud Computing
- Bab 5 Arsitektur Cloud Computing
- Bab 6 Keamanan dalam Cloud Computing
- Bab 7 Keuntungan dan Kerugian Cloud Computing
- Bab 8 Virtualisasi dan Penggunaan Cloud
- Bab 9 Manajemen Proyek Sistem Informasi Berbasis Cloud
- Bab 10 Cloud Computing Dalam Pendidikan
- Bab 11 Tantangan dalam Penggunaan Cloud Computing
- Bab 12 Tren Masa Depan Cloud Computing



YAYASAN KITA MENULIS  
press@kitamenulis.id  
www.kitamenulis.id

