



Cloud System

Knowledge Management

Disusun Oleh:

Tim Pengampu Mata Kuliah

Dr. Valentino Aris, S.Kom., MM.

Hartoto, S.Pd., M.Pd.

Muh. Qardawi Hamzah, S.Pd., M.Si.

Support By



Kata Pengantar

Puji syukur ke hadirat Allah SWT atas segala rahmat dan karunia-Nya sehingga penulisan buku yang berjudul *Cloud System* ini dapat diselesaikan. Buku ini hadir sebagai salah satu upaya untuk memberikan pemahaman mengenai sistem komputasi, yang kini menjadi fokus dalam pengelolaan data dan layanan teknologi informasi di era digital.

Penulisan buku ini dilatarbelakangi oleh kebutuhan yang semakin meningkat akan pengetahuan tentang cloud system, baik dalam bidang akademik maupun profesional. Sistem komputasi telah mengubah cara organisasi dan individu mengakses serta memanfaatkan teknologi, mulai dari penyimpanan data hingga pemrosesan informasi yang lebih efisien dan fleksibel.

Saya menyadari bahwa buku ini jauh dari kata sempurna, namun saya berharap bahwa karya ini dapat menjadi salah satu referensi yang bermanfaat, khususnya bagi mahasiswa, praktisi, serta siapa pun yang tertarik mempelajari lebih dalam mengenai cloud system. Dengan bahasa yang sederhana, diharapkan pembaca dapat memahami konsep dengan lebih mudah.

Ucapan terima kasih saya sampaikan kepada semua pihak yang telah memberikan dukungan, baik secara langsung maupun tidak langsung, sehingga buku ini bisa terwujud. Kepada para mahasiswa, kolega, dan pembaca, saya berharap kritik dan saran yang membangun demi kesempurnaan buku ini di masa mendatang.

Akhir kata, semoga buku ini dapat memberikan manfaat dan menjadi inspirasi bagi pembaca dalam memahami dan mengaplikasikan teknologi cloud system di kehidupan sehari-hari maupun dunia kerja.

Makassar, ... September 2024

Tim Penulis,

Daftar Isi

Kata Pengantar.....	ii
Daftar Isi	iii
BAB. INTRODUCTION TO CLOUD SYSTEM.....	1
A. Cloud System.....	1
B. Three Layers of Computing.....	3
C. Akhir Komputasi Tradisional	7
D. Latihan.....	8
BAB II. CLOUD SYSTEM :VOLUTION AND ENABLING TECHNOLOGY	10
A. Evolusi Teknologi Cloud.....	11
B. Latihan.....	23
BAB III. LOUD SYSTEM: BENEFIT AND CHALLENGES	25
A. Inisiator Awal <i>Cloud System</i>	25
B. Manfaat Cloud System	28
C. Tantangan Cloud System.....	31
D. Solusi mengatasi tantangan <i>Cloud System</i>	33
E. Latihan.....	36
BAB IV. CLOUD SYSTEM: BASIC NETWORK.....	39
A. Jaringan dan Jaringan Komputer	39
B. Jenis-Jenis Jaringan Komputer	42
C. Jaringan Komputer dan Cloud System	56
D. Latihan.....	60
BAB V. CLOUD SYSTEM SERVICE.....	62
A. SERVICE DELIVERY MODEL PADA CLOUD SYSTEM.....	62
B. SISTEM TRADISIONAL VS SISTEM CLOUD.....	73
C. Latihan.....	75
BAB VI. IMPLEMENTASI CLOUD SYSTEM	79

A.	Virtualisasi.....	79
B.	Virtual Private Cloud.....	800
C.	Virtual Data Center.....	833
D.	Latihan.....	86
BAB VII. CLOUD SYSTEM: SECURITY.....		8989
A.	Keamanan Cloud System (Cloud Security).....	889
B.	Ancaman Pada Cloud	92
C.	Cloud Security Design Principle	966
D.	Latihan.....	99
DAFTAR PUSTAKA.....		1022

BAB I

INTRODUCTION TO CLOUD SYSTEM

TUJUAN PEMBELAJARAN

1. Mahasiswa mampu memahami konsep *cloud system* atau *cloud computing*
2. Mahasiswa mampu menjelaskan keterbatasan komputasi tradisional
3. Mahasiswa mampu menjelaskan tiga lapisan dalam sistem komputasi berbasis cloud (*three layers of computing*)

Perkembangan teknologi komputasi sangat berkembang beberapa tahun terakhir. Telah terjadi perkembangan yang signifikan di bidang perangkat keras komputasi, arsitektur perangkat lunak, teknologi web, dan komunikasi jaringan. Akses dan kecepatan jaringan internet terus meningkat dan lebih murah. Perkembangan ini menyebabkan mulai dikenal sebuah konsep revolusioner yaitu “*cloud system*” atau “*cloud computing*”. Cloud system menyediakan teknologi yang lebih baik, cerdas dan murah untuk individu maupun pengguna bisnis. Bab ini mencoba untuk mengeksplorasi mengenai lapisan komputasi tradisional yang digunakan untuk bisnis yang menyebabkan munculnya teknologi cloud. Selain itu akan dibahas mengenai konsep cloud system. Perkembangan “*cloud system*” atau “*cloud computing*” ini telah mengubah cara pemanfaatan infrastruktur komputasi untuk keperluan individu maupun bisnis.

A. Cloud System

Cloud system menyediakan sarana dan fasilitas bagi pengguna untuk memanfaatkan fasilitas komputasi dengan mudah kapan pun dan dimanapun dengan memanfaatkan jaringan internet. Pengguna tidak perlu lagi menyediakan infrastruktur fisik dan membeli lisensi sebuah perangkat lunak. Pengguna fasilitas komputasi diberikan fasilitas berupa akses ke perangkat komputasi dengan biaya yang murah dan dapat diakses kapan saja. Dengan sarana dan fasilitas ini, *cloud system* memberikan manfaat yang sangat besar bagi pengguna individu maupun pengguna bisnis.

Perkembangan *cloud system* tidak lepas dari peran sistem komputasi tradisional selama beberapa tahun terakhir. Pada awal-awal penerapan system komputasi, perusahaan masih menjalankan bisnisnya dengan menggunakan perangkat-perangkat manual seperti pena, kertas, telepon, dan mesin faks. Secara bertahap, sistem komputer menggantikan proses manual dan mulai dikenal istilah otomatisasi. Pena dan kertas digantikan oleh perangkat digital dan bahkan layanan telepon dan faks mulai dikelola oleh komputer. Saat ini, bisnis mulai dari lokal hingga global mulai sangat bergantung pada sistem komputasi untuk melakukan semua aktivitas bisnisnya. Bahkan individu juga sudah sangat bergantung pada sistem komputasi untuk aktivitas sehari-hari.

Penerapan sistem komputasi tradisional ini mulai menimbulkan beberapa kendala dalam penerapannya pada bisnis. Kendala utamanya adalah kebutuhan infrastruktur yang besar untuk penerapan system komputasi yang baik. Tentunya pengadaan infrastruktur ini membutuhkan biaya yang besar mulai dari pembelian perangkat, pemeliharaan, pembayaran tenaga ahli untuk mengelola infrastruktur dan bahkan penyediaan ruangan dan fasilitas penunjang perangkat infrastruktur tersebut. Kendala lain, lisensi perangkat lunak yang berjalan pada perangkat keras infrastruktur juga menjadi beban bagi perusahaan. Hal ini menyebabkan system komputasi hanya dapat dimanfaatkan oleh perusahaan yang sudah memiliki nama besar dan penghasilan yang besar. Tidak hanya bagi pengguna bisnis, pengguna individu juga memiliki kendala yang hampir serupa.

Kondisi tersebut menyebabkan jika seorang individu atau pelaku bisnis ingin menyiapkan infrastruktur komputasi baik itu dalam kategori yang kecil maupun besar maka ada dua pilihan yang dapat dilakukan. Pilihannya adalah membeli sendiri perangkat infrastrukturnya atau menyewa dari penyedia jasa atau pihak ketiga. Tentunya opsi pertama terbatas hanya untuk Perusahaan yang sudah mapan dan berpenghasilan besar sedangkan opsi kedua dapat dipilih oleh Perusahaan baru atau yang sedang berkembang.

Menyewa dari pihak ketiga telah menjadi opsi yang digunakan oleh Perusahaan dalam beberapa tahun terakhir. Namun, pertanyaan besarnya adalah apakah optimal jika menyerahkan semua tanggungjawab pengembangan dan

pengelolaan infrastruktur dan aplikasi kepada pihak ketiga. Menggunakan jasa pihak ketiga tentunya dapat menghilangkan kebutuhan akan pengembangan dan pemeliharaan sistem atau aplikasi sampai pada batas tertentu, tapi tentunya memiliki beberapa persyaratan-persyaratan yang harus dipenuhi oleh Perusahaan dalam penyediaan jasa tersebut. Intinya bahwa kesulitan yang dihadapi oleh pengguna akan bergantung pada lapisan komputasi yang digunakan.

B. Three Layers of Computing

Komputer dan komputasi telah menjadi bagian tak terpisahkan dari kehidupan kita sehari-hari. Berbagai orang menggunakan berbagai kategori fasilitas komputasi. Fasilitas komputasi ini dapat disegmentasikan menjadi tiga kategori: infrastruktur, platform, dan aplikasi. Ketiga kategori fasilitas komputasi ini membentuk tiga lapisan dalam arsitektur dasar komputasi.

1. Lapisan Infrastruktur

Definisi dan Tujuan: Lapisan Infrastruktur adalah lapisan dasar dalam komputasi. Ini mencakup sumber daya fisik dan virtual yang diperlukan untuk mendukung operasi TI. Lapisan ini menyediakan daya komputasi mentah, kapasitas penyimpanan, dan kemampuan jaringan yang esensial bagi berjalannya perangkat lunak atau layanan apa pun.

Komponen:

- a. **Perangkat Keras Fisik:** Server, perangkat penyimpanan, dan peralatan jaringan yang ditempatkan di pusat data. Perangkat keras ini adalah dasar dari semua operasi komputasi.
- b. **Virtualisasi:** Teknologi seperti hypervisor (misalnya, VMware, Hyper-V, KVM) yang memungkinkan pembuatan mesin virtual (VM) di atas perangkat keras fisik. Virtualisasi memungkinkan pemanfaatan sumber daya fisik secara efisien dengan menjalankan beberapa VM pada satu server fisik.
- c. **Jaringan:** Router, switch, firewall, dan load balancer yang mengelola lalu lintas data dan memastikan komunikasi yang aman dan andal antar bagian infrastruktur.
- d. **Sistem Penyimpanan:** Termasuk penyimpanan blok (seperti SAN, DAS), penyimpanan objek (seperti Amazon S3), dan penyimpanan file (seperti

NAS). Sistem ini menyimpan data yang perlu diakses dan dimanipulasi oleh aplikasi.

- e. **Pusat Data:** Fasilitas fisik yang menampung perangkat keras dengan dukungan daya, pendinginan, dan keamanan yang diperlukan.

Peran:

- a. **Sumber Daya Komputasi:** Menyediakan daya pemrosesan melalui CPU dan GPU, yang memungkinkan eksekusi aplikasi dan layanan.
- b. **Sumber Daya Penyimpanan:** Menjamin ketahanan data, memungkinkan penyimpanan dan pengambilan file, basis data, dan lainnya.
- c. **Sumber Daya Jaringan:** Mengelola aliran data antara berbagai sistem, aplikasi, dan pengguna, baik di dalam pusat data maupun melalui internet.

Contoh:

- a. **Berbasis Cloud:** Amazon EC2 (Elastic Compute Cloud), Google Compute Engine, Microsoft Azure Virtual Machines.
- b. **On-Premises:** Pusat data milik perusahaan dengan server fisik dan penyimpanan array.

Pentingnya: Lapisan infrastruktur sangat penting karena menjadi dasar dari seluruh tumpukan TI. Tanpa infrastruktur yang andal, layanan di tingkat yang lebih tinggi (platform dan aplikasi) tidak dapat berfungsi dengan efisien atau andal.

2. Lapisan Platform

Definisi dan Tujuan: Lapisan Platform mengabstraksi kompleksitas manajemen infrastruktur yang mendasarinya, menyediakan lingkungan bagi pengembang untuk membangun, menerapkan, dan mengelola aplikasi. Lapisan ini dirancang untuk merampingkan siklus hidup pengembangan perangkat lunak dengan menawarkan alat, kerangka kerja, dan layanan yang menyederhanakan prosesnya.

Komponen:

- a. **Sistem Operasi:** Menyediakan lingkungan perangkat lunak dasar tempat aplikasi berjalan (misalnya, Linux, Windows Server).
- b. **Middleware:** Perangkat lunak yang menghubungkan berbagai aplikasi dan memungkinkan mereka untuk berkomunikasi (misalnya, server aplikasi

seperti Apache Tomcat, server web seperti Nginx, basis data seperti MySQL, antrean pesan seperti RabbitMQ).

- c. **Framework Pengembangan:** Alat dan perpustakaan yang menyederhanakan pembuatan perangkat lunak (misalnya, .NET, Java EE, Ruby on Rails).
- d. **Lingkungan Runtime:** Lingkungan tempat aplikasi dijalankan (misalnya, Java Runtime Environment, Node.js, runtime Python).
- e. **API dan SDK:** Antarmuka dan kit pengembangan yang memungkinkan pengembang berinteraksi dengan kapabilitas platform (misalnya, Google Maps API, AWS SDK).

Peran:

- a. **Abstraksi:** Menyembunyikan kompleksitas infrastruktur, memungkinkan pengembang fokus pada penulisan kode daripada mengelola perangkat keras dan konfigurasi tingkat rendah.
- b. **Skalabilitas:** Secara otomatis meningkatkan atau menurunkan sumber daya berdasarkan permintaan, memastikan aplikasi berjalan efisien tanpa intervensi manual.
- c. **Manajemen Lingkungan:** Menyediakan lingkungan untuk pengembangan, pengujian, staging, dan produksi, memungkinkan praktik integrasi dan pengiriman terus-menerus (CI/CD).
- d. **Integrasi Layanan:** Menawarkan layanan siap pakai (seperti basis data, alat AI/ML, dan analitik) yang dapat dengan mudah diintegrasikan ke dalam aplikasi, mempercepat pengembangan.

Contoh:

- a. **Berbasis Cloud:** Google App Engine, Microsoft Azure App Services, AWS Elastic Beanstalk.
- b. **On-Premises:** Platform seperti Red Hat OpenShift, VMware Tanzu.

Pentingnya: Lapisan platform sangat penting untuk mempercepat pengembangan dan penerapan aplikasi. Dengan mengabstraksi kompleksitas manajemen infrastruktur, lapisan ini memungkinkan pengembang berinovasi lebih cepat dan fokus pada penciptaan nilai bisnis.

3. Lapisan Aplikasi

Definisi dan Tujuan: Lapisan Aplikasi adalah lapisan teratas yang mencakup aplikasi end-user yang dibangun di atas platform. Ini adalah produk perangkat lunak yang berinteraksi langsung dengan pengguna akhir untuk melakukan tugas, baik untuk penggunaan pribadi, operasi bisnis, atau tujuan lainnya.

Komponen:

- a. **Aplikasi Pengguna Akhir:** Perangkat lunak yang digunakan oleh individu atau organisasi untuk menyelesaikan tugas tertentu (misalnya, Microsoft Office, Google Workspace, Salesforce).
- b. **Aplikasi Bisnis:** Solusi perangkat lunak perusahaan yang dirancang untuk memenuhi kebutuhan bisnis tertentu, seperti Sistem Manajemen Hubungan Pelanggan (CRM), Sistem Perencanaan Sumber Daya Perusahaan (ERP), dan alat kolaborasi.
- c. **Aplikasi Web:** Aplikasi yang berjalan di browser web, dapat diakses dari perangkat apa pun dengan akses internet (misalnya, Gmail, Trello, Slack).
- d. **Aplikasi Seluler:** Perangkat lunak yang dirancang untuk perangkat seluler, menyediakan fungsionalitas saat bepergian (misalnya, WhatsApp, Instagram, aplikasi perbankan seluler).

Peran:

- a. **Interaksi Pengguna:** Menyediakan antarmuka bagi pengguna untuk berinteraksi dengan perangkat lunak, baik melalui browser web, perangkat seluler, atau aplikasi desktop.
- b. **Fungsionalitas Bisnis:** Menyediakan fungsionalitas spesifik yang dibutuhkan oleh bisnis, seperti memproses transaksi, mengelola hubungan pelanggan, atau mengotomatisasi alur kerja.
- c. **Manipulasi Data:** Berinteraksi dengan lapisan platform dan infrastruktur untuk mengambil, memproses, dan menyimpan data berdasarkan input pengguna dan logika bisnis.
- d. **Pengiriman Layanan:** Menyediakan perangkat lunak sebagai layanan (SaaS) di mana aplikasi dihosting dan dikelola oleh penyedia pihak ketiga, dapat diakses melalui internet.

Contoh:

- a. **Cloud-Based SaaS:** Google Workspace (Gmail, Google Drive), Salesforce CRM, Microsoft Office 365.
- b. **Aplikasi On-Premises:** Perangkat lunak desktop tradisional seperti Microsoft Word, aplikasi perusahaan yang di-hosting di dalam pusat data perusahaan.

Pentingnya: Lapisan aplikasi adalah tempat nilai komputasi diterjemahkan ke dalam penggunaan akhir. Lapisan ini sangat penting untuk menerjemahkan persyaratan bisnis dan kebutuhan pengguna menjadi solusi perangkat lunak fungsional yang mendorong produktivitas, kolaborasi, dan inovasi.

Interaksi Antarlapisan

1. **Infrastruktur Mendukung Platform:** Lapisan infrastruktur menyediakan sumber daya komputasi, penyimpanan, dan jaringan yang diperlukan agar lapisan platform dapat beroperasi. Tanpa infrastruktur yang andal, platform tidak dapat memberikan layanan yang skalabel dan andal.
2. **Platform Mendukung Aplikasi:** Lapisan platform menyederhanakan proses pengembangan, penerapan, dan pengelolaan aplikasi. Ia mengabstraksi kompleksitas infrastruktur yang mendasarinya, memungkinkan pengembang fokus pada pembangunan aplikasi fungsional.
3. **Aplikasi Memberikan Nilai kepada Pengguna Akhir:** Lapisan aplikasi menyediakan alat dan layanan perangkat lunak yang berinteraksi dengan pengguna setiap hari. Aplikasi ini dibangun di atas platform, yang pada gilirannya bergantung pada infrastruktur yang mendasarinya.

C. Akhir Komputasi Tradisional

Keterbatasan yang dimiliki oleh komputasi tradisional yang telah dijelaskan pada sub bab sebelumnya menyebabkan berkembangnya ide-ide futuristik mengenai solusi untuk mengatasi permasalahan tersebut. Perkembangan teknologi informasi dan komunikasi menyebabkan beberapa perusahaan besar dibidang teknologi mengembangkan ide penyediaan sistem komputasi berdasarkan lapisan komputasi. Filosofinya bahwa fasilitas komputasi dapat diberikan kepada pengguna dalam bentuk layanan. Hal ini memberikan aksesibilitas pengguna terhadap sistem komputasi semakin terbuka, mereka tidak perlu lagi membeli infrastruktur,

melakukan perawatan, dan menyewa tenaga ahli. Semua layanan tersebut akan diberikan oleh penyedia layanan.

Layanan ini akan disediakan oleh vendor yang berkualitas dimana mereka adalah Perusahaan teknologi yang besar dan kredible. Vendor ini akan menyediakan layanan dalam tiga kategori sesuai dengan lapisan komputasi yaitu infrastruktur, platform dan aplikasi. Pelanggan dapat menyesuaikan kebutuhannya berdasarkan tiga kategori lapisan tersebut. Jika pelanggan hanya membutuhkan aplikasi. Pada lapisan ini, pelanggan tidak perlu lagi repot dalam mengelola infrastruktur sehingga mereka dapat lebih fokus terhadap kebutuhannya berupa aplikasi. Layanan ini dipercaya akan membantu perusahaan lebih fokus pada bisnisnya tanpa pusing memikirkan infrastruktur komputasi. Layanan ini juga dapat membantu mengurangi biaya infrastruktur komputasi dengan sangat signifikan.

D. Latihan

a. Pilihan Ganda

Jawablah soal pilihan ganda berikut ini!

1. Pada awal penerapan system komputasi, perusahaan menggunakan perangkat apa untuk menjalankan bisnisnya?
 - a. Komputer server
 - b. Pena, kertas, telepon, dan mesin faks
 - c. Cloud server
 - d. Database Modern
 - e. Perangkat lunak otomatisasi
2. Apa yang termasuk dalam komponen perangkat keras fisik di lapisan infrastruktur ?
 - a. Virtual machine
 - b. Hypervisor
 - c. Server, perangkat penyimpanan dan peralatan jaringan
 - d. Software aplikasi
 - e. Firewall dan load balancer
3. Apa tujuan utama dari lapisan infrastruktur dalam komputasi?
 - a. Menyimpan data cadangan

- b. Mengelola perangkat lunak
 - c. Mengatur perangkat virtual
 - d. Menyediakan daya komputasi mentah
 - e. Menyediakan aplikasi untuk pengguna
4. Contoh aplikasi pengguna akhir di lapisan aplikasi adalah
- a. System perencanaan sumber daya perusahaan (ERP)
 - b. Microsoft Office dan Google Workspace
 - c. Hypervisor dan mesin virtual
 - d. Switch dan router
 - e. Amazon web services (AWS)
5. Apa keuntungan dari penggunaan cloud system?
- a. Pengguna tidak perlu menyediakan infrastruktur fisik dan membeli lisensi perangkat lunak
 - b. Pengguna harus mengelola infrastrukturnya sendiri
 - c. Pengguna harus membayar biaya tinggi untuk pemeliharaan perangkat
 - d. Pengguna tidak memerlukan koneksi internet
 - e. Pengguna harus membeli perangkat keras secara manual

a. Esai

Jawablah pertanyaan dibawah ini!

1. Lapisan Infrastruktur adalah lapisan dasar dalam komputasi. Lapisan infrastruktur memiliki beberapa komponen. Jelaskan komponen-komponen yang termasuk dalam Lapisan Infrastruktur!
2. Perkembangan *cloud system* tidak lepas dari peran sistem komputasi tradisional selama beberapa tahun terakhir. Namun system komputasi tradisional memiliki kendala. Jelaskan kendala yang dimaksud!
3. Dengan menggunakan contoh nyata, analisis interaksi antara lapisan infrastruktur, *platform*, dan aplikasi dalam *cloud computing*. Bagaimana ketiga lapisan ini berkolaborasi untuk meningkatkan performa dan efisiensi bisnis!

BAB II

CLOUD SYSTEM: EVOLUTION AND ENABLING TECHNOLOGY

TUJUAN PEMBELAJARAN

1. Mahasiswa mampu menjelaskan evolusi teknologi yang mempengaruhi perkembangan teknologi *cloud system* atau *cloud computing*
2. Mahasiswa mampu menjelaskan teknologi enabler yang mempengaruhi perkembangan teknologi *cloud system* atau *cloud computing*

Cloud computing bukanlah sebuah inovasi yang terjadi secara tiba-tiba. Sebaliknya, ini merupakan rangkaian perkembangan yang berlangsung selama beberapa dekade terakhir. Kemajuan dalam teknologi komputasi, sejak masa awalnya, secara perlahan berkembang menjadi cloud computing di era modern ini. Meskipun gagasan tentang cloud computing telah muncul sejak lama, konsep tersebut tidak dapat terwujud karena kurangnya elemen teknologi yang diperlukan.

Bukti dokumentasi dapat ditelusuri hingga tahun 1960-an, ketika John McCarthy (yang menciptakan istilah '*artificial intelligence*') menulis bahwa 'suatu hari nanti, komputasi dapat diorganisasikan sebagai utilitas publik.' Sejak saat itu, teknologi komputasi telah melalui berbagai fase perkembangan. Teknologi perangkat keras dan komunikasi terus maju, internet telah mengubah dunia, dan pada saat yang sama, arsitektur perangkat lunak berbasis web juga semakin matang.

Seiring dengan kemajuan di semua bidang terkait yang secara perlahan mengatasi keterbatasan pendekatan sebelumnya, mimpi untuk mewujudkan komputasi sebagai bentuk utilitas publik baru akhirnya dapat tercapai. Bab ini berfokus pada evolusi cloud computing dan membahas bagaimana perkembangannya melalui tahapan seperti komputasi terpusat, komputasi *client-server*, komputasi terdistribusi, dan komputasi grid hingga mencapai *cloud computing*.

A. Evolusi Teknologi Cloud

Beberapa dekade penelitian, khususnya dalam bidang komputasi paralel dan terdistribusi, telah membuka jalan bagi cloud computing. Berikut beberapa perkembangan teknologi sehingga teknologi cloud dapat berkembang seperti saat ini:

1. Mainframe Architecture

Mainframe architecture adalah arsitektur komputasi yang berpusat pada penggunaan komputer mainframe, yang merupakan sistem komputer besar dan kuat yang dirancang untuk menangani beban kerja yang sangat besar, memproses data dalam jumlah besar, serta menyediakan layanan komputasi yang sangat andal dan aman. Pada arsitektur mainframe, semua pemrosesan utama dilakukan di satu komputer sentral, yaitu **mainframe**. Terminal-terminal pengguna, yang dulu dikenal sebagai "dumb terminals," terhubung ke mainframe, namun terminal-terminal ini hanya berfungsi sebagai antarmuka untuk berinteraksi dengan mainframe dan tidak memiliki kemampuan pemrosesan sendiri. Semua perhitungan, pemrosesan data, dan penyimpanan dilakukan di mainframe.

Mainframe dikenal karena kemampuannya memproses sejumlah besar transaksi sekaligus dan mengelola data dalam skala besar. Misalnya, mainframe digunakan di berbagai institusi seperti bank, pemerintah, dan perusahaan besar untuk memproses jutaan transaksi per detik. Sistem mainframe terkenal karena tingkat reliabilitas (keandalan) yang sangat tinggi. Mainframe biasanya dirancang dengan toleransi kesalahan yang baik, artinya jika ada komponen yang gagal, sistem tetap bisa berjalan tanpa mengganggu operasi yang sedang berlangsung. Dalam konteks bisnis yang sangat kritis, seperti sistem perbankan atau penerbangan, downtime hampir tidak dapat diterima, sehingga arsitektur mainframe sangat ideal untuk skenario ini.

Arsitektur mainframe menyediakan lapisan keamanan yang kuat, baik dari sisi perangkat keras maupun perangkat lunak. Sistem ini sangat dilindungi dari gangguan luar seperti serangan siber, menjadikannya pilihan utama bagi organisasi yang membutuhkan perlindungan data yang ketat.

Mainframe biasanya menggunakan sistem operasi khusus, seperti z/OS dari IBM, yang dirancang untuk mendukung multitasking, multiproses, dan memaksimalkan kinerja perangkat keras mainframe. Mainframe mendukung dua jenis pemrosesan utama yaitu Pemrosesan Batch: Memproses data dalam jumlah besar sekaligus, seperti pengolahan transaksi keuangan pada akhir hari dan Pemrosesan Online (OLTP - Online Transaction Processing): Memproses transaksi dalam waktu nyata atau seketika, seperti transaksi ATM yang segera memperbarui saldo rekening. Mainframe biasanya menggunakan sistem operasi khusus, seperti z/OS dari IBM, yang dirancang untuk mendukung multitasking, multiproses, dan memaksimalkan kinerja perangkat keras mainframe. Mainframe mampu menjalankan beberapa mesin virtual dalam satu perangkat fisik melalui partisi logis (Logical Partitions, atau LPARs). Setiap partisi ini dapat menjalankan sistem operasi yang berbeda atau aplikasi yang berbeda secara bersamaan, tanpa mengganggu satu sama lain. Banyak perusahaan besar masih menggunakan **sistem lama** yang berbasis mainframe karena sulit memigrasikan sistem yang sudah sangat mapan ini ke platform modern. Mainframe sering diintegrasikan dengan teknologi terbaru untuk mempertahankan fungsionalitas sambil memanfaatkan keandalan arsitektur tradisional.

2. Intelligence Terminal

Intelligent terminal adalah perangkat keras komputasi yang mampu memproses data secara lokal sebelum mengirimkannya ke sistem pusat atau server. Tidak seperti dumb terminal yang hanya berfungsi sebagai antarmuka pengguna dan bergantung sepenuhnya pada komputer pusat untuk pemrosesan data, intelligent terminal memiliki kemampuan pemrosesan sendiri. Hal ini membuatnya dapat melakukan sejumlah tugas mandiri, seperti memvalidasi data, memproses input, dan menjalankan aplikasi sederhana, sebelum berkomunikasi dengan sistem utama.

Karakteristik Utama Intelligent Terminal:

- a. Kemampuan Pemrosesan Lokal: Intelligent terminal dilengkapi dengan CPU, memori, dan terkadang penyimpanan lokal. Ini memungkinkannya untuk menjalankan aplikasi dasar, memproses data secara lokal, dan menyimpan data sementara sebelum berkomunikasi dengan komputer pusat.
- b. Konektivitas ke Sistem Pusat: Intelligent terminal masih terhubung dengan mainframe atau server, tetapi tidak bergantung sepenuhnya pada sistem tersebut. Terminal ini dapat mengirim dan menerima data, tetapi banyak pemrosesan terjadi di terminal itu sendiri, mengurangi beban pada sistem pusat.
- c. Efisiensi Operasional: Dengan pemrosesan lokal, intelligent terminal mengurangi jumlah data mentah yang perlu dikirimkan ke sistem pusat. Hanya data yang telah diproses atau hasil akhirnya yang dikirimkan, yang membantu mengurangi lalu lintas jaringan dan meningkatkan efisiensi sistem secara keseluruhan.
- d. Contoh Penggunaan:

ATM (Anjungan Tunai Mandiri): ATM merupakan salah satu contoh nyata intelligent terminal. ATM dapat melakukan sejumlah pemrosesan mandiri, seperti memvalidasi kartu, menghitung saldo, dan berinteraksi dengan pengguna, sebelum berkomunikasi dengan server bank untuk otorisasi transaksi.

POS (Point of Sale): Terminal penjualan (POS) di kasir adalah contoh lain. Terminal ini memproses transaksi penjualan lokal, seperti menghitung total, memproses pembayaran kartu, dan mencetak struk, kemudian mengirim hasil akhirnya ke server pusat.
- e. Aplikasi Tersimpan Lokal: Intelligent terminal sering kali memiliki perangkat lunak atau aplikasi yang diinstal secara lokal. Ini memungkinkan terminal untuk menangani berbagai tugas tanpa selalu harus mengakses server atau mainframe.
- f. Pengurangan Ketergantungan pada Sistem Pusat: Dibandingkan dengan dumb terminal, intelligent terminal lebih mandiri. Jika sambungan ke

sistem pusat terganggu, terminal ini masih bisa menjalankan beberapa fungsi dasar karena adanya pemrosesan lokal.

Perbedaan Intelligence Terminal dengan Dumb Terminal

Aspek	Intelligence Terminal	Dumb Terminal
Kemampuan Pemrosesan	Memiliki kemampuan pemrosesan lokal (CPU, memori)	Tidak memiliki kemampuan pemrosesan lokal
Ketergantungan	Mandiri, bisa memproses data tanpa terus-menerus terhubung ke server	Sangat tergantung pada mainframe atau server
Kinerja	Lebih cepat karena tidak semua tugas dikirim ke server	Bergantung pada kecepatan dan kapasitas sistem pusat
Contoh	ATM, POS, terminal medis	Terminal lama untuk mainframe atau komputer mini

3. Revolusi Personal Computer

Revolusi PC mengacu pada periode transformatif pada 1980-an dan 1990-an ketika komputer pribadi (PC) menjadi lebih luas, terjangkau, dan terintegrasi ke dalam kehidupan sehari-hari. Ini secara fundamental mengubah cara individu dan bisnis berinteraksi dengan teknologi, menggeser komputasi dari sistem terpusat (seperti mainframe) ke sistem individual yang terlokalisasi. Sebelum revolusi PC, komputasi sangat bergantung pada mainframe atau minikomputer di mana pengguna mengakses kekuatan pemrosesan melalui terminal. PC memungkinkan pengguna untuk memproses secara lokal tanpa bergantung pada sistem jarak jauh, memberikan otonomi dalam pemrosesan, penyimpanan data, dan eksekusi perangkat lunak.

Dengan munculnya PC, individu dapat menjalankan berbagai aplikasi (seperti pengolah kata, spreadsheet, dan perangkat lunak grafis) langsung di

komputer mereka sendiri. Microsoft Office dan Lotus 1-2-3 adalah contoh perangkat lunak yang berjalan secara lokal yang meningkatkan produktivitas tanpa perlu mengakses sistem yang lebih besar. Pengenalan hard drive dan floppy disk pada komputer pribadi memungkinkan pengguna untuk menyimpan dan mengambil data secara lokal. Ini menghasilkan workflow berbasis data di mana individu dapat mengontrol informasi mereka sendiri, yang merupakan perubahan signifikan dari ketergantungan pada database terpusat.

PC berkembang untuk menangani tugas-tugas kompleks seperti pemrosesan audio-visual, permainan, dan pembuatan media secara lokal. Ini menjadikan PC alat penting bagi para profesional kreatif, yang meningkatkan kemampuan mereka untuk merancang, mengedit, dan menghasilkan konten langsung di perangkat mereka sendiri. Alat jaringan awal memungkinkan beberapa PC untuk berkomunikasi dalam jaringan area lokal (LAN), tetapi pemrosesan dan penyimpanan tetap dilakukan terutama pada mesin lokal. Ini meningkatkan lingkungan kerja kolaboratif tanpa memerlukan pusat data eksternal.

Kesimpulannya, revolusi PC memungkinkan ruang lingkup untuk komputasi secara lokal dengan memberdayakan pengguna dengan kontrol pribadi atas pemrosesan, penyimpanan, dan aplikasi. Meskipun PC awal memiliki keterbatasan, evolusinya meletakkan dasar untuk komputasi lokal yang independen, dan kemudian, integrasi dengan teknologi cloud.

4. Jaringan PC: Kemunculan Komunikasi Langsung atau Peer-to-Peer

Kemunculan jaringan PC dan komunikasi peer-to-peer (P2P) adalah tonggak penting dalam evolusi teknologi informasi, yang memungkinkan PC untuk berkomunikasi langsung satu sama lain tanpa perlu melalui server pusat atau sistem terpusat. Jaringan PC adalah struktur di mana beberapa komputer pribadi dihubungkan satu sama lain, baik melalui kabel jaringan (seperti Ethernet) atau secara nirkabel (seperti Wi-Fi). Tujuan dari jaringan ini adalah untuk memungkinkan berbagi sumber daya, seperti file, printer, dan akses internet, di antara komputer yang terhubung.

Dalam model P2P, setiap komputer dalam jaringan bertindak sebagai peer yang setara dengan yang lainnya, tidak ada komputer yang berfungsi sebagai server pusat. Setiap peer dapat berfungsi sebagai penyedia dan pengguna layanan, serta dapat berbagi data dan sumber daya secara langsung dengan peers lainnya. Manfaat model P2P yaitu Komunikasi P2P menghilangkan kebutuhan akan server pusat, mengurangi beban pada satu titik dan meningkatkan keandalan jaringan. Jika salah satu peer mengalami masalah, peer lain tetap dapat berfungsi tanpa gangguan besar. Selain itu, Dengan distribusi tugas dan data di antara semua peers, komunikasi P2P dapat mengurangi kemacetan yang sering terjadi pada server pusat. Ini juga memungkinkan transfer data yang lebih cepat dan efisien karena data tidak harus melalui satu server pusat. Jaringan P2P dapat mengurangi biaya infrastruktur dan pemeliharaan, karena tidak memerlukan server pusat yang mahal dan rumit. Peer-peer network biasanya lebih murah untuk diatur dan dipelihara.

Aplikasi komunikasi peer to peer berupa Sistem berbagi file seperti BitTorrent menggunakan model P2P untuk membagi file besar menjadi potongan-potongan kecil yang kemudian dibagikan di antara banyak pengguna. Ini meningkatkan kecepatan unduhan dan mengurangi beban pada server pusat. Aplikasi komunikasi seperti Skype dan WhatsApp menggunakan arsitektur P2P untuk panggilan suara dan video, memungkinkan komunikasi langsung antara pengguna tanpa memerlukan server pusat untuk mengelola data. Teknologi blockchain yang mendasari mata uang kripto seperti Bitcoin juga menggunakan model P2P. Dalam blockchain, setiap node dalam jaringan peer-to-peer berfungsi sebagai pencatat transaksi, memastikan integritas dan transparansi tanpa memerlukan otoritas pusat.

5. Komunikasi Jaringan Cepat: Menyediakan Jalan bagi Komputasi Terdistribusi

Komunikasi jaringan cepat merupakan salah satu faktor kunci yang memfasilitasi perkembangan komputasi terdistribusi. Merujuk pada

kemampuan jaringan untuk mengirimkan data dengan kecepatan tinggi antara komputer dan perangkat lain. Ini mencakup berbagai teknologi jaringan seperti Ethernet berkecepatan tinggi, serat optik, dan koneksi nirkabel berkecepatan tinggi seperti Wi-Fi 6. Komunikasi jaringan yang cepat sangat penting untuk memastikan bahwa data dapat dikirim dan diterima dalam waktu yang sangat singkat. Hal ini mengurangi latensi dan meningkatkan kinerja aplikasi yang memerlukan transfer data besar atau waktu respons yang cepat.

Komputasi terdistribusi adalah model di mana tugas komputasi dibagi di antara beberapa komputer atau node yang terhubung melalui jaringan. Setiap node dalam sistem terdistribusi berkontribusi pada pemrosesan data dan menyelesaikan bagian dari tugas secara bersamaan. Tujuan dari komputasi terdistribusi adalah untuk meningkatkan skalabilitas, kecepatan pemrosesan, dan keandalan. Dengan membagi beban kerja, sistem terdistribusi dapat menangani tugas yang lebih besar dan lebih kompleks daripada sistem yang hanya menggunakan satu komputer.

Jaringan cepat mengurangi latensi atau waktu yang dibutuhkan untuk data melakukan perjalanan antara node dalam sistem terdistribusi. Latensi yang rendah sangat penting dalam komputasi terdistribusi untuk memastikan bahwa node dapat berkomunikasi secara efisien dan sinkron. Dengan kecepatan tinggi, data dapat ditransfer dengan lebih cepat antara node, memungkinkan sistem untuk memproses data lebih cepat dan lebih efisien. Ini meningkatkan kinerja aplikasi yang bergantung pada komputasi terdistribusi, seperti big data analytics, rendering grafis, dan komputasi ilmiah. Komunikasi jaringan yang cepat memungkinkan sistem terdistribusi untuk skala horizontal, yaitu menambah lebih banyak node untuk menangani beban kerja yang lebih besar tanpa mengorbankan kinerja. Ini sangat penting untuk aplikasi yang memerlukan pemrosesan data dalam jumlah besar.

Aplikasi Komputasi Terdistribusi yang Bergantung pada Komunikasi Jaringan Cepat seperti *cloud computing*, *grid computing*, dan *distributed*

database. Layanan cloud computing seperti Amazon Web Services (AWS), Microsoft Azure, dan Google Cloud Platform mengandalkan komunikasi jaringan cepat untuk menyediakan komputasi, penyimpanan, dan layanan berbasis data yang dapat diakses secara global. Jaringan cepat memungkinkan pengguna untuk berinteraksi dengan layanan cloud secara efisien. Grid computing menggabungkan sumber daya komputasi dari berbagai lokasi untuk menyelesaikan tugas-tugas besar. Komunikasi cepat antara node dalam grid sangat penting untuk koordinasi dan sinkronisasi yang efektif. Basis data terdistribusi seperti Apache Cassandra dan Google Bigtable menggunakan jaringan cepat untuk menjaga konsistensi dan ketersediaan data di seluruh node. Kecepatan komunikasi memastikan bahwa data dapat diperbarui dan diakses dengan cepat.

6. Cluster Computing

Cluster computing merupakan model komputasi di mana sejumlah komputer atau node terhubung dalam suatu sistem yang terkoordinasi untuk bekerja bersama sebagai satu unit komputasi yang terintegrasi. Tujuan dari cluster computing adalah untuk meningkatkan kinerja, ketersediaan, dan skalabilitas melalui distribusi beban kerja di antara beberapa komputer. Cluster computing adalah model komputasi di mana sejumlah komputer atau node terhubung dalam suatu sistem yang terkoordinasi untuk bekerja bersama sebagai satu unit komputasi yang terintegrasi. Tujuan dari cluster computing adalah untuk meningkatkan kinerja, ketersediaan, dan skalabilitas melalui distribusi beban kerja di antara beberapa komputer. Komponen utama cluster computing yaitu *node*, *network*, *cluster management software*. Node merupakan komputer individu dalam cluster yang bertindak sebagai unit pemrosesan. Setiap node memiliki CPU, memori, dan penyimpanan lokalnya sendiri. Network merupakan koneksi antara node dalam cluster biasanya menggunakan Ethernet atau InfiniBand untuk memastikan komunikasi yang cepat dan efisien antar node. Cluster Management Software adalah

Perangkat lunak yang mengelola operasi cluster, mengatur distribusi beban kerja, dan memantau kesehatan node. Contoh perangkat lunak ini termasuk Hadoop untuk komputasi terdistribusi dan Slurm untuk manajemen antrian pekerjaan.

Jenis-jenis Cluster Computing yaitu High-Performance Computing, High-Availability, Cluster Komputasi Terdistribusi, dan Cluster Komputasi Grid. Cluster Komputasi Kekuatan Tinggi (High-Performance Computing, HPC): Didesain untuk aplikasi yang memerlukan pemrosesan yang sangat cepat, seperti simulasi ilmiah, permodelan cuaca, dan analisis data besar. Contoh: Superkomputer yang sering digunakan di lembaga penelitian dan universitas. Cluster Komputasi Ketersediaan Tinggi (High-Availability, HA): Didesain untuk memastikan ketersediaan layanan yang terus menerus. Jika salah satu node mengalami kegagalan, node lain dalam cluster dapat mengambil alih tugasnya. Ini umum digunakan dalam server web dan database.

Cluster Komputasi Terdistribusi: Menggunakan node-node yang tersebar di lokasi yang berbeda, sering kali digunakan untuk memanfaatkan sumber daya komputasi yang ada di berbagai lokasi untuk meningkatkan skalabilitas dan redundansi. Cluster Komputasi Grid: Menggabungkan sumber daya dari beberapa komputer dan jaringan untuk mencapai tujuan komputasi yang besar. Ini berbeda dari cluster karena node dalam grid tidak harus berada di lokasi yang sama.

Keuntungan menggunakan cluster computer yaitu Peningkatan Kinerja. Dengan membagi beban kerja di antara banyak node, cluster dapat menyelesaikan tugas komputasi yang kompleks dan berat dengan lebih cepat daripada satu komputer tunggal. Keuntungan lain yaitu dengan menambahkan lebih banyak node ke cluster memungkinkan sistem untuk menangani beban kerja yang lebih besar atau lebih kompleks tanpa perlu merombak sistem yang ada. Dalam cluster HA, kegagalan satu node tidak akan menyebabkan gangguan layanan secara keseluruhan, karena node lain dapat mengambil alih tugasnya, memastikan ketersediaan yang tinggi. ika

satu node gagal, node lain dapat memastikan bahwa proses tetap berjalan, yang meningkatkan ketahanan sistem.

7. Grid Computing

Grid computing merupakan model komputasi yang memungkinkan penggunaan dan pengelolaan sumber daya komputer yang tersebar di berbagai lokasi sebagai satu sistem terkoordinasi. Konsep ini bertujuan untuk memanfaatkan kekuatan komputasi dari banyak komputer atau server yang berada di berbagai tempat, baik di dalam satu organisasi atau tersebar di berbagai lokasi geografis, untuk menyelesaikan tugas-tugas komputasi yang besar dan kompleks. Grid Computing adalah sistem komputasi yang menggabungkan sumber daya komputasi, penyimpanan, dan jaringan dari berbagai komputer atau node yang terhubung untuk menjalankan aplikasi dan menyelesaikan tugas-tugas besar. Ini memungkinkan kolaborasi dan pemanfaatan sumber daya yang tidak berada di satu lokasi fisik.

Komponen utama *grid computing* meliputi sumber daya, *middleware*, jaringan, dan manajemen dan keamanan. Sumber Daya (Resources) merupakan komputer atau node yang terhubung dalam grid, yang menyediakan kapasitas pemrosesan, penyimpanan, dan bandwidth. Setiap node dalam grid dapat berlokasi di berbagai tempat, termasuk di luar batas organisasi.

Middleware merupakan perangkat lunak yang mengelola dan mengkoordinasikan sumber daya di dalam grid. Middleware menyediakan fungsionalitas untuk penjadwalan tugas, komunikasi antar node, dan manajemen sumber daya. Contoh *middleware* grid termasuk Globus Toolkit dan Unicore. Jaringan mencakup Infrastruktur komunikasi yang menghubungkan node-node dalam grid. Jaringan harus mendukung transfer data yang cepat dan andal antara berbagai lokasi. Manajemen dan Keamanan merupakan sistem manajemen dan keamanan untuk memastikan kontrol akses, otentikasi, dan perlindungan data. Manajemen grid memastikan bahwa sumber daya digunakan secara efisien dan aman.

Jenis-jenis Grid Computing: Computational Grid: Fokus pada pemrosesan komputasi, memungkinkan tugas-tugas berat seperti simulasi ilmiah, analisis data besar, dan permodelan matematis untuk dibagi di antara banyak node. Data Grid: Berfokus pada penyimpanan dan pengelolaan data yang besar dan tersebar, memungkinkan akses dan pengolahan data yang terdistribusi di berbagai lokasi. Ini sering digunakan dalam penelitian ilmiah dan analisis data besar. Desktop Grid: Menggunakan komputer pribadi yang berada di luar organisasi atau individu, sering kali dengan bantuan pengguna sukarela. Contoh terkenal adalah SETI@home, yang menggunakan komputer pribadi di seluruh dunia untuk menganalisis sinyal radio dari luar angkasa. Service Grid: Menyediakan layanan berbasis web yang dapat diakses oleh aplikasi dan pengguna dari berbagai lokasi. Ini memanfaatkan infrastruktur grid untuk mendistribusikan layanan dan aplikasi.

Keuntungan Grid Computing: Peningkatan Kinerja: Dengan membagi beban kerja di antara banyak node, grid computing dapat menyelesaikan tugas-tugas komputasi yang besar dan kompleks dengan lebih cepat daripada yang bisa dilakukan oleh satu sistem tunggal. Skalabilitas: Grid computing memungkinkan penambahan lebih banyak node untuk meningkatkan kapasitas komputasi dan penyimpanan sesuai kebutuhan, mendukung pertumbuhan dan peningkatan beban kerja. Pemanfaatan Sumber Daya: Memungkinkan pemanfaatan sumber daya yang tidak terpakai atau idle dari berbagai komputer di berbagai lokasi, meningkatkan efisiensi penggunaan sumber daya. Kolaborasi: Memfasilitasi kolaborasi antara organisasi dan individu dengan berbagi sumber daya komputasi dan data, yang mendukung proyek-proyek besar yang melibatkan berbagai pihak.

8. Utility Computing

Utility computing merupakan model komputasi di mana sumber daya komputasi (seperti pemrosesan, penyimpanan, dan jaringan) disediakan kepada pengguna sebagai layanan sesuai permintaan, mirip dengan utilitas publik seperti listrik atau air. Dalam utility computing, pengguna hanya

membayar untuk sumber daya yang mereka gunakan, dan penyedia layanan bertanggung jawab untuk menyediakan infrastruktur yang dibutuhkan. Utility computing adalah model di mana layanan komputasi diberikan sesuai permintaan kepada pengguna, memungkinkan mereka untuk mengakses sumber daya komputasi sesuai kebutuhan mereka tanpa perlu mengelola infrastruktur sendiri. Pengguna hanya membayar berdasarkan konsumsi layanan, seperti kapasitas pemrosesan atau penyimpanan, sehingga mirip dengan model utilitas seperti listrik atau gas.

Fitur Utama Utility Computing meliputi **pembayaran berdasarkan penggunaan (pay-as-you-go)** yaitu pengguna hanya membayar untuk sumber daya yang mereka gunakan. Tidak ada biaya tetap, sehingga biaya dapat disesuaikan dengan kebutuhan. **Skalabilitas** yaitu sumber daya dapat diukur dan disesuaikan sesuai dengan permintaan. Jika pengguna memerlukan lebih banyak kapasitas, mereka dapat memperolehnya tanpa harus mengelola perangkat keras fisik. **Akses Sesuai Permintaan** yaitu pengguna dapat mengakses sumber daya kapan saja dan dari mana saja, melalui internet atau jaringan privat. **Abstraksi Infrastruktur** yaitu pengguna tidak perlu khawatir tentang detail teknis infrastruktur seperti pengelolaan server, penyimpanan, atau jaringan. Penyedia layanan menangani semua operasi backend.

Komponen Utility Computing yaitu penyedia layanan meliputi organisasi yang menyediakan infrastruktur dan layanan komputasi, seperti Amazon Web Services (AWS), Microsoft Azure, atau Google Cloud. Infrastruktur Virtualisasi berupa teknologi virtualisasi yang digunakan oleh penyedia layanan untuk mengalokasikan sumber daya komputasi kepada pengguna secara dinamis. Platform manajemen seperti perangkat lunak yang mengelola akses pengguna ke sumber daya komputasi, melacak penggunaan, dan menangani penagihan.

Keuntungan Utility Computing yaitu **Efisiensi Biaya**: Karena pengguna hanya membayar untuk sumber daya yang mereka gunakan, ini menghilangkan kebutuhan untuk membeli dan memelihara perangkat keras

sendiri. Biaya operasional menjadi lebih rendah dan dapat diprediksi. **Fleksibilitas dan Skalabilitas:** Pengguna dapat dengan mudah menambah atau mengurangi penggunaan sumber daya sesuai dengan kebutuhan mereka, tanpa perlu mengkhawatirkan keterbatasan infrastruktur fisik. **Akses Global:** Dengan infrastruktur berbasis cloud, pengguna dapat mengakses sumber daya dari berbagai lokasi, yang sangat mendukung operasi bisnis global. **Peningkatan Efisiensi Operasional:** Perusahaan tidak perlu mengelola, memelihara, atau meningkatkan perangkat keras dan perangkat lunak secara manual, karena ini diurus oleh penyedia layanan.

B. Latihan

a. Pilihan Ganda

1. Apa yang menjadi ciri utama dari mainframe architecture?
 - a. Semua pemrosesan dilakukan di perangkat pengguna
 - b. Pemrosesan utama dilakukan di computer sentral yaitu mainframe
 - c. Semua data disimpan di terminal pengguna
 - d. Pemrosesan dilakukan di beberapa computer terdistribusi
 - e. Terminal pengguna memiliki kemampuan pemrosesan sendiri
2. Apa contoh fungsi yang dilakukan oleh ATM sebagai intelligent terminal sebelum berkomunikasi dengan server bank?
 - a. Menjalankan semua pemrosesan secara manual
 - b. Memproses kartu kredit tanpa otorisasi
 - c. Memvalidasi kartu, menghitung saldo, dan berinteraksi dengan pengguna
 - d. Mengelola seluruh jaringan bank
 - e. Menjalankan fungsi server pusat
3. Apa salah satu perubahan penting yang dibawa oleh revolusi PC dalam pengolahan data?
 - a. Pengguna tetap bergabung pada mainframe untuk pemrosesan data
 - b. Pengguna dapat mengendalikan dan mengelola daya mereka secara local
 - c. Semua pemrosesan data dilakukan melalui cloud
 - d. PC menggantikan server dalam menjalankan aplikasi besar
 - e. Data diproses di terminal tanpa control lokal

4. Jenis cluster computing yang dirancang untuk memastikan ketersediaan layanan secara terus menerus disebut?
 - a. High-Performance Computing (HPC)
 - b. High-Availability (HA)
 - c. Cluster Komputasi Grid
 - d. Cluster Komputasi Terdistribusi
 - e. Superkomputer
5. Apa yang dimaksud dengan utility computing
 - a. Model komputasi di mana pengguna membeli perangkat keras sendiri
 - b. Model komputasi dimana sumber daya komputasi disediakan sebagai layanan sesuai permintaan
 - c. Model komputasi di mana pengguna harus mengelola semua infrastruktur
 - d. Model komputasi yang hanya tersedia untuk perusahaan besar
 - e. Model komputasi yang berfokus pada perangkat lunak saja

b. Esai

Jawablah pertanyaan dibawah ini!

1. Arsitektur mainframe menyediakan lapisan keamanan yang kuat, baik dari sisi perangkat keras maupun perangkat lunak. Sistem ini sangat dilindungi dari gangguan luar seperti serangan siber. Jelaskan system keamanan yang dimaksud diatas!.
2. Selain daripada efisiensi pengiriman data. Mengapa Komunikasi Jaringan Cepat sangat penting bagi Komputasi Terdistribusi!
3. Terdapat 4 Jenis-jenis Cluster Computing. Sebutkan dan jelaskan dari keempat jenis tersebut!

BAB III

CLOUD SYSTEM: BENEFIT AND CHALLENGES

TUJUAN PEMBELAJARAN

1. Mahasiswa mampu menjelaskan manfaat dalam penerapan *cloud system* atau *cloud computing*
2. Mahasiswa mampu menjelaskan tantangan dalam penerapan *cloud system* atau *cloud computing*
3. Mahasiswa mampu menganalisis Solusi untuk mengatasi tantangan dalam penerapan *cloud system* atau *cloud computing*

Teknologi *cloud system* atau *cloud computing* memberikan manfaat berupa model layanan utilitas bagi pengguna komputasi. Pengguna yang tidak dapat mengadakan infrastrukturnya sendiri dapat menggunakan layanan komputasi yang disediakan oleh pihak ketiga melalui jaringan internet. Pengguna dapat menggunakan layanan tersebut dengan system berlangganan sesuai dengan penggunaan dan dapat diakses dimana saja dan kapan saja. Bab ini akan membahas mengenai manfaat-manfaat yang diberikan oleh layanan *cloud system* atau *cloud computing*.

Selain manfaat yang diberikan oleh layanan *cloud system* atau *cloud computing*, terdapat tantangan besar dalam penerapannya. Tantangan terbesarnya adalah terkait isu keamanan dan kepatuhan data. Tantangan lainnya adalah vendor cenderung mengembangkan teknologi cloudnya masing-masing tanpa memiliki standar teknologi. Beberapa hal tersebut menjadi tantangan dalam penerapan layanan *cloud system* atau *cloud computing*. Meskipun telah dilakukan beberapa perbaikan untuk mengatasi hal tersebut tetapi masih menjadi hal yang menarik untuk didiskusikan dan pada bab ini kita akan membahas mengenai hal tersebut. Bab ini juga akan menjelaskan mengenai solusi-solusi untuk mengatasi tantangan dalam implementasi layanan *cloud system* atau *cloud computing*.

A. Inisiator Awal Cloud System

J.C.R. Licklider (1960-an): Licklider adalah seorang ilmuwan komputer yang dikenal karena visinya tentang "jaringan galaksi". Dia membayangkan sebuah

dunia di mana komputer dapat berkomunikasi satu sama lain dan berbagi informasi secara global. Meskipun ide ini tidak secara langsung sama dengan *cloud computing* modern, konsep berbagi sumber daya dan komunikasi jarak jauh adalah fondasi awalnya.

John McCarthy (1960-an): McCarthy, seorang pionir dalam ilmu komputer, mengusulkan bahwa komputasi suatu hari nanti akan menjadi layanan utilitas, mirip dengan listrik atau air. Ide ini juga merupakan salah satu pijakan awal untuk perkembangan *cloud computing*.

IBM (1970-an): IBM mengembangkan teknologi virtualisasi pada mainframe mereka. Konsep ini memungkinkan beberapa sistem operasi untuk berjalan pada satu mesin fisik secara bersamaan, menciptakan lingkungan virtual yang independen. Teknologi ini adalah dasar dari banyak prinsip *cloud computing* seperti pembagian sumber daya dan isolasi. Virtualisasi IBM adalah salah satu tonggak penting dalam sejarah teknologi komputasi, memberikan dasar bagi banyak konsep modern dalam *cloud computing*. Virtualisasi IBM telah berkembang dari konsep awal tentang manajemen sumber daya ke solusi canggih yang mendukung berbagai model komputasi modern, termasuk *cloud computing* dan kontainerisasi. Dari sistem mainframe awal hingga platform *cloud* saat ini, inovasi IBM dalam virtualisasi telah memainkan peran penting dalam membentuk cara kita mengelola dan menggunakan sumber daya komputasi.

Inisiator awal dalam penerapan *cloud system* atau *cloud computing* adalah Salesforce. Salesforce adalah salah satu pelopor dalam adopsi dan pengembangan teknologi *cloud computing*. Salesforce didirikan pada tahun 1999 oleh **Marc Benioff**, seorang mantan eksekutif dari Oracle. Benioff, bersama dengan rekan-rekannya, menciptakan Salesforce dengan visi untuk mengubah cara perusahaan mengelola hubungan pelanggan (CRM) melalui model berbasis *cloud*. Marc Benioff melihat potensi untuk menyediakan aplikasi CRM sebagai layanan yang diakses melalui web, bukan diinstal di server lokal perusahaan. Ini bertentangan dengan model perangkat lunak tradisional, yang sering kali memerlukan perangkat keras khusus dan instalasi yang rumit.

Salesforce meluncurkan layanan CRM berbasis web pertama mereka pada tahun 1999. Ini adalah salah satu contoh awal dari model *Software as a Service* (SaaS), yang memungkinkan pengguna untuk mengakses perangkat lunak melalui internet tanpa harus mengelolanya secara lokal. Salesforce memperkenalkan model berlangganan, yang memungkinkan perusahaan untuk membayar untuk layanan perangkat lunak dengan biaya tetap bulanan atau tahunan, mengurangi kebutuhan untuk investasi awal yang besar dan perawatan perangkat lunak.

Salesforce telah memainkan peran kunci dalam mempopulerkan dan mengembangkan model cloud computing, khususnya dalam konteks *Software as a Service* (SaaS). Dengan inovasi produk berkelanjutan, akuisisi strategis, dan fokus pada pelanggan, Salesforce telah menetapkan standar tinggi dalam industri CRM dan cloud computing secara umum. Sejak diluncurkan pada tahun 1999, Salesforce telah menjadi salah satu pelopor utama dalam mengubah cara perusahaan mengelola hubungan pelanggan dan menggunakan teknologi cloud.

Perkembangan infrastruktur cloud hingga diposisi saat ini tidak lepas dari pengaruh beberapa perusahaan besar seperti Amazon, Google, dan Microsoft. Amazon Web Services (AWS) adalah salah satu penyedia layanan cloud computing terkemuka di dunia. Pada awal 2000-an, Amazon, yang awalnya dikenal sebagai perusahaan e-commerce, menghadapi tantangan dalam mengelola infrastruktur TI mereka sendiri untuk mendukung pertumbuhan bisnisnya. Tim TI Amazon mengembangkan solusi internal untuk memenuhi kebutuhan infrastruktur mereka, yang akhirnya mengarah pada konsep penyediaan layanan infrastruktur sebagai layanan (*Infrastructure as a Service/IaaS*).

Amazon meluncurkan AWS secara resmi pada Maret 2006. AWS dimulai dengan layanan Amazon Elastic Compute Cloud (EC2) dan Amazon Simple Storage Service (S3). Ini menandai awal dari model cloud computing publik dan layanan berbasis pemakaian yang memungkinkan pelanggan untuk menyewa kapasitas komputasi dan penyimpanan berdasarkan kebutuhannya. Amazon EC2 merupakan layanan menyediakan kapasitas komputasi elastis yang dapat diskalakan, memungkinkan pengguna untuk menyewa server virtual (dikenal

sebagai instance) dan menjalankan aplikasi di cloud tanpa harus membeli dan mengelola perangkat keras fisik sendiri. Amazon S3 merupakan layanan penyimpanan berbasis objek ini menawarkan penyimpanan data yang skalabel dan tahan lama, memungkinkan pengguna untuk menyimpan dan mengambil data kapan saja dari web.

Teknologi cloud computing adalah hasil dari evolusi bertahap yang melibatkan berbagai inovasi dalam virtualisasi, model layanan, dan infrastruktur. Konsep-konsep awal dari para pionir seperti J.C.R. Licklider dan John McCarthy, teknologi virtualisasi dari IBM, serta penerapan praktis oleh perusahaan seperti Salesforce, AWS, Google, dan Microsoft, semuanya berkontribusi pada pengembangan cloud computing yang kita kenal hari ini.

B. Manfaat Cloud System

Sistem *cloud computing* menawarkan berbagai manfaat yang dapat meningkatkan efisiensi, fleksibilitas, dan skalabilitas bagi organisasi dari berbagai ukuran. Berikut adalah beberapa manfaat utama dari sistem *cloud*:

1. Skalabilitas dan Elastisitas
 - a. Skalabilitas On-Demand: Cloud computing memungkinkan pengguna untuk dengan mudah meningkatkan atau mengurangi kapasitas sumber daya sesuai kebutuhan. Ini berarti Anda dapat menambah kapasitas server atau penyimpanan dengan cepat saat permintaan meningkat, dan mengurangnya saat beban menurun.
 - b. Elastisitas: Dengan cloud computing, Anda hanya membayar untuk sumber daya yang Anda gunakan. Ini membantu menghindari investasi besar di infrastruktur yang mungkin tidak digunakan secara maksimal, dan memungkinkan penyesuaian cepat terhadap perubahan permintaan.
2. Pengurangan Biaya
 - a. Model Pembayaran Pay-as-You-Go: Banyak layanan cloud mengadopsi model pembayaran pay-as-you-go, yang memungkinkan Anda membayar hanya untuk sumber daya yang Anda gunakan. Ini dapat mengurangi biaya awal dan biaya tetap yang biasanya terkait dengan infrastruktur TI tradisional.

- b. Pengurangan Biaya Infrastruktur: Dengan cloud computing, Anda tidak perlu membeli, mengelola, atau memelihara perangkat keras dan perangkat lunak secara fisik. Ini mengurangi biaya modal dan operasional terkait dengan infrastruktur TI.
3. Akses dan Fleksibilitas
- a. Akses Global: Layanan cloud dapat diakses dari mana saja di dunia dengan koneksi internet. Ini memungkinkan pekerja untuk bekerja dari jarak jauh dan tim untuk berkolaborasi secara efektif tanpa batasan lokasi.
 - b. Fleksibilitas dalam Pengembangan dan Implementasi: Cloud computing memungkinkan pengembang untuk menguji, mengembangkan, dan meluncurkan aplikasi lebih cepat dan dengan lebih sedikit batasan dibandingkan dengan infrastruktur tradisional.
4. Keandalan dan Ketersediaan
- a. Cadangan dan Pemulihan Bencana: Banyak penyedia cloud menawarkan solusi cadangan dan pemulihan bencana yang otomatis dan terintegrasi. Ini membantu memastikan data Anda aman dan dapat dipulihkan jika terjadi kegagalan sistem atau bencana.
 - b. Uptime Tinggi: Penyedia cloud biasanya menawarkan tingkat ketersediaan yang sangat tinggi dengan SLA (Service Level Agreements) yang menetapkan jaminan uptime, sering kali mencapai 99,9% atau lebih.
5. Keamanan dan Kepatuhan
- a. Keamanan Data: Penyedia cloud sering kali memiliki tim keamanan yang berdedikasi dan teknologi canggih untuk melindungi data pelanggan. Mereka juga menerapkan kontrol akses, enkripsi, dan audit untuk menjaga data tetap aman.
 - b. Kepatuhan dan Sertifikasi: Banyak penyedia cloud mematuhi standar dan sertifikasi industri, seperti ISO 27001, GDPR, dan HIPAA, yang membantu organisasi memenuhi persyaratan kepatuhan yang relevan.
6. Inovasi dan Integrasi

- a. Inovasi Teknologi: Penyedia cloud sering memperkenalkan fitur dan teknologi baru, seperti kecerdasan buatan (AI), pembelajaran mesin (ML), analitik data besar, dan Internet of Things (IoT), yang dapat diakses dengan mudah oleh pelanggan.
 - b. Integrasi dan Ekosistem: Cloud computing memungkinkan integrasi mudah dengan berbagai aplikasi dan layanan, baik yang disediakan oleh penyedia cloud itu sendiri maupun oleh pihak ketiga, melalui API dan platform marketplace.
7. Pengelolaan dan Otomatisasi
- a. Manajemen Sederhana: Layanan cloud sering menyediakan alat manajemen yang intuitif untuk memantau dan mengelola sumber daya TI, sehingga mengurangi beban administrasi.
 - b. Otomatisasi: Banyak layanan cloud menawarkan otomatisasi tugas rutin, seperti pembaruan perangkat lunak, patch keamanan, dan pemantauan, sehingga memungkinkan tim TI untuk fokus pada tugas strategis lainnya.
8. Skalabilitas Global dan Performa
- a. Skalabilitas Global: Penyedia cloud memiliki pusat data di berbagai lokasi di seluruh dunia, yang memungkinkan Anda untuk menempatkan aplikasi dan data lebih dekat dengan pengguna akhir, mengurangi latensi dan meningkatkan performa aplikasi.
 - b. Performansi yang Ditingkatkan: Dengan akses ke infrastruktur kelas dunia dan teknologi terbaru, cloud computing dapat menyediakan performa yang lebih baik dibandingkan dengan perangkat keras lokal yang lebih lama atau tidak dikelola dengan baik.

Cloud computing menawarkan banyak manfaat yang membantu organisasi meningkatkan efisiensi operasional, mengurangi biaya, dan mempercepat inovasi. Dengan skalabilitas, fleksibilitas, dan akses global yang kuat, *cloud computing* memungkinkan organisasi untuk beradaptasi dengan cepat terhadap perubahan pasar, memenuhi kebutuhan pelanggan dengan lebih baik, dan memanfaatkan teknologi terbaru tanpa beban pengelolaan infrastruktur yang berat.

C. Tantangan Cloud System

Meskipun *cloud computing* menawarkan banyak manfaat, ada juga sejumlah tantangan yang dapat dihadapi oleh organisasi ketika mengadopsi dan mengelola sistem cloud. Berikut adalah beberapa tantangan utama dalam *cloud computing*:

1. Keamanan dan Privasi

- a. Data Breaches: Mengandalkan penyedia cloud untuk mengamankan data dapat menjadi risiko jika penyedia tidak memiliki kontrol keamanan yang memadai. Kebocoran data atau pelanggaran dapat terjadi jika langkah-langkah keamanan tidak memadai.
- b. Kepatuhan dan Regulasi: Menyimpan data di cloud dapat menimbulkan tantangan terkait kepatuhan dengan berbagai regulasi dan standar privasi, seperti GDPR (General Data Protection Regulation) atau HIPAA (Health Insurance Portability and Accountability Act). Memastikan bahwa data disimpan dan dikelola sesuai dengan persyaratan hukum yang berlaku adalah hal yang penting.

2. Kinerja dan Latensi

- a. Kinerja Aplikasi: Kinerja aplikasi dapat dipengaruhi oleh latency jaringan dan koneksi internet. Akses ke data dan aplikasi di cloud bisa lebih lambat dibandingkan dengan infrastruktur lokal jika koneksi internet tidak optimal.
- b. Skalabilitas dan Kontrol: Meskipun cloud menawarkan skalabilitas, ada kalanya pengaturan dan kontrol skalabilitas mungkin tidak sepenuhnya di tangan pengguna. Pengaturan yang tidak tepat bisa menyebabkan masalah performa.

3. Manajemen dan Pengelolaan

- a. Kompleksitas Pengelolaan: Mengelola layanan cloud yang terdistribusi di berbagai wilayah dan penyedia dapat menjadi kompleks. Pengelolaan yang tidak efisien dapat mengakibatkan masalah dalam integrasi dan koordinasi layanan.
- b. Biaya Tak Terduga: Meskipun model pay-as-you-go mengurangi biaya awal, biaya bisa meningkat jika sumber daya tidak dikelola dengan baik.

Penggunaan yang tidak efisien atau tidak terkelola dapat menyebabkan tagihan yang lebih tinggi dari yang diantisipasi.

4. Downtime dan Ketergantungan pada Penyedia

- a. Downtime: Meskipun banyak penyedia cloud menawarkan tingkat ketersediaan tinggi, downtime atau gangguan layanan dapat terjadi. Ketergantungan pada penyedia cloud untuk ketersediaan layanan memerlukan perencanaan pemulihan dan strategi mitigasi risiko.
- b. Ketergantungan pada Penyedia: Bergantung pada satu penyedia cloud dapat menimbulkan risiko jika penyedia mengalami masalah atau berubah kebijakan. Mempertimbangkan strategi multi-cloud atau hibrida bisa membantu mengurangi risiko ketergantungan.

5. Kepatuhan dan Data Sovereignty

- a. Data Sovereignty: Data yang disimpan di cloud dapat berada di server yang berada di negara yang berbeda, yang dapat menimbulkan masalah hukum terkait dengan hukum dan regulasi lokal tentang data.
- b. Kepatuhan Regulasi: Menjaga kepatuhan terhadap regulasi industri dan peraturan data saat menggunakan layanan cloud, terutama ketika data di-host di berbagai lokasi geografis, memerlukan perhatian khusus dan sering kali pengawasan tambahan.

6. Integrasi dan Migrasi

- a. Integrasi Aplikasi: Mengintegrasikan aplikasi dan sistem lokal dengan layanan cloud bisa menjadi kompleks. Tidak semua aplikasi dan sistem kompatibel secara langsung dengan layanan cloud, memerlukan solusi atau middleware tambahan.
- b. Migrasi Data: Proses migrasi data dari sistem lokal ke cloud bisa menjadi rumit dan memerlukan waktu. Selain itu, migrasi juga dapat melibatkan risiko kehilangan data atau ketidakcocokan data.

7. Ketersediaan Konektivitas

- Ketergantungan pada Koneksi Internet: Cloud computing sangat bergantung pada konektivitas internet. Di lokasi dengan konektivitas

internet yang tidak stabil atau terbatas, akses ke layanan cloud dapat terhambat.

- Bandwith dan Latensi: Untuk aplikasi yang memerlukan bandwidth tinggi atau latensi rendah, konektivitas internet yang tidak memadai dapat mempengaruhi performa aplikasi secara signifikan.

8. Kompetensi dan Pelatihan

- Kekurangan Keterampilan: Kebutuhan untuk keterampilan khusus dalam mengelola dan mengoptimalkan layanan cloud dapat menjadi tantangan. Keterampilan baru mungkin diperlukan untuk memanfaatkan fitur dan kapabilitas cloud secara efektif.
- Pelatihan dan Adopsi: Karyawan dan tim TI perlu dilatih untuk memahami dan menggunakan platform cloud secara efektif. Proses pelatihan dapat memerlukan waktu dan sumber daya.

Meskipun *cloud computing* menawarkan banyak keuntungan, tantangan-tantangan ini memerlukan perhatian dan perencanaan yang cermat. Organisasi harus mempertimbangkan faktor-faktor ini dan mengembangkan strategi yang sesuai untuk mengatasi risiko dan memaksimalkan manfaat dari adopsi *cloud computing*. Dengan pendekatan yang hati-hati dan pengelolaan yang baik, banyak dari tantangan ini dapat dikelola dan mitigasi dengan efektif.

D. Solusi mengatasi tantangan *Cloud System*

Mengatasi tantangan dalam sistem *cloud computing* memerlukan pendekatan strategis dan solusi teknologi yang tepat. Berikut adalah beberapa cara untuk mengatasi tantangan umum dalam *cloud computing*:

1. Keamanan dan Privasi

- a. Penerapan Kebijakan Keamanan yang Ketat: Implementasikan kebijakan keamanan yang kuat, termasuk kontrol akses berbasis peran, autentikasi multi-faktor (MFA), dan enkripsi data baik saat transit maupun saat disimpan.
- b. Audit dan Pemantauan: Gunakan alat pemantauan dan log untuk mengawasi aktivitas yang mencurigakan dan memastikan kepatuhan

- terhadap kebijakan keamanan. Lakukan audit keamanan secara berkala untuk mengidentifikasi dan mengatasi potensi kelemahan.
- c. **Pemahaman dan Kepatuhan:** Pastikan bahwa penyedia cloud mematuhi standar dan regulasi keamanan yang relevan, seperti GDPR atau HIPAA. Gunakan fitur kepatuhan dan keamanan yang disediakan oleh penyedia cloud, seperti enkripsi dan pelaporan.
2. **Kinerja dan Latensi**
 - a. **Optimisasi Jaringan:** Gunakan Content Delivery Networks (CDNs) dan solusi caching untuk mengurangi latensi dan meningkatkan kecepatan akses data. Pilih pusat data yang dekat dengan lokasi pengguna untuk mengurangi latensi.
 - b. **Pemantauan Kinerja:** Implementasikan alat pemantauan kinerja untuk melacak dan menganalisis penggunaan sumber daya. Ini memungkinkan Anda untuk mengidentifikasi dan menangani masalah kinerja dengan cepat.
 - c. **Pengelolaan Beban Kerja:** Sesuaikan konfigurasi sumber daya untuk memastikan bahwa aplikasi dan layanan memiliki kapasitas yang memadai untuk menangani beban kerja yang bervariasi.
 3. **Manajemen dan Pengelolaan**
 - a. **Pengelolaan Sumber Daya yang Efisien:** Gunakan alat manajemen cloud untuk memantau penggunaan dan biaya sumber daya secara real-time. Implementasikan praktik terbaik dalam pengelolaan tagihan dan alokasi sumber daya.
 - b. **Automatisasi dan Orkestrasi:** Manfaatkan otomatisasi untuk tugas-tugas rutin, seperti pemantauan, pemeliharaan, dan skala otomatis, untuk mengurangi beban administrasi dan meningkatkan efisiensi.
 - c. **Pelatihan dan Keterampilan:** Investasikan dalam pelatihan dan pengembangan keterampilan untuk tim TI Anda, sehingga mereka dapat mengelola dan mengoptimalkan lingkungan cloud dengan efektif.
 4. **Downtime dan Ketergantungan pada Penyedia**

- a. Rencana Pemulihan Bencana: Buat dan uji rencana pemulihan bencana yang mencakup strategi cadangan dan pemulihan data. Gunakan layanan cadangan otomatis yang disediakan oleh penyedia cloud.
 - b. Diversifikasi Penyedia: Pertimbangkan untuk menggunakan beberapa penyedia cloud (multi-cloud) untuk mengurangi risiko ketergantungan pada satu penyedia dan meningkatkan ketersediaan layanan.
 - c. Perjanjian Layanan (SLA): Tinjau dan negosiasikan SLA dengan penyedia cloud untuk memastikan bahwa mereka memenuhi standar ketersediaan dan performa yang dibutuhkan oleh organisasi Anda.
5. Kepatuhan dan Data Sovereignty
- a. Pengelolaan Data dan Lokasi: Pilih penyedia cloud yang memungkinkan Anda mengontrol lokasi penyimpanan data dan memastikan bahwa data dikelola sesuai dengan peraturan lokal dan internasional.
 - b. Kepatuhan dan Audit: Gunakan alat kepatuhan yang disediakan oleh penyedia cloud untuk memantau dan memastikan bahwa data dan proses Anda mematuhi regulasi yang berlaku. Lakukan audit kepatuhan secara teratur.
6. Integrasi dan Migrasi
- a. Strategi Migrasi yang Terencana: Kembangkan rencana migrasi yang terperinci untuk memindahkan data dan aplikasi ke cloud. Ini termasuk evaluasi aplikasi, pemetaan dependensi, dan uji coba sebelum migrasi penuh.
 - b. Tool Integrasi: Gunakan alat dan platform integrasi yang mendukung penghubungan aplikasi dan data antara lingkungan lokal dan cloud, serta antar layanan cloud.
 - c. Uji Coba dan Validasi: Lakukan uji coba dan validasi untuk memastikan bahwa aplikasi dan data berfungsi dengan baik setelah migrasi dan integrasi.
7. Ketersediaan Konektivitas

- a. Cadangan Koneksi Internet: Implementasikan koneksi internet cadangan atau solusi failover untuk mengurangi risiko gangguan layanan akibat masalah konektivitas.
 - b. Optimisasi Bandwidth: Manfaatkan teknik kompresi data dan pengelolaan bandwidth untuk memaksimalkan performa dan mengurangi dampak dari keterbatasan bandwidth.
8. Kompetensi dan Pelatihan
- a. Pelatihan Berkelanjutan: Berikan pelatihan berkelanjutan untuk staf TI mengenai teknologi cloud terbaru, praktik terbaik, dan alat yang tersedia.
 - b. Sumber Daya dan Dukungan: Manfaatkan sumber daya dan dukungan dari penyedia cloud, termasuk dokumentasi, forum komunitas, dan layanan dukungan pelanggan.

Mengatasi tantangan dalam cloud computing memerlukan pendekatan yang terencana dan komprehensif. Dengan menerapkan langkah-langkah keamanan yang kuat, mengelola kinerja dan biaya dengan bijaksana, serta mengembangkan keterampilan dan pengetahuan tim TI, organisasi dapat memaksimalkan manfaat dari teknologi cloud sambil mengurangi risiko dan masalah yang mungkin timbul. Pendekatan proaktif dan pengelolaan yang baik adalah kunci untuk sukses dalam mengadopsi dan memanfaatkan solusi cloud.

E. Latihan

a. Pilihan Ganda

1. Apa inovasi penting yang dikembangkan oleh IBM pada tahun 197—an yang berkontribusi pada kemajuan cloud computing
 - a. Jaringan galaksi
 - b. Teknologi virtualisasi pada mainframe
 - c. Layanan software as a service (SaaS)
 - d. Amazon web services (AWS)
 - e. Model CRM berbasis cloud
2. Apa model layanan cloud computing yang diperkenalkan oleh Salesforce dengan menyediakan perangkat lunak sebagai layanan melalui internet?
 - a. Platform as a Service (PaaS)

- b. Infrastructure as a Service (IaaS)
 - c. Database as a Service (DaaS)
 - d. Software as a Service (SaaS)
 - e. Network as a Service (NaaS)
3. Apa keuntungan utama dari fitur cadangan dan pemulihan bencana yang ditawarkan oleh penyedia cloud?
- a. Menyimpan semua data di lokasi terpisah
 - b. Membuat Salinan cadangan manual secara regular
 - c. Mengamankan data secara otomatis dan memulihkan data jika terjadi bencana
 - d. Menyediakan proteksi data tanpa perlu enkripsi
 - e. Mencegah downtime yang disebabkan oleh bencana alam
4. Apa tantangan utama yang dihadapi organisasi dalam manajemen dan pengelolaan layanan cloud?
- a. Kecepatan akses internet
 - b. Kompleksitas pengelolaan layanan cloud yang terdistribusi
 - c. Jumlah pengguna yang mengakses cloud
 - d. Memilih penyedia cloud yang tepat
 - e. Tidak ada tantangan sama sekali
5. Apa yang menjadi langkah pertama untuk mengatasi tantangan keamanan dan privasi dalam cloud computing?
- a. Audit dan pemantauan
 - b. Penerapan kebijakan keamanan yang ketat
 - c. Pengurangan biaya
 - d. Pelatihan karyawan
 - e. Penggunaan CDN

b. Esai

Jawablah pertanyaan dibawah ini!

1. *Teknologi Cloud system atau Cloud computing* banyak digunakan oleh organisasi atau perusahaan. Jelaskan apa dan mengapa teknologi ini menjadi primadona bagi perusahaan atau organisasi!

2. Dari banyaknya tantangan dalam *cloud computing*. Menurut kamu tantangan apa yang paling berpengaruh jika system tersebut digunakan oleh perusahaan bisnis!
3. Selain dari pada tantangan cloud computing yang menjadi aspek untuk berhati-hati, terdapat beberapa solusi untuk mengatasi tantangan tersebut. Jika sebuah perusahaan atau organisasi mengutamakan manajemen dan pengelolaan. Jelaskan aspek apa yang harus diperhatikan perusahaan tersebut!

BAB IV

CLOUD SYSTEM: BASIC NETWORK

TUJUAN PEMBELAJARAN

1. Mahasiswa mampu menjelaskan konsep jaringan dan jaringan komputer?
2. Mahasiswa mampu menjelaskan jenis jaringan komputer dan topologi jaringan komputer?
3. Mahasiswa mampu menjelaskan jaringan *cloud computing*?

Jaringan komputer dan *cloud computing* saling melengkapi. Bayangkan *cloud computing* sebagai sebuah lautan data yang luas dan tak terbatas. Untuk mengakses lautan data ini, kita membutuhkan sebuah perahu atau kapal, dan perahu atau kapal ini adalah jaringan komputer. Jaringan komputer memungkinkan perangkat kita (komputer, ponsel, tablet) terhubung ke internet, yang menjadi pintu gerbang menuju layanan *cloud*. Tanpa jaringan, kita tidak akan bisa mengakses data, aplikasi, atau layanan yang berada di *cloud*. Jaringan komputer menyediakan infrastruktur yang memungkinkan kita mengakses dan memanfaatkan layanan *cloud*. Sementara itu, *cloud computing* memberikan fleksibilitas, skalabilitas, dan kemudahan akses yang tidak dapat diberikan oleh sistem komputasi tradisional. Pada bab ini kita akan membahas mengenai dasar jaringan komputer agar memberikan gambaran kepada pembaca mengenai pentingnya jaringan komputer dalam implementasi *cloud system*.

A. Jaringan dan Jaringan Komputer

Jaringan secara umum dapat didefinisikan sebagai kumpulan dari titik-titik atau entitas yang saling terhubung untuk berbagi informasi, sumber daya, atau energi. Jaringan ada di berbagai aspek kehidupan, mulai dari jaringan sosial, listrik, hingga transportasi. Dalam konteks komputer, jaringan berperan dalam menghubungkan perangkat satu dengan yang lainnya untuk komunikasi data, berbagi perangkat keras, atau layanan. Jaringan adalah interkoneksi atau hubungan antara beberapa elemen atau komponen yang membentuk suatu sistem. Elemen-elemen ini bisa berupa benda fisik, konsep abstrak, atau keduanya. Tujuan dari

jaringan adalah untuk memungkinkan terjadinya pertukaran informasi, sumber daya, atau pengaruh antara elemen-elemen tersebut.

Jaringan, baik itu jaringan komputer, sosial, atau jenis jaringan lainnya, memiliki beberapa karakteristik utama yang membedakannya dari sistem yang terisolasi. Berikut adalah beberapa karakteristik tersebut:

1. **Interkoneksi:** Elemen-elemen dalam jaringan saling terhubung satu sama lain melalui tautan atau saluran komunikasi. Hubungan ini terbentuk melalui berbagai media, seperti kabel, sinyal radio, atau bahkan hubungan sosial. Struktur interkoneksi ini membentuk pola tertentu, seperti star, bus, ring, atau mesh.
2. **Tujuan bersama:** Jaringan dibentuk untuk mencapai tujuan tertentu, seperti berbagi informasi, mengkoordinasikan aktivitas, atau meningkatkan efisiensi. Jaringan dibangun dengan tujuan spesifik, misalnya untuk berbagi informasi, mengkoordinasikan aktivitas, atau mencapai tujuan bersama. Elemen-elemen dalam jaringan bekerja sama untuk mencapai tujuan yang lebih besar daripada jika mereka bekerja sendiri-sendiri.
3. **Struktur:** Jaringan memiliki struktur tertentu, yang dapat berupa hierarkis, peer-to-peer, atau kombinasi keduanya. Beberapa jaringan memiliki struktur hierarkis, di mana ada elemen pusat yang mengontrol elemen lainnya. Jaringan lain memiliki struktur yang lebih datar, di mana semua elemen memiliki status yang sama. Struktur jaringan dapat berubah seiring waktu, tergantung pada kebutuhan dan kondisi.
4. **Dinamika:** Jaringan bersifat dinamis, artinya struktur dan hubungan antar elemen dapat berubah seiring waktu. Jaringan bersifat dinamis, artinya struktur, hubungan, dan perilaku elemen-elemen di dalamnya dapat berubah seiring waktu. Jaringan mampu beradaptasi dengan perubahan lingkungan dan kondisi.

Memahami karakteristik jaringan sangat penting untuk merancang jaringan yang efektif dengan memahami karakteristik jaringan, kita dapat merancang jaringan yang sesuai dengan kebutuhan dan tujuan. Mengelola jaringan berupa pemahaman terhadap karakteristik jaringan membantu dalam memecahkan

masalah dan mengoptimalkan kinerja jaringan. Mengelola keamanan jaringan dengan memahami bagaimana jaringan bekerja, kita dapat menerapkan langkah-langkah keamanan yang tepat untuk melindungi jaringan dari ancaman.

Jaringan komputer adalah sistem yang terdiri dari dua atau lebih perangkat komputer yang saling terhubung melalui media komunikasi sehingga memungkinkan transfer data atau berbagi sumber daya, seperti perangkat keras (printer, scanner), perangkat lunak, maupun file data. Tujuan dari jaringan komputer adalah untuk memungkinkan komunikasi yang efisien dan berbagi sumber daya secara lebih optimal.

Untuk memahami jaringan komputer secara mendalam, kita perlu mengetahui komponen utama yang membentuk sebuah jaringan komputer.

1. Perangkat Keras (*Hardware*)

- a. Komputer/Klien: Perangkat utama yang berpartisipasi dalam jaringan.
- b. Server: Komputer yang menyediakan layanan atau sumber daya ke perangkat lain dalam jaringan.
- c. Router: Perangkat yang menghubungkan beberapa jaringan berbeda dan mengarahkan lalu lintas data antar jaringan tersebut.
- d. Switch: Menghubungkan perangkat dalam jaringan lokal dan mendistribusikan data antar perangkat.
- e. Modem: Mengubah sinyal digital menjadi analog untuk transmisi data melalui jaringan telekomunikasi.
- f. NIC (*Network Interface Card*): Perangkat yang memungkinkan komputer untuk terhubung ke jaringan.

2. Perangkat Lunak (*Software*)

- a. Sistem Operasi Jaringan: Sistem operasi yang mendukung komunikasi antar perangkat di jaringan, misalnya Windows Server atau Linux.
- b. Protokol Jaringan: Kumpulan aturan yang mengatur komunikasi antar perangkat di jaringan, seperti TCP/IP (*Transmission Control Protocol/Internet Protocol*).

B. Jenis-Jenis Jaringan Komputer

Jaringan komputer dikelompokkan berdasarkan skala, area geografis yang dicakup, dan tujuan pembentukannya. Berikut ini adalah jenis-jenis jaringan komputer:

1. LAN (*Local Area Network*)

LAN adalah jaringan komputer yang mencakup area geografis kecil, seperti dalam satu gedung, rumah, atau sekolah. LAN sering digunakan untuk berbagi sumber daya internal seperti file dan printer. LAN memungkinkan komputer dan perangkat lain seperti printer, server, dan perangkat penyimpanan terhubung satu sama lain untuk berbagi data, sumber daya, dan layanan seperti internet. LAN adalah jenis jaringan yang paling umum digunakan, terutama untuk penggunaan internal di perusahaan, sekolah, atau rumah. Dengan LAN, perangkat-perangkat dalam jaringan bisa saling berkomunikasi secara cepat dan efisien tanpa perlu bergantung pada koneksi internet eksternal.

LAN digunakan untuk berbagai tujuan, termasuk:

- a. Berbagi Sumber Daya: Pengguna dapat berbagi printer, penyimpanan jaringan, atau perangkat lunak yang diakses oleh beberapa komputer.
- b. Akses Internet Terpusat: Dalam sebuah LAN, beberapa komputer dapat berbagi satu koneksi internet yang sama.
- c. File Sharing: Pengguna dapat dengan mudah berbagi file dan folder antar komputer di jaringan.
- d. Komunikasi Internal: LAN memungkinkan pengguna berkomunikasi secara instan, seperti melalui email, pesan instan, atau sistem kolaborasi perusahaan.
- e. Keamanan Data: Administrator jaringan dapat mengontrol akses pengguna, mengatur hak istimewa, serta mengelola keamanan jaringan untuk melindungi informasi sensitif.

Untuk memahami LAN dengan lebih baik, mari kita lihat komponen-komponen yang membentuk jaringan ini:

- a. Komputer/Host: Perangkat utama yang terhubung dalam jaringan. Ini bisa berupa komputer desktop, laptop, atau perangkat mobile.
- b. Switch: Perangkat keras yang menghubungkan beberapa perangkat dalam jaringan lokal. Switch berfungsi untuk menerima paket data dan meneruskannya ke perangkat yang dituju, sehingga tidak terjadi tabrakan data.
- c. Router: Jika LAN ingin terhubung dengan jaringan lain (misalnya, internet), router diperlukan untuk menghubungkan LAN dengan WAN (Wide Area Network).
- d. Access Point: Jika menggunakan teknologi nirkabel (Wi-Fi), Access Point dibutuhkan untuk memungkinkan perangkat terhubung secara wireless ke LAN.
- e. Media Transmisi: Media fisik yang digunakan untuk mentransfer data, seperti kabel Ethernet (Cat5e, Cat6) atau sinyal radio dalam jaringan Wi-Fi.
- f. Server: Dalam beberapa konfigurasi LAN, server bertindak sebagai penyedia layanan seperti penyimpanan data, aplikasi, atau pengelolaan database.
- g. NIC (Network Interface Card): Setiap perangkat dalam LAN membutuhkan NIC untuk berkomunikasi melalui jaringan. Kartu jaringan ini bisa terintegrasi atau dalam bentuk tambahan.

LAN digunakan untuk berbagai tujuan, termasuk:

- a. Berbagi Sumber Daya: Pengguna dapat berbagi printer, penyimpanan jaringan, atau perangkat lunak yang diakses oleh beberapa komputer.
- b. Akses Internet Terpusat: Dalam sebuah LAN, beberapa komputer dapat berbagi satu koneksi internet yang sama.
- c. File Sharing: Pengguna dapat dengan mudah berbagi file dan folder antar komputer di jaringan.

- d. Komunikasi Internal: LAN memungkinkan pengguna berkomunikasi secara instan, seperti melalui email, pesan instan, atau sistem kolaborasi perusahaan.
- e. Keamanan Data: Administrator jaringan dapat mengontrol akses pengguna, mengatur hak istimewa, serta mengelola keamanan jaringan untuk melindungi informasi sensitif.

Keuntungan menggunakan LAN yaitu:

- a. Kecepatan Transfer yang Tinggi: LAN menawarkan kecepatan tinggi untuk mengirim dan menerima data antar perangkat di dalam jaringan.
- b. Biaya Murah: Menghubungkan komputer dan perangkat lain dalam satu area menggunakan kabel atau Wi-Fi lebih hemat biaya dibandingkan WAN yang memerlukan infrastruktur yang lebih besar.
- c. Kemudahan Pengelolaan: Karena jangkauan terbatas, pengelolaan dan pengaturan LAN lebih sederhana.
- d. Keamanan Terpusat: Administrator jaringan dapat mengontrol akses ke sumber daya dan data, serta melindungi jaringan dari ancaman eksternal.

Kelemahan menggunakan LAN yaitu:

- a. Jangkauan Terbatas: LAN hanya cocok untuk area kecil. Untuk area yang lebih luas, jaringan lain seperti MAN atau WAN diperlukan.
- b. Ketergantungan pada Perangkat Pusat: Jika switch atau router pusat dalam jaringan LAN mengalami kerusakan, seluruh jaringan bisa terganggu.
- c. Masalah Kepadatan: Jika terlalu banyak perangkat terhubung ke satu LAN tanpa manajemen yang tepat, kinerja jaringan bisa menurun.

LAN adalah jaringan yang efisien untuk menghubungkan perangkat dalam area yang kecil, memungkinkan pertukaran data, akses internet, dan berbagi sumber daya dengan kecepatan tinggi dan biaya yang relatif rendah. Topologi dan perangkat keras yang digunakan dalam LAN memberikan fleksibilitas bagi pengguna untuk mengelola jaringan secara optimal, dengan kontrol keamanan yang terpusat.

2. MAN (*Metropolitan Area Network*)

MAN adalah jaringan yang mencakup area lebih luas dibandingkan LAN, biasanya dalam satu kota. MAN menghubungkan beberapa LAN dan sering digunakan oleh perusahaan besar atau instansi pemerintah untuk menghubungkan cabang di kota yang sama.

Metropolitan Area Network (MAN) adalah jaringan komputer yang mencakup area yang lebih luas daripada Local Area Network (LAN), tetapi lebih kecil daripada Wide Area Network (WAN). MAN biasanya mencakup satu kota atau wilayah metropolitan dan sering digunakan untuk menghubungkan beberapa LAN di area yang lebih besar, seperti kampus universitas, pusat bisnis, atau berbagai kantor pemerintah yang tersebar di seluruh kota.

MAN dirancang untuk menyediakan koneksi berkecepatan tinggi dan andal dalam area metropolitan, serta menghubungkan berbagai bangunan atau kantor yang berjauhan tetapi masih berada dalam satu kota. MAN sering digunakan untuk menyatukan jaringan yang tersebar dalam satu organisasi, perusahaan besar, atau lembaga pendidikan yang memiliki banyak lokasi. Untuk memahami MAN dengan lebih baik, mari kita pelajari karakteristiknya:

- a. Cakupan Wilayah Menengah: MAN mencakup area yang lebih luas daripada LAN, umumnya satu kota atau wilayah metropolitan.
- b. Kecepatan Tinggi: MAN mendukung kecepatan yang cukup tinggi (mulai dari 10 Mbps hingga 10 Gbps), terutama jika menggunakan kabel serat optik atau teknologi nirkabel kecepatan tinggi.
- c. Penggunaan Infrastruktur Publik dan Swasta: MAN sering menggunakan infrastruktur telekomunikasi publik atau swasta untuk menyediakan layanan jaringan.
- d. Jaringan Penghubung: MAN menghubungkan beberapa LAN, sehingga memungkinkan komunikasi yang cepat antar organisasi atau departemen yang tersebar di satu wilayah metropolitan.

Komponen MAN yaitu:

- a. Router: Router digunakan untuk menghubungkan jaringan-jaringan LAN yang berbeda dan memastikan data dikirimkan ke tujuan yang benar di dalam MAN.
- b. Switch: Switch digunakan untuk menghubungkan beberapa perangkat dalam jaringan LAN atau MAN. Switch berkecepatan tinggi sering digunakan dalam MAN untuk memastikan transmisi data yang efisien.
- c. Serat Optik: MAN sering menggunakan kabel serat optik karena mampu mendukung kecepatan transmisi data yang sangat tinggi dan memiliki jangkauan yang lebih luas dibandingkan dengan kabel tembaga.
- d. Hubungan Point-to-Point (PTP): Untuk menghubungkan dua jaringan atau dua lokasi yang berjauhan dalam satu area metropolitan, hubungan point-to-point (misalnya, menggunakan serat optik) sering digunakan.
- e. Jaringan Nirkabel: Selain kabel serat optik, MAN juga dapat menggunakan teknologi nirkabel seperti WiMAX atau microwave link untuk menghubungkan area yang lebih luas tanpa kabel fisik.

Keuntungan MAN:

- a. Kecepatan Tinggi dan Jangkauan Luas: MAN memberikan akses ke jaringan berkecepatan tinggi di seluruh area metropolitan, memungkinkan komunikasi yang cepat dan efisien antara lokasi-lokasi yang berbeda.
- b. Integrasi Antar Jaringan: Dengan MAN, beberapa LAN yang terpisah dapat diintegrasikan, memungkinkan berbagi sumber daya dan informasi di seluruh organisasi atau kota.
- c. Biaya Lebih Rendah Dibanding WAN: MAN lebih murah untuk diimplementasikan dan dikelola dibandingkan dengan WAN, terutama jika menggunakan infrastruktur publik atau teknologi nirkabel.
- d. Konektivitas Stabil: MAN memberikan konektivitas yang lebih stabil dan andal dibandingkan dengan jaringan yang mengandalkan internet publik untuk menghubungkan berbagai lokasi.

Kekurangan MAN:

- a. Biaya Implementasi yang Cukup Tinggi: Meski lebih murah dibandingkan WAN, pembangunan MAN tetap memerlukan biaya yang besar, terutama jika memerlukan pemasangan kabel serat optik atau perangkat nirkabel khusus.
- b. Kerumitan Administrasi: Mengelola dan mengamankan MAN bisa lebih rumit daripada LAN, terutama karena banyaknya perangkat dan jaringan yang harus dihubungkan.
- c. Rentan terhadap Serangan Keamanan: Karena cakupannya yang luas, MAN lebih rentan terhadap ancaman keamanan, seperti penyadapan, serangan DDoS, atau intrusi jaringan.

Metropolitan Area Network (MAN) adalah jaringan yang menghubungkan beberapa Local Area Network (LAN) dalam satu area metropolitan, memberikan solusi konektivitas berkecepatan tinggi dan memungkinkan komunikasi yang efisien antar lokasi yang tersebar di satu kota atau wilayah. MAN cocok untuk digunakan oleh perusahaan besar, kampus, dan lembaga pemerintahan untuk memfasilitasi komunikasi dan berbagi sumber daya secara cepat dan efisien.

3. WAN (*Wide Area Network*)

WAN mencakup area geografis yang sangat luas, bisa antar negara atau benua. Contoh terbaik dari WAN adalah internet. WAN memungkinkan komunikasi antar jaringan yang tersebar di lokasi yang jauh.

Wide Area Network (WAN) adalah jaringan komputer yang mencakup area geografis yang sangat luas, bahkan antar negara atau benua. WAN menghubungkan beberapa Local Area Network (LAN) atau Metropolitan Area Network (MAN) yang terpisah secara geografis, memungkinkan perangkat-perangkat di berbagai lokasi untuk saling berkomunikasi dan berbagi informasi.

WAN biasanya digunakan oleh organisasi besar, perusahaan multinasional, atau penyedia layanan internet (ISP) untuk memungkinkan komunikasi antar lokasi di berbagai negara atau benua. Teknologi WAN menggunakan

media komunikasi jarak jauh seperti kabel serat optik, satelit, atau koneksi internet publik.

Karakteristik WAN yaitu:

- a. Cakupan Area Sangat Luas: WAN mencakup area geografis yang besar, mulai dari beberapa kota hingga seluruh negara atau benua.
- b. Kecepatan Transfer Data Variatif: WAN bisa memiliki kecepatan transfer data yang beragam tergantung pada teknologi yang digunakan, dari koneksi standar hingga koneksi broadband berkecepatan tinggi.
- c. Menggunakan Teknologi Telekomunikasi: WAN sering menggunakan infrastruktur telekomunikasi publik, termasuk satelit, serat optik, dan jaringan telepon.
- d. Konektivitas Antarlokasi yang Jauh: WAN menghubungkan beberapa LAN atau MAN di berbagai lokasi geografis yang berjauhan.
- e. Jaringan Swasta dan Publik: WAN dapat dioperasikan oleh perusahaan secara pribadi atau menggunakan layanan publik yang disediakan oleh penyedia layanan jaringan (ISP).

Untuk memahami WAN dengan lebih baik, mari kita pelajari karakteristiknya:

- a. Router: Router dalam WAN digunakan untuk mengarahkan lalu lintas data antar jaringan yang berbeda. Router WAN lebih canggih dan mampu menangani komunikasi jarak jauh.
- b. Switch: Switch digunakan untuk menghubungkan beberapa perangkat dalam LAN sebelum data dikirimkan melalui router ke WAN.
- c. Media Transmisi Jarak Jauh: WAN memanfaatkan berbagai jenis media transmisi jarak jauh, seperti serat optik, satelit, gelombang radio (microwave), dan koneksi telepon.
- d. Leased Line: Banyak WAN menggunakan leased line (saluran yang disewa) dari perusahaan telekomunikasi untuk menjamin koneksi yang cepat dan aman antara dua titik jaringan.

- e. Modem: Modem digunakan untuk mengubah data digital menjadi sinyal analog (dan sebaliknya) sehingga dapat dikirim melalui saluran telepon atau teknologi lainnya.
- f. Internet Backbone: WAN sering memanfaatkan backbone internet global untuk menyediakan konektivitas antar wilayah yang sangat luas.

Keuntungan WAN, yaitu:

- a. Konektivitas Jarak Jauh: WAN memungkinkan konektivitas antar lokasi yang sangat jauh, dari satu kota hingga negara lain.
- b. Skalabilitas Tinggi: WAN dapat dengan mudah diperluas sesuai dengan kebutuhan perusahaan atau organisasi, mencakup lebih banyak lokasi atau meningkatkan kapasitas jaringan.
- c. Sentralisasi Data: WAN memungkinkan organisasi untuk menyimpan data di pusat data terpusat, memungkinkan manajemen yang lebih efisien dan keamanan yang lebih baik.
- d. Akses ke Layanan Cloud: WAN memungkinkan akses ke layanan berbasis cloud, seperti penyimpanan data, aplikasi SaaS (Software as a Service), dan lainnya, dari berbagai lokasi di seluruh dunia.

Kekurangan WAN, yaitu:

- 1. Biaya Tinggi: Membangun dan mengelola WAN bisa sangat mahal, terutama karena memerlukan infrastruktur khusus seperti leased line dan router kelas atas.
- 2. Kecepatan yang Berbeda-beda: Kecepatan transfer data pada WAN sering kali bervariasi tergantung pada media transmisi yang digunakan. Beberapa wilayah mungkin memiliki koneksi yang lebih lambat dibandingkan wilayah lain.
- 3. Keamanan yang Rentan: Karena mencakup area yang luas, WAN lebih rentan terhadap ancaman keamanan seperti peretasan, penyadapan, atau serangan DDoS.
- 4. Kompleksitas Pengelolaan: Mengelola WAN memerlukan tim ahli jaringan dan perangkat keras khusus karena kompleksitasnya, terutama ketika melibatkan koneksi antar negara atau benua.

Wide Area Network (WAN) adalah jaringan yang mencakup area geografis yang luas dan menghubungkan beberapa Local Area Network (LAN) yang terpisah secara geografis. WAN memungkinkan organisasi global, perusahaan besar, atau pemerintah untuk berkomunikasi dan berbagi data antar wilayah yang berjauhan, menggunakan infrastruktur telekomunikasi seperti serat optik, satelit, dan jaringan internet. WAN mendukung koneksi global, tetapi juga membutuhkan infrastruktur yang kompleks dan biaya yang besar.

4. PAN (*Personal Area Network*)

PAN adalah jaringan pribadi yang biasanya digunakan untuk menghubungkan perangkat seperti komputer, ponsel, atau tablet dalam jarak yang sangat dekat (sekitar 10 meter). Contoh umum PAN adalah jaringan Bluetooth dan koneksi Wi-Fi di rumah.

Personal Area Network (PAN) adalah jaringan komputer yang mencakup area pribadi yang sangat kecil, biasanya dalam jangkauan beberapa meter. PAN dirancang untuk menghubungkan perangkat pribadi seperti smartphone, laptop, tablet, headphone, printer, dan perangkat wearable (seperti smartwatch) dalam lingkup individu. Jaringan ini biasanya digunakan untuk komunikasi data jarak dekat antara perangkat pribadi dan dapat menggunakan koneksi nirkabel maupun kabel.

PAN umumnya digunakan untuk berbagi data, sinkronisasi perangkat, atau untuk menghubungkan perangkat ke internet melalui perangkat lain (misalnya tethering). Dalam kehidupan sehari-hari, PAN menjadi penting untuk mendukung berbagai aktivitas individu dalam mengakses, berbagi, dan menggunakan informasi secara efisien.

Karakteristik Personal Area Network (PAN), meliputi:

- a. Cakupan Terbatas: PAN biasanya mencakup area yang sangat kecil, biasanya hanya sekitar 10 meter atau kurang, seperti di sekitar tubuh atau di dalam ruangan.

- b. Komunikasi Antar Perangkat Pribadi: PAN menghubungkan perangkat pribadi seperti ponsel, laptop, dan tablet yang dimiliki oleh satu individu.
- c. Teknologi Nirkabel: PAN sering menggunakan teknologi nirkabel seperti Bluetooth, Wi-Fi, atau Near Field Communication (NFC) untuk komunikasi antar perangkat.
- d. Transmisi Data Cepat dan Langsung: PAN mendukung transfer data cepat antar perangkat tanpa memerlukan jaringan internet eksternal. Misalnya, Bluetooth digunakan untuk berbagi file antar perangkat yang berdekatan.
- e. Jaringan yang Dikelola Secara Pribadi: PAN diatur dan digunakan oleh satu individu untuk memenuhi kebutuhan komunikasi pribadinya.

Untuk memahami PAN dengan lebih baik, mari kita pelajari karakteristiknya:

- a. Perangkat Bluetooth: Bluetooth adalah salah satu teknologi utama yang digunakan dalam PAN untuk memungkinkan komunikasi nirkabel antara perangkat dalam jarak pendek, seperti ponsel, headset, atau perangkat wearable.
- b. Perangkat Wi-Fi: Wi-Fi juga dapat digunakan untuk PAN ketika perangkat-perangkat pribadi menghubungkan ke satu jaringan lokal kecil (misalnya hotspot dari smartphone).
- c. USB: Untuk PAN berbasis kabel, USB digunakan sebagai metode utama untuk menghubungkan dan mentransfer data antar perangkat, seperti saat menghubungkan ponsel ke laptop.
- d. NFC (Near Field Communication): NFC memungkinkan komunikasi antar perangkat dengan jangkauan yang sangat pendek, biasanya hanya beberapa sentimeter, seperti saat melakukan pembayaran dengan ponsel.

Keuntungan PAN, yaitu:

- a. **Mobilitas Tinggi:** PAN memungkinkan pengguna untuk tetap terhubung dan berbagi data antar perangkat pribadi secara fleksibel dan mudah, tanpa memerlukan infrastruktur jaringan yang rumit.
- b. **Hemat Biaya:** PAN biasanya tidak memerlukan perangkat keras atau layanan tambahan untuk digunakan, terutama pada koneksi Bluetooth atau Wi-Fi yang sudah tersedia di sebagian besar perangkat.
- c. **Sinkronisasi Data yang Mudah:** PAN mempermudah sinkronisasi data antar perangkat pribadi, seperti sinkronisasi file, kontak, atau aplikasi antara ponsel dan komputer.
- d. **Konsumsi Daya yang Rendah:** Teknologi PAN seperti Bluetooth umumnya memiliki konsumsi daya yang rendah, yang membuatnya ideal untuk perangkat mobile yang bergantung pada baterai.

Kekurangan PAN, yaitu:

- a. **Cakupan Terbatas:** Jangkauan PAN sangat terbatas, biasanya hanya beberapa meter, sehingga tidak ideal untuk komunikasi jarak jauh.
- b. **Kecepatan Transfer yang Terbatas:** Kecepatan transfer data melalui Bluetooth atau NFC biasanya lebih lambat dibandingkan dengan teknologi jaringan yang lebih besar seperti Wi-Fi atau jaringan seluler.
- c. **Keamanan:** Karena PAN sering menggunakan teknologi nirkabel, ada risiko keamanan seperti penyadapan data atau serangan oleh perangkat yang tidak dikenal jika tidak dikonfigurasi dengan benar.

5. **Internet**

Internet adalah jaringan global yang menghubungkan jutaan perangkat komputer di seluruh dunia. Dengan menggunakan protokol seperti TCP/IP, internet memungkinkan pertukaran informasi global melalui berbagai media komunikasi.

Internet adalah jaringan global yang menghubungkan jutaan komputer dan perangkat di seluruh dunia, memungkinkan komunikasi, pertukaran data, dan akses informasi dalam skala yang sangat besar. Secara sederhana, internet adalah "jaringan dari jaringan" (*network of networks*), di mana berbagai jaringan komputer, baik besar maupun kecil, terhubung

menggunakan protokol yang sama, yaitu *Transmission Control Protocol/Internet Protocol* (TCP/IP).

Internet mencakup berbagai layanan, seperti *World Wide Web* (WWW), email, transfer file, media sosial, aplikasi berbasis cloud, dan streaming. Teknologi internet memungkinkan kita untuk berkomunikasi secara instan, mengakses informasi dalam jumlah besar, dan menjalankan berbagai aktivitas digital, seperti belanja online, pendidikan, hiburan, dan bekerja dari jarak jauh.

Untuk memahami PAN dengan lebih baik, mari kita pelajari karakteristiknya:

- a. Jaringan Global: Internet adalah jaringan global yang menghubungkan berbagai perangkat di seluruh dunia, mencakup berbagai jaringan lokal (LAN) dan jaringan luas (WAN).
- b. Protokol Standar: Internet beroperasi menggunakan protokol standar, yaitu TCP/IP, yang memungkinkan perangkat dari berbagai vendor dan sistem operasi untuk saling berkomunikasi.
- c. Akses Terdistribusi: Internet memungkinkan pengguna untuk mengakses data dan informasi yang disimpan di server di seluruh dunia secara terdistribusi.
- d. Layanan Beragam: Selain World Wide Web, internet menyediakan berbagai layanan seperti email, forum, media sosial, aplikasi cloud, video streaming, dan banyak lagi.
- e. Interkoneksi Jaringan: Berbagai jaringan, dari jaringan rumah tangga hingga jaringan perusahaan besar, terhubung ke internet melalui penyedia layanan internet (ISP).

Komponen Internet, yaitu:

- a. Client: Perangkat pengguna seperti komputer, laptop, smartphone, atau tablet yang mengakses internet untuk meminta layanan atau informasi.
- b. Server: Komputer atau sistem yang menyediakan layanan atau informasi kepada client, seperti server web yang mengirimkan halaman web ke browser.

- c. Router: Perangkat jaringan yang mengarahkan lalu lintas data di antara berbagai jaringan komputer yang terhubung ke internet.
- d. ISP (Internet Service Provider): Penyedia layanan internet yang memungkinkan perangkat pengguna untuk terhubung ke internet melalui infrastruktur mereka.
- e. Modem: Perangkat yang mengubah sinyal digital dari komputer menjadi sinyal analog (atau sebaliknya) agar dapat dikirimkan melalui saluran telepon, kabel, atau serat optik.
- f. DNS (Domain Name System): Sistem yang menerjemahkan nama domain (seperti www.google.com) menjadi alamat IP numerik yang dapat dikenali oleh komputer.

Keuntungan Internet, yaitu:

- a. Akses ke Informasi Global: Pengguna dapat mengakses informasi dari seluruh dunia dengan cepat dan mudah.
- b. Kemudahan Komunikasi: Komunikasi jarak jauh menjadi lebih mudah dengan layanan seperti email, media sosial, dan pesan instan.
- c. Kolaborasi Global: Internet memungkinkan kolaborasi di antara tim yang tersebar di berbagai lokasi geografis, seperti dalam proyek-proyek kerja atau penelitian.
- d. Efisiensi Bisnis: E-commerce dan aplikasi berbasis internet memungkinkan bisnis beroperasi lebih efisien dan menjangkau pelanggan di seluruh dunia.
- e. Sumber Hiburan Tanpa Batas: Pengguna dapat menikmati berbagai konten hiburan seperti video, musik, permainan, dan lainnya melalui internet.

Kekurangan Internet, yaitu:

- 1. Keamanan: Internet rentan terhadap serangan siber seperti peretasan, pencurian data, dan malware yang dapat mengancam privasi dan keamanan pengguna.

2. Ketergantungan: Pengguna mungkin menjadi terlalu bergantung pada internet untuk melakukan pekerjaan, berkomunikasi, atau bersosialisasi.
3. Penyebaran Informasi Salah: Internet memungkinkan penyebaran informasi yang salah atau hoaks, yang dapat menyebabkan kebingungan atau kerugian.
4. Privasi: Dengan semakin banyaknya informasi pribadi yang disimpan secara online, risiko pelanggaran privasi semakin meningkat.

Internet adalah jaringan global yang memungkinkan komunikasi, berbagi informasi, dan akses ke berbagai layanan dari berbagai perangkat di seluruh dunia. Dengan memanfaatkan teknologi seperti TCP/IP, HTTP, dan DNS, internet telah mengubah cara kita bekerja, belajar, dan bersosialisasi. Meskipun memiliki banyak manfaat, seperti akses informasi yang mudah dan kemudahan komunikasi, internet juga menghadapi tantangan dalam hal keamanan dan privasi.

Topologi jaringan merujuk pada cara fisik atau logis di mana perangkat jaringan dihubungkan. Ada beberapa jenis topologi yang sering digunakan:

1. **Topologi Bus**

Pada topologi ini, semua perangkat terhubung ke satu kabel utama atau bus, dan sinyal data dikirimkan ke semua perangkat dalam jaringan. Kelebihannya sederhana dan murah, namun jika kabel bus mengalami masalah, seluruh jaringan terputus.

2. **Topologi Star**

Semua perangkat terhubung ke satu pusat atau hub/switch. Jika salah satu perangkat mengalami gangguan, perangkat lain tidak terpengaruh. Namun, jika hub pusat bermasalah, seluruh jaringan akan terganggu.

3. **Topologi Ring**

Pada topologi ini, perangkat dihubungkan dalam bentuk cincin, di mana data mengalir searah jarum jam atau sebaliknya. Masalah di satu titik dapat mengganggu seluruh jaringan.

4. **Topologi Mesh**

Dalam topologi mesh, setiap perangkat terhubung langsung ke perangkat lain. Hal ini menciptakan redundansi dan sangat andal, namun biaya instalasi tinggi karena memerlukan banyak koneksi.

Protokol adalah aturan yang menentukan bagaimana data dikirim dan diterima dalam jaringan komputer. Beberapa protokol penting dalam jaringan komputer adalah:

1. **TCP/IP (Transmission Control Protocol/Internet Protocol)**. Ini adalah protokol dasar yang digunakan di internet. TCP/IP mengatur bagaimana data dibagi menjadi paket, dikirim, dan kemudian disusun kembali.
2. **HTTP (Hypertext Transfer Protocol)**. Protokol yang digunakan untuk mentransfer halaman web di internet.
3. **FTP (File Transfer Protocol)**. Digunakan untuk mentransfer file antar komputer dalam jaringan.
4. **SMTP (Simple Mail Transfer Protocol)**. Protokol yang digunakan untuk mengirim email antar server.

Jaringan komputer adalah fondasi dari dunia digital modern, memungkinkan komunikasi, kolaborasi, dan akses ke sumber daya dengan cara yang belum pernah ada sebelumnya. Dengan memahami komponen, jenis, topologi, protokol, dan keamanannya, kita dapat mengoptimalkan manfaat jaringan sekaligus menghadapi tantangan yang mungkin muncul.

C. Jaringan Komputer dan Cloud System

Cloud system atau *cloud computing* adalah teknologi yang memungkinkan penyimpanan, pengelolaan, dan pengolahan data melalui internet, dengan menggunakan server yang di-hosting di pusat data jarak jauh. Alih-alih mengandalkan perangkat keras lokal seperti komputer atau server fisik, cloud system menyediakan layanan komputasi secara *on-demand* melalui jaringan.

Konsep Utama Cloud Computing:

1. **On-Demand Self-Service**: Pengguna dapat mengakses sumber daya komputasi kapan saja tanpa interaksi manusia dengan penyedia layanan.
2. **Broad Network Access**: Sumber daya cloud dapat diakses melalui jaringan internet dari berbagai perangkat seperti laptop, tablet, atau smartphone.

3. Resource Pooling: Sumber daya komputasi seperti penyimpanan dan daya pemrosesan dibagikan kepada beberapa pengguna melalui sistem multi-tenant (penggunaan sumber daya yang sama oleh banyak pelanggan).
4. Rapid Elasticity: Kapasitas komputasi dapat ditingkatkan atau dikurangi dengan cepat sesuai kebutuhan pengguna, membuatnya sangat fleksibel.
5. Measured Service: Cloud system menggunakan model pembayaran berdasarkan penggunaan, sehingga pengguna hanya membayar sesuai dengan kapasitas yang mereka gunakan.

Cloud computing dan jaringan komputer memiliki hubungan yang sangat erat, karena keduanya saling bergantung dalam menyediakan layanan dan akses yang efisien kepada pengguna. Berikut adalah penjelasan lebih detail mengenai hubungan antara keduanya:

1. Koneksi dan Infrastruktur
 - a. Cloud computing bergantung pada jaringan komputer untuk menyediakan akses ke layanan berbasis cloud. Layanan cloud (seperti penyimpanan, server virtual, aplikasi) di-host di data center yang terletak di berbagai lokasi geografis.
 - b. Jaringan komputer, baik LAN, MAN, maupun WAN, digunakan untuk menghubungkan perangkat pengguna ke pusat data cloud. Tanpa jaringan yang cepat dan stabil, pengguna tidak dapat mengakses layanan cloud dengan efisien.
2. Internet sebagai Penghubung Cloud
 - a. Internet adalah bentuk dari Wide Area Network (WAN) yang menjadi penghubung utama untuk mengakses layanan cloud. Internet memungkinkan pengguna untuk berkomunikasi dengan infrastruktur cloud yang mungkin terletak di berbagai belahan dunia.
 - b. Layanan cloud biasanya diakses melalui broad network access, yang berarti perangkat pengguna di seluruh dunia terhubung melalui jaringan komputer yang besar, termasuk internet.
3. Performa Jaringan Mempengaruhi Cloud

- a. Kecepatan dan kualitas jaringan komputer sangat mempengaruhi pengalaman pengguna dalam mengakses cloud. Jika jaringan lambat atau tidak stabil, akses ke layanan cloud seperti aplikasi berbasis web, penyimpanan cloud, atau komputasi jarak jauh akan terganggu.
 - b. Jaringan dengan latensi rendah dan bandwidth tinggi sangat penting untuk layanan cloud yang membutuhkan performa real-time, seperti video conferencing, gaming online, atau aplikasi IoT (*Internet of Things*).
4. Keamanan Jaringan dan Cloud
- a. Keamanan dalam cloud computing sangat bergantung pada keamanan jaringan. Jaringan komputer harus dilindungi dari serangan siber, seperti DDoS (*Distributed Denial of Service*), peretasan, atau penyusupan data, yang dapat mengganggu akses ke layanan cloud atau mencuri informasi penting.
 - b. Layanan cloud sering menggunakan protokol jaringan yang aman seperti VPN (*Virtual Private Network*), SSL/TLS, dan firewall untuk menjaga keamanan data yang dikirimkan melalui jaringan.
5. Komputasi Terdistribusi
- a. Cloud computing memungkinkan komputasi terdistribusi, di mana sumber daya komputasi tersebar di berbagai pusat data di seluruh dunia. Jaringan komputer diperlukan untuk menghubungkan pusat data tersebut, sehingga memungkinkan data dan aplikasi di-host di banyak tempat secara bersamaan.
 - b. Misalnya, dalam Content Delivery Network (CDN), data di-cache dan didistribusikan di server yang dekat dengan lokasi pengguna, dan jaringan komputer mengatur komunikasi antara server cloud dan pengguna akhir.
6. Virtualisasi dan Jaringan Virtual
- a. Dalam cloud computing, teknologi virtualisasi memungkinkan server fisik di jaringan komputer dibagi menjadi beberapa mesin virtual. Jaringan virtual ini beroperasi di atas jaringan fisik dan memungkinkan cloud

provider untuk memberikan layanan seperti Infrastructure as a Service (IaaS) atau Platform as a Service (PaaS).

- b. Jaringan *Software-Defined* (SDN) memungkinkan administrator cloud untuk mengelola jaringan secara fleksibel, mengubah konfigurasi dan routing tanpa harus mengubah infrastruktur fisik. SDN sangat terkait dengan *cloud networking* untuk mengatur lalu lintas data di pusat data cloud.

7. Skalabilitas Cloud Berkat Jaringan Komputer

- a. Cloud computing menawarkan skalabilitas yang tinggi, artinya sumber daya komputasi dapat dengan mudah diperbesar atau diperkecil berdasarkan kebutuhan pengguna. Jaringan komputer berperan penting dalam mendukung skalabilitas ini dengan memastikan bahwa saat lebih banyak server atau perangkat terhubung, jaringan tetap stabil dan dapat menangani peningkatan lalu lintas data.
- b. Infrastruktur jaringan yang kuat memungkinkan cloud provider untuk menambahkan server baru dengan cepat ke sistem cloud tanpa mengganggu kinerja layanan bagi pengguna.

8. Akses Global dan Cloud Multi-Lokasi

- a. Jaringan komputer memungkinkan akses global ke layanan cloud. *Data center cloud* berada di lokasi yang berbeda secara geografis, namun mereka semua dihubungkan melalui jaringan komputer, memungkinkan pengguna dari berbagai wilayah mengakses data dan aplikasi yang sama tanpa keterbatasan geografis.
- b. Redundansi jaringan juga meningkatkan keandalan cloud computing. Jika ada gangguan di satu pusat data atau wilayah jaringan, layanan cloud dapat dipindahkan ke server lain yang masih berfungsi tanpa mengganggu pengguna.

Hubungan antara jaringan komputer dan *cloud computing* sangat erat dan saling bergantung. Jaringan komputer menyediakan infrastruktur fisik dan jalur komunikasi yang memungkinkan *cloud computing* berfungsi dengan baik. Sebaliknya, *cloud computing* menggunakan teknologi jaringan untuk mengelola

dan mendistribusikan layanan secara global. Tanpa jaringan komputer yang andal dan efisien, cloud computing tidak akan dapat diakses dengan mudah, tidak aman, dan tidak mampu memberikan performa yang optimal bagi penggunanya.

D. Latihan

a. Pilihan Ganda

1. Apa yang dimaksud dengan jaringan secara umum?
 - a. Kumpulan perangkat keras yang tidak terhubung
 - b. Kumpulan titik-titik atau entitas yang saling terhubung untuk berbagi informasi
 - c. Hanya system transportasi yang saling terhubung
 - d. System yang tidak memiliki tujuan tertentu
 - e. Hanya perangkat lunak yang berfungsi untuk komunikasi
2. Salah satu contoh system operasi jaringan adalah
 - a. Microsoft Office
 - b. Windows Server
 - c. Adobe Photoshop
 - d. Google Chrome
 - e. VLC Media Player
3. Apa yang membedakan struktur jaringan hierarkis dan peer-to-peer?
 - a. Jaringan hierarkis memiliki elemen pusat, sedangkan peer-to-peer tidak
 - b. Jaringan peer-to-peer lebih mahal
 - c. Jaringan hierarkis lebih sederhana
 - d. Jaringan peer-to-peer tidak terhubung
 - e. Jaringan hierarkis tidak dapat berubah
4. Apa yang dimaksud dengan internet?
 - a. Jaringan lokal yang hanya menghubungkan komputer di satu tempat
 - b. Jaringan global yang menghubungkan jutaan perangkat di seluruh dunia
 - c. Hanya sistem komunikasi untuk email
 - d. Jaringan yang tidak memerlukan protokol untuk beroperasi
 - e. Jaringan pribadi yang tidak dapat diakses publik

5. Topologi jaringan yang menghubungkan semua perangkat ke satu pusat atau hub disebut
 - a. Topologi Ring
 - b. Topologi Star
 - c. Topologi Bus
 - d. Topologi Mesh
 - e. Topologi Hybrid

b. Esai

Jawablah pertanyaan dibawah ini!

1. Jaringan adalah interkoneksi atau hubungan antara beberapa elemen atau komponen yang membentuk suatu sistem. Dalam jaringan terdapat dinamika elemen yang bersifat dinamis. Jelaskan mengapa jaringan tersebut dikatakan bersifat dinamis!
2. Jika dibandingkan kelebihan dan kekurangan internet tersebut. Menurut kamu hal apa yang menjadi tantangan utama dalam penggunaan internet saat ini!
3. Jelaskan mengapa jaringan computer sangat mempengaruhi performa cloud computing!

BAB V

CLOUD SYSTEM SERVICE

TUJUAN PEMBELAJARAN

1. Mahasiswa mampu menjelaskan konsep *service delivery model* pada cloud?
2. Mahasiswa mampu menjelaskan layanan yang ada pada *cloud system*?
3. Mahasiswa mampu menganalisis penggunaan layanan pada *cloud system*?

Telah dibahas pada bab sebelumnya bahwa layanan cloud system akan disampaikan kepada penggunanya melalui jaringan internet. Model komputasi memperlakukan metodologi komputasi dari dua perspektif sebagai penyebaran dan sebagai layanan. Untuk memahami bagaimana *cloud system* dapat bermanfaat bagi konsumen, penting untuk memahami layanan yang ditawarkannya. Bab ini berfokus pada semua model pengiriman layanan ini.

A. SERVICE DELIVERY MODEL PADA CLOUD SYSTEM

Service Delivery Model pada Cloud Computing adalah pendekatan yang digunakan oleh penyedia layanan cloud untuk memberikan layanan kepada pengguna melalui berbagai model. Tiga model utama cloud computing yaitu *Infrastructure as a Service (IaaS)*, *Platform as a Service (PaaS)*, dan *Software as a Service (SaaS)*. Masing-masing model memberikan pengguna dan penyedia layanan tingkat kendali dan tanggung jawab yang berbeda. Masing-masing model dijelaskan di bawah ini:

1. Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) merupakan model layanan cloud yang mencakup infrastruktur TI dasar seperti sistem operasi, penyimpanan, jaringan, dan server. Infrastructure as a Service (IaaS) adalah model layanan cloud di mana penyedia layanan cloud menyediakan infrastruktur komputasi dasar kepada pengguna melalui internet. Infrastruktur ini meliputi komponen-komponen seperti server fisik atau virtual, penyimpanan data, jaringan, dan kadang-kadang sistem operasi dasar. Pengguna memiliki kendali penuh atas infrastruktur ini, memungkinkan mereka untuk menginstal sistem operasi,

aplikasi, dan software lainnya sesuai kebutuhan mereka. Contoh penggunaan termasuk hosting web, server virtual, dan penyimpanan data. Layanan IaaS seperti Amazon Web Services (AWS), Microsoft Azure, dan Google Compute Engine merupakan contoh layanan IaaS.

Tugas Pengguna pada layanan IaaS adalah melakukan pengelolaan pada aplikasi, *middleware*, dan sistem operasi, serta pengaturan keamanan dan data. Tugas Penyedia pada layanan IaaS adalah melakukan pengawasan infrastruktur fisik, termasuk server, penyimpanan, dan jaringan. Fitur Utama Layanan IaaS adalah sebagai berikut:

- a. Virtualisasi: Pengguna dapat membuat dan mengelola mesin virtual (VM), yang memungkinkan mereka untuk menjalankan beberapa sistem operasi dan aplikasi di atas satu perangkat keras fisik.
- b. Penyimpanan: IaaS menyediakan layanan penyimpanan berbasis cloud, baik dalam bentuk penyimpanan objek maupun block storage. Pengguna dapat menyimpan data dalam jumlah besar tanpa perlu khawatir tentang pengelolaan fisik perangkat penyimpanan.
- c. Jaringan: IaaS menyediakan kemampuan untuk mengonfigurasi jaringan virtual, termasuk subnet, IP address, dan firewall. Pengguna dapat mengatur arsitektur jaringan sesuai kebutuhan mereka.
- d. Keamanan: IaaS biasanya menyediakan alat keamanan, seperti firewall, enkripsi, dan pengelolaan identitas. Namun, pengguna bertanggung jawab atas manajemen keamanan di tingkat aplikasi.
- e. Skalabilitas: Infrastruktur dapat dengan mudah ditingkatkan atau diturunkan (scale up/scale down) sesuai dengan kebutuhan pengguna, memberikan fleksibilitas dalam penggunaan sumber daya.

Keuntungan IaaS:

- a. Penghematan Biaya: Pengguna tidak perlu membeli atau memelihara perangkat keras fisik. Biaya hanya dikenakan berdasarkan sumber daya yang digunakan, yang biasanya dihitung dalam satuan jam atau bulan.

- b. **Fleksibilitas dan Kontrol:** Pengguna memiliki kontrol penuh atas sistem operasi, aplikasi, dan lingkungan pengembangan. Ini memungkinkan penyesuaian tinggi sesuai dengan kebutuhan spesifik bisnis.
- c. **Skalabilitas Dinamis:** IaaS memungkinkan pengguna untuk dengan mudah menambah atau mengurangi kapasitas infrastruktur sesuai dengan fluktuasi kebutuhan.
- d. **Kecepatan Implementasi:** Pengguna dapat langsung memanfaatkan infrastruktur tanpa harus melalui proses pengadaan perangkat keras yang memakan waktu.
- e. **Keandalan:** Penyedia IaaS biasanya memiliki data center yang tersebar di berbagai lokasi, sehingga memberikan tingkat redundansi dan ketersediaan yang tinggi.

Komponen IaaS:

- a. **Komputasi:** Virtual Machines (VMs) atau container yang disediakan oleh penyedia cloud untuk menjalankan aplikasi pengguna. Contoh: Amazon EC2, Google Compute Engine.
- b. **Penyimpanan:** Penyediaan ruang penyimpanan berbasis cloud untuk menyimpan file, database, dan backup. Contoh: Amazon S3, Google Cloud Storage.
- c. **Jaringan:** Infrastruktur jaringan virtual yang menghubungkan berbagai VM dan layanan, termasuk load balancer, firewall, dan jaringan pribadi virtual (VPN). Contoh: Azure Virtual Network, AWS VPC.
- d. **Keamanan:** Perlindungan infrastruktur melalui firewall, VPN, enkripsi, dan sistem manajemen identitas. Penyedia IaaS sering menawarkan fitur keamanan tambahan, tetapi tanggung jawab utama berada pada pengguna.

Kapan Menggunakan IaaS:

- a. **Pengembangan dan Pengujian:** Perusahaan dapat menggunakan IaaS untuk membuat lingkungan pengembangan dan pengujian yang cepat dan murah tanpa perlu membeli perangkat keras.

- b. **Hosting Aplikasi Web:** IaaS ideal untuk menjalankan aplikasi web, terutama aplikasi yang memerlukan skalabilitas dan fleksibilitas.
- c. **Penyimpanan dan Pemulihan Data:** IaaS sering digunakan untuk menyediakan penyimpanan skala besar dan solusi pemulihan bencana yang lebih murah dibandingkan solusi tradisional.
- d. **Big Data dan Analytics:** Organisasi dapat menggunakan IaaS untuk memproses volume data yang sangat besar dan menjalankan aplikasi analitik kompleks.

2. Platform as a Service (PaaS)

PaaS adalah model layanan cloud di mana penyedia cloud menyediakan platform yang memungkinkan pengguna untuk mengembangkan, menjalankan, dan mengelola aplikasi tanpa perlu menangani infrastruktur yang mendasarinya. Platform as a Service (PaaS) adalah model layanan cloud yang menyediakan lingkungan platform lengkap untuk pengembangan, pengujian, pengelolaan, dan pengoperasian aplikasi. PaaS memungkinkan pengembang untuk fokus pada pengembangan aplikasi tanpa perlu khawatir tentang pengelolaan infrastruktur dasar seperti server, penyimpanan, atau jaringan. Dengan PaaS, pengembang dapat fokus pada pengembangan aplikasi daripada infrastruktur yang dibutuhkan.

Fitur Utama yang disediakan pada layanan PaaS sebagai berikut:

- a. **Lingkungan Pengembangan Terintegrasi:** PaaS menyediakan alat-alat pengembangan seperti IDE (Integrated Development Environment), tools kolaborasi, dan manajemen aplikasi, sehingga pengembang dapat fokus pada kode dan logika bisnis.
- b. **Manajemen Middleware:** PaaS menyertakan middleware seperti database, server aplikasi, serta server web yang sudah diatur dan dikelola oleh penyedia. Pengguna hanya perlu mengkonfigurasi dan menggunakannya.

- c. Dukungan Multi-Lingkungan: PaaS biasanya mendukung berbagai bahasa pemrograman seperti Java, Python, Ruby, Node.js, dan lain-lain, serta menyediakan kerangka kerja dan pustaka yang diperlukan.
- d. Otomasi Penyebaran: PaaS menawarkan kemampuan untuk secara otomatis menyebarkan aplikasi ke cloud tanpa harus menangani infrastruktur. Pengembang dapat dengan mudah mem-build, test, dan deploy aplikasi mereka.
- e. Skalabilitas Otomatis: PaaS memungkinkan aplikasi untuk menskalakan secara otomatis sesuai kebutuhan tanpa intervensi manual.
- f. Pengelolaan Database: Penyedia PaaS menawarkan integrasi dengan database yang sudah terkelola, memungkinkan pengguna untuk memilih dan menggunakan basis data tanpa perlu melakukan setup atau manajemen.

Keuntungan PaaS yang disediakan pada layanan PaaS sebagai berikut:

- a. Fokus pada Pengembangan: Dengan PaaS, pengembang tidak perlu khawatir tentang manajemen infrastruktur, sehingga dapat fokus pada pengembangan dan inovasi aplikasi.
- b. Penghematan Waktu dan Biaya: PaaS mengeliminasi kebutuhan untuk membeli, mengatur, atau memelihara infrastruktur. Ini mempercepat waktu peluncuran aplikasi dan mengurangi biaya.
- c. Kolaborasi yang Lebih Baik: PaaS sering kali mendukung kolaborasi tim dengan menyediakan akses terpusat ke alat-alat pengembangan, manajemen proyek, dan sumber daya cloud.
- d. Skalabilitas: Aplikasi yang dibangun di atas PaaS dapat secara otomatis meningkat atau menurun dalam hal kapasitas komputasi, tergantung pada beban kerja yang berubah-ubah.
- e. Ketersediaan dan Keandalan: Penyedia PaaS biasanya memiliki jaminan uptime yang tinggi, membuat aplikasi yang dihosting menjadi lebih stabil dan selalu tersedia.

Komponen PaaS yang disediakan pada layanan PaaS sebagai berikut:

- a. Infrastruktur Virtual: PaaS berjalan di atas infrastruktur cloud (IaaS) seperti server virtual, penyimpanan, dan jaringan, tetapi pengguna tidak perlu mengelola komponen ini.
- b. Lingkungan Pengembangan: Platform ini menyediakan alat pengembangan seperti compiler, debugger, libraries, API, dan framework yang diperlukan untuk membangun aplikasi.
- c. Sistem Operasi dan Middleware: PaaS mencakup sistem operasi dan middleware seperti server database, server aplikasi, atau web server yang sudah dikelola.
- d. Manajemen Aplikasi: PaaS biasanya menawarkan manajemen siklus hidup aplikasi, termasuk fitur deployment, monitoring, dan versioning yang memudahkan pengelolaan aplikasi sepanjang siklus hidupnya.
- e. Keamanan dan Monitoring: PaaS menyertakan fitur-fitur keamanan seperti autentikasi, otorisasi, enkripsi, serta monitoring aplikasi untuk memantau performa dan keamanan.

Contoh Layanan PaaS adalah sebagai berikut

- a. Google App Engine – Layanan PaaS dari Google yang mendukung berbagai bahasa pemrograman dan memungkinkan pengguna untuk membangun aplikasi web dan mobile tanpa mengelola server.
- b. Microsoft Azure App Services – Platform dari Microsoft untuk membangun, menyebarkan, dan mengelola aplikasi web dan mobile.
- c. Heroku – Layanan PaaS yang mendukung berbagai bahasa pemrograman seperti Ruby, Java, Python, dan Node.js.
- d. AWS Elastic Beanstalk – Layanan dari Amazon Web Services yang memungkinkan pengguna untuk dengan cepat menyebarkan dan mengelola aplikasi di cloud.
- e. Red Hat OpenShift – PaaS berbasis Kubernetes yang menyediakan platform untuk membangun dan menjalankan aplikasi containerized.

Tanggung Jawab dalam pengelolaan layanan PaaS, adalah sebagai berikut:

- a. Penyedia PaaS: Bertanggung jawab atas pengelolaan infrastruktur dasar, sistem operasi, middleware, dan alat pengembangan. Mereka juga menangani keamanan dan pembaruan platform.
- b. Pengguna PaaS: Fokus pada pengembangan dan pengelolaan aplikasi yang mereka buat, serta konfigurasi lingkungan aplikasi.

Kapan pengguna dapat memanfaatkan layanan PaaS?

- a. Pengembangan Aplikasi Web dan Mobile: PaaS sangat ideal untuk pengembang yang ingin membangun aplikasi web atau mobile dengan cepat tanpa harus memikirkan manajemen infrastruktur.
- b. Proyek Kolaboratif: Untuk tim pengembangan besar atau terdistribusi, PaaS memfasilitasi kolaborasi melalui akses terpusat ke alat pengembangan dan penyebaran aplikasi.
- c. Prototyping dan MVP (Minimum Viable Product): Startup atau bisnis yang ingin cepat membangun prototipe atau MVP dapat memanfaatkan PaaS untuk mempercepat pengembangan dan pengujian.
- d. Aplikasi dengan Beban Kerja yang Fluktuatif: PaaS sangat bermanfaat bagi aplikasi yang mengalami lonjakan penggunaan musiman atau tak terduga karena kemampuan skalabilitasnya.
- e. Pengelolaan Siklus Hidup Aplikasi: Jika aplikasi memerlukan siklus hidup yang dikelola secara end-to-end, PaaS menawarkan solusi dengan alat bawaan untuk pengembangan, penyebaran, dan pemantauan aplikasi.

Tantangan yang dihadapi dalam implementasi layanan PaaS adalah sebagai berikut:

- a. Keterbatasan Kustomisasi: Karena penyedia PaaS mengelola sebagian besar infrastruktur, ada keterbatasan dalam kustomisasi lingkungan, yang mungkin tidak cocok untuk semua jenis aplikasi.
- b. Vendor Lock-in: Karena setiap platform PaaS memiliki alat dan sistem yang berbeda, berpindah dari satu penyedia PaaS ke yang lain bisa menjadi sulit dan memerlukan penyesuaian aplikasi.

- c. Keamanan: Meskipun penyedia PaaS mengelola infrastruktur dan platform, pengguna tetap bertanggung jawab atas keamanan aplikasi dan data yang mereka kelola.

3. Software as a Service (SaaS)

Software as a Service (SaaS) adalah model layanan cloud di mana penyedia cloud menawarkan aplikasi perangkat lunak lengkap yang dapat diakses pengguna melalui internet. Pengguna tidak perlu khawatir tentang pengelolaan infrastruktur, middleware, atau aplikasi itu sendiri karena semua sudah ditangani oleh penyedia. SaaS adalah model layanan cloud di mana aplikasi perangkat lunak disediakan oleh penyedia cloud dan diakses oleh pengguna melalui internet. Pengguna tidak perlu menginstal, mengelola, atau memperbarui aplikasi ini karena semua pengelolaan dilakukan oleh penyedia SaaS. Pengguna hanya perlu mengakses aplikasi melalui browser atau antarmuka web, biasanya dengan model berlangganan atau *pay-as-you-go*.

Fitur Utama yang diberikan pada layanan SaaS adalah sebagai berikut:

- a. Akses Melalui Internet: Aplikasi SaaS dapat diakses dari perangkat apa pun yang terhubung ke internet menggunakan browser web, sehingga memberikan fleksibilitas tinggi.
- b. Manajemen Terpusat: Penyedia SaaS mengelola semua aspek aplikasi, termasuk infrastruktur, keamanan, pembaruan, dan ketersediaan. Pengguna tidak perlu mengelola atau mengonfigurasi perangkat keras atau perangkat lunak di sisi mereka.
- c. Skalabilitas: SaaS dirancang untuk dapat dengan mudah meningkatkan kapasitas sesuai kebutuhan pengguna. Pengguna dapat menambah atau mengurangi jumlah lisensi atau kapasitas sesuai dengan pertumbuhan bisnis.
- d. Pembayaran Berbasis Langganan: Biasanya, layanan SaaS ditawarkan dengan model pembayaran berbasis langganan bulanan atau tahunan, memungkinkan bisnis untuk mengontrol biaya sesuai dengan penggunaan.

- e. **Pembaruan Otomatis:** Pembaruan perangkat lunak dan fitur baru secara otomatis dilakukan oleh penyedia tanpa memerlukan intervensi dari pengguna.

Keuntungan yang diperoleh oleh pengguna jika menggunakan layanan SaaS, yaitu:

- a. **Penghematan Biaya:** Tidak ada kebutuhan untuk membeli perangkat keras atau lisensi perangkat lunak yang mahal, karena semua biaya sudah termasuk dalam langganan.
- b. **Penerapan Cepat:** Aplikasi SaaS biasanya sudah siap digunakan, sehingga tidak memerlukan waktu pemasangan yang lama. Pengguna dapat langsung mengakses aplikasi melalui internet.
- c. **Akses dari Mana Saja:** SaaS memberikan fleksibilitas untuk mengakses aplikasi dari mana saja selama ada koneksi internet, yang sangat berguna untuk bisnis dengan tenaga kerja yang terdistribusi.
- d. **Pengelolaan yang Sederhana:** Penyedia SaaS menangani semua pembaruan, pemeliharaan, dan pengelolaan infrastruktur. Ini mengurangi beban administrasi bagi pengguna dan tim TI.
- e. **Skalabilitas Dinamis:** SaaS memudahkan pengguna untuk menambah atau mengurangi jumlah pengguna atau kapasitas penyimpanan sesuai kebutuhan bisnis, tanpa harus membeli atau menginstal perangkat keras tambahan.
- f. **Keamanan Terpusat:** Penyedia SaaS biasanya menawarkan keamanan tingkat tinggi yang mencakup enkripsi data, cadangan otomatis, dan kontrol akses, seringkali dengan biaya lebih rendah daripada jika perusahaan harus membangun keamanan ini sendiri.

Komponen utama yang disediakan pada layanan SaaS adalah sebagai berikut:

- a. **Aplikasi Perangkat Lunak:** Aplikasi yang digunakan oleh pengguna, seperti alat manajemen proyek, aplikasi CRM, atau perangkat lunak kolaborasi. Semua fitur ini diakses melalui antarmuka web atau aplikasi yang diunduh.

- b. Infrastruktur: Penyedia SaaS bertanggung jawab atas infrastruktur yang mendukung aplikasi, seperti server, penyimpanan, dan jaringan.
- c. Keamanan dan Backup: Penyedia SaaS mengelola keamanan, autentikasi, dan pencadangan data untuk melindungi aplikasi dan informasi pengguna.

Contoh Layanan SaaS, yaitu:

- a. Google Workspace (sebelumnya G Suite): Layanan berbasis cloud yang menawarkan aplikasi untuk email, penyimpanan file, dokumen, spreadsheet, dan kalender.
- b. Microsoft 365: Paket aplikasi berbasis cloud yang mencakup Word, Excel, PowerPoint, serta layanan email dan penyimpanan OneDrive.
- c. Salesforce: Salah satu SaaS terpopuler di dunia yang menyediakan solusi Customer Relationship Management (CRM) berbasis cloud.
- d. Dropbox: Layanan penyimpanan dan berbagi file berbasis cloud.
- e. Zoom: Aplikasi konferensi video dan kolaborasi online yang digunakan untuk rapat, webinar, dan komunikasi tim.
- f. Slack: Aplikasi komunikasi dan kolaborasi tim yang berfungsi sebagai pusat percakapan untuk bisnis.

Pembagian Tanggung Jawab kepada pelanggan yang menggunakan layanan SaaS yaitu:

- a. Penyedia SaaS: Menyediakan, memelihara, dan memperbarui aplikasi serta infrastruktur pendukung. Mereka juga bertanggung jawab atas keamanan data, ketersediaan layanan, dan pembaruan perangkat lunak.
- b. Pengguna SaaS: Menggunakan aplikasi sesuai dengan kebutuhan bisnis dan memastikan bahwa konfigurasi aplikasi sesuai dengan proses bisnis mereka. Pengguna juga bertanggung jawab atas manajemen data dan kontrol akses.

Kapan sebaiknya menggunakan layanan SaaS:

- a. Aplikasi Standar yang Dibutuhkan Banyak Pengguna: SaaS ideal untuk aplikasi yang digunakan oleh banyak pengguna dalam suatu organisasi, seperti email, kolaborasi tim, atau CRM.

- b. **Bisnis yang Menginginkan Penghematan Biaya dan Penerapan Cepat:** SaaS menawarkan solusi yang hemat biaya dan cepat diterapkan, sehingga cocok untuk bisnis yang ingin menghindari investasi awal yang besar dalam perangkat keras atau pengembangan perangkat lunak.
- c. **Bisnis yang Memerlukan Skalabilitas:** SaaS memungkinkan perusahaan untuk dengan mudah menambah atau mengurangi jumlah pengguna sesuai dengan pertumbuhan atau pengurangan kebutuhan bisnis.
- d. **Mobilitas Tinggi dan Kerja Jarak Jauh:** SaaS memberikan fleksibilitas kepada tenaga kerja yang terdistribusi atau bekerja dari jarak jauh karena akses aplikasi tersedia dari mana saja melalui internet.
- e. **Penggunaan Perangkat Lunak Tanpa Keahlian TI Khusus:** Bisnis yang tidak memiliki tim TI yang kuat dapat menggunakan SaaS tanpa memerlukan keahlian teknis khusus untuk mengelola atau memelihara aplikasi.

Tantangan yang dihadapi dalam penerapan layanan SaaS adalah sebagai berikut:

- a. **Kurangnya Kustomisasi:** Meskipun SaaS menyediakan berbagai fitur, aplikasi ini seringkali tidak dapat dikustomisasi sebanyak solusi on-premise. Ini bisa menjadi masalah jika bisnis memerlukan solusi yang sangat spesifik.
- b. **Ketergantungan pada Koneksi Internet:** SaaS sepenuhnya bergantung pada koneksi internet. Jika terjadi gangguan internet, pengguna tidak akan dapat mengakses aplikasi mereka.
- c. **Keamanan Data:** Meskipun penyedia SaaS biasanya menyediakan keamanan tingkat tinggi, bisnis tetap bertanggung jawab atas pengelolaan data mereka. Ada kekhawatiran tentang bagaimana data disimpan dan dilindungi oleh penyedia layanan.
- d. **Vendor Lock-in:** Berpindah dari satu penyedia SaaS ke penyedia lain bisa menjadi tantangan, terutama jika terdapat data yang besar dan sistem yang terintegrasi dengan platform SaaS tertentu.

B. SISTEM TRADISIONAL VS SISTEM CLOUD

Sistem Tradisional dan Sistem Cloud adalah dua pendekatan yang berbeda dalam mengelola infrastruktur, perangkat lunak, dan layanan IT. Perbedaan utamanya terletak pada cara penyimpanan, pengelolaan, dan pengaksesan data dan aplikasi. Berikut adalah perbandingan antara kedua sistem tersebut:

1. Pengelolaan Infrastruktur

Sistem Tradisional:

Infrastruktur fisik (server, penyimpanan, dan jaringan) dikelola secara internal di perusahaan atau organisasi. Organisasi harus membeli, mengelola, dan memelihara perangkat keras serta perangkat lunak. Perlu adanya tim IT yang terlatih untuk mengelola seluruh operasi seperti instalasi, pemeliharaan, dan pembaruan perangkat lunak serta hardware.

Sistem Cloud:

Infrastruktur dikelola oleh penyedia cloud, dan pengguna hanya mengakses sumber daya IT yang diperlukan melalui internet. Penyedia cloud menangani operasi harian seperti pemeliharaan, pembaruan, dan keamanan. Organisasi hanya perlu mengelola aplikasi atau data mereka tanpa perlu mengurus hardware fisik.

2. Biaya

Sistem Tradisional:

Biaya awal yang tinggi untuk membeli perangkat keras, lisensi perangkat lunak, serta biaya untuk instalasi dan pemeliharaan. Biaya perawatan yang berkelanjutan termasuk daya listrik, pendinginan, dan perbaikan hardware. Perlu biaya tambahan untuk menambah kapasitas infrastruktur jika perusahaan berkembang.

Sistem Cloud:

Biaya berdasarkan penggunaan (pay-as-you-go), sehingga pengguna hanya membayar untuk layanan yang mereka gunakan. Tidak ada biaya awal yang besar, sehingga sangat cocok untuk bisnis yang ingin menghindari investasi awal yang besar. Mudah untuk menambah atau

mengurangi kapasitas sesuai kebutuhan tanpa biaya penambahan hardware.

3. Skalabilitas

Sistem Tradisional:

Skalabilitas terbatas dan lambat karena membutuhkan pembelian dan pemasangan perangkat keras baru. Proses peningkatan kapasitas memerlukan perencanaan yang matang serta biaya dan waktu tambahan.

Sistem Cloud:

Skalabilitas yang mudah dan hampir tidak terbatas, karena pengguna dapat menambah kapasitas komputasi, penyimpanan, atau sumber daya lainnya sesuai kebutuhan hanya dengan beberapa klik. Penyedia cloud dapat menyediakan layanan otomatis untuk skala naik atau turun sesuai dengan beban kerja.

4. Aksesibilitas dan Mobilitas

Sistem Tradisional:

Aksesibilitas terbatas pada lokasi fisik di mana infrastruktur dan sistem IT ditempatkan. Akses jarak jauh mungkin memerlukan jaringan privat (VPN) atau koneksi yang sangat terkontrol, sehingga lebih terbatas dan kurang fleksibel.

Sistem Cloud:

Akses dapat dilakukan dari mana saja melalui internet, selama ada koneksi. Ini memberikan fleksibilitas lebih bagi pekerja jarak jauh dan tim yang terdistribusi. Aplikasi dan data dapat diakses di berbagai perangkat (komputer, tablet, ponsel).

5. Keamanan

Sistem Tradisional:

Keamanan sepenuhnya dikelola oleh organisasi, termasuk perlindungan data, firewall, kontrol akses, dan backup. Organisasi bertanggung jawab atas semua aspek perlindungan data dan perangkat. Organisasi memiliki kontrol penuh atas data mereka, yang bisa lebih aman, tetapi juga menambah tanggung jawab besar.

Sistem Cloud:

Penyedia cloud umumnya menawarkan standar keamanan yang tinggi, termasuk enkripsi, otentikasi, dan kontrol akses. Keamanan, patching, dan backup sering kali ditangani secara otomatis. Namun, keamanan data bisa menjadi perhatian terutama jika terjadi insiden peretasan atau kebocoran data dari penyedia cloud.

6. Waktu Penerapan

Sistem Tradisional:

Proses penerapan aplikasi dan sistem baru memerlukan waktu lama karena harus dilakukan instalasi perangkat keras, sistem operasi, middleware, dan konfigurasi manual. Penerapan sistem tradisional sering kali memerlukan waktu berminggu-minggu atau bahkan berbulan-bulan.

Sistem Cloud:

Penerapan aplikasi jauh lebih cepat, karena infrastruktur dan platform sudah disediakan oleh penyedia cloud. Pengguna dapat mulai menggunakan layanan dalam hitungan menit atau jam. Aplikasi siap pakai dapat segera digunakan tanpa perlu persiapan infrastruktur fisik.

7. Pemeliharaan

Sistem Tradisional:

Pemeliharaan dilakukan oleh tim internal, yang meliputi pembaruan perangkat lunak, penggantian perangkat keras, pemecahan masalah, serta pemeliharaan fisik seperti sistem pendingin. Ini menambah beban biaya dan waktu bagi organisasi.

Sistem Cloud:

Penyedia cloud menangani semua aspek pemeliharaan, termasuk pembaruan perangkat lunak, perbaikan perangkat keras, dan pemantauan sistem. Pengguna fokus hanya pada pengelolaan data dan aplikasi mereka, dengan pembaruan dan pemeliharaan dilakukan secara otomatis.

C. Latihan

a. Pilihan Ganda

1. Layanan Infrastructure as a Service (IaaS) memungkinkan perusahaan untuk mengelola infrastruktur komputasi dengan fleksibilitas tinggi. Dalam implementasinya, perusahaan X memilih menggunakan IaaS untuk mengelola aplikasi kritikal dengan beban kerja yang dinamis. Berdasarkan skenario ini, analisislah alasan utama pemilihan IaaS dibandingkan PaaS.
 - a. IaaS menawarkan kontrol penuh atas infrastruktur, memungkinkan pengelolaan perangkat keras dan perangkat lunak
 - b. IaaS menyediakan lingkungan pengembangan aplikasi yang lebih mudah diakses oleh pengembang.
 - c. IaaS menghilangkan kebutuhan untuk mengelola sistem operasi, middleware, dan runtime
 - d. IaaS lebih cocok untuk aplikasi yang dikembangkan secara native di cloud dengan arsitektur skala kecil.
 - e. IaaS memudahkan kolaborasi antar pengembang dalam satu platform pengembangan terpadu.
2. Dalam konteks layanan cloud, Platform as a Service (PaaS) sering dipilih oleh perusahaan yang menginginkan efisiensi dalam pengembangan aplikasi. Namun, terdapat kelemahan pada fleksibilitas yang ditawarkan PaaS. Berdasarkan analisis fungsi PaaS, mengapa fleksibilitas ini lebih rendah dibandingkan dengan IaaS?
 - a. Karena PaaS memiliki keterbatasan dalam mengelola aplikasi yang membutuhkan integrasi dengan perangkat keras spesifik.
 - b. PaaS memberikan pengelolaan sistem operasi dan middleware, sehingga mengurangi kontrol pengembang atas infrastruktur.
 - c. PaaS hanya menyediakan layanan komputasi dasar, tidak seperti IaaS yang lebih komprehensif.
 - d. PaaS mengharuskan pengguna untuk memiliki lisensi perangkat lunak yang spesifik untuk menggunakan infrastruktur cloud.
- b PaaS dirancang hanya untuk aplikasi berbasis web, sementara IaaS bisa digunakan untuk aplikasi desktop.

3. Software as a Service (SaaS) sering kali dipilih oleh perusahaan karena kemudahan dalam penerapan dan skalabilitas yang tinggi. Namun, dalam beberapa kasus, terdapat kekhawatiran terhadap privasi dan keamanan data. Berdasarkan analisis risiko keamanan, apa alasan utama mengapa perusahaan tertentu mungkin tidak memilih SaaS untuk aplikasi yang menangani data sensitif?
 - a. Karena perusahaan tidak dapat mengontrol pembaruan sistem yang diterapkan oleh penyedia SaaS.
 - b. Penyedia SaaS memiliki akses penuh terhadap data perusahaan dan tidak dapat disesuaikan dengan kebutuhan spesifik perusahaan.
 - c. Model keamanan di SaaS sering kali lebih lemah dibandingkan dengan model keamanan di IaaS dan PaaS.
 - d. Data yang disimpan di SaaS selalu disimpan di server fisik milik perusahaan, sehingga tidak aman untuk penggunaan publik.
 - e. SaaS tidak dapat diintegrasikan dengan solusi keamanan pihak ketiga untuk memperkuat perlindungan data.
4. Sebuah perusahaan startup memilih menggunakan layanan PaaS untuk pengembangan aplikasi berbasis cloud. Namun, setelah beberapa waktu, mereka mengalami kesulitan dalam menyesuaikan lingkungan pengembangan dengan kebutuhan bisnis yang berubah cepat. Berdasarkan analisis, apakah tantangan utama yang sering dihadapi saat menggunakan PaaS untuk bisnis yang berkembang dengan cepat?
 - a. Keterbatasan dalam mengelola beban kerja yang terus meningkat karena platform yang terisolasi.
 - b. Kurangnya kontrol atas lapisan infrastruktur yang penting dalam menyesuaikan performa aplikasi.
 - c. Ketidakmampuan untuk melakukan penyesuaian terhadap perangkat keras server yang digunakan oleh PaaS.
 - d. Tidak adanya dukungan untuk integrasi dengan berbagai jenis database dalam satu platform.

- e. Ketidakmampuan untuk menjalankan aplikasi di berbagai jenis sistem operasi dalam satu lingkungan.
- 5. Saat memilih layanan cloud, perusahaan sering kali perlu mempertimbangkan aspek ketersediaan dan skalabilitas. Dalam konteks PaaS dan IaaS, bagaimana model skalabilitas di kedua layanan tersebut berbeda secara fundamental?
 - a. PaaS menawarkan skalabilitas vertikal dengan menambahkan kapasitas ke server yang ada, sedangkan IaaS hanya menawarkan skalabilitas horizontal.
 - b. IaaS memungkinkan pengguna untuk secara otomatis menambah kapasitas server tanpa batas, sedangkan PaaS memiliki batasan infrastruktur yang lebih ketat.
 - c. Skalabilitas di PaaS lebih mudah diimplementasikan karena pengguna hanya perlu menyesuaikan komponen aplikasi, sementara di IaaS, pengguna harus mengelola seluruh stack infrastruktur.
 - d. PaaS menyediakan skalabilitas berdasarkan beban aplikasi secara otomatis, sedangkan IaaS membutuhkan konfigurasi manual untuk setiap komponen infrastruktur.
 - e. IaaS memiliki keterbatasan dalam hal skalabilitas aplikasi yang tidak dimiliki PaaS karena tidak didesain untuk aplikasi skala besar.

b. Esai

Jawablah pertanyaan dibawah ini!

1. Jelaskan perbedaan 3 model utama service delivery model pada cloud computing!
2. Jika sebuah perusahaan bisnis lebih mementingkan keamanan dengan standar yang tinggi termasuk enkripsi, otentikasi dan kontrol akses, jelaskan sistem apa yang akan menjadi pilihan utama perusahaan bisnis tersebut!
3. Biaya merupakan hal yang paling utama yang diperhatikan oleh sebuah organisasi atau perusahaan. Dalam system tradisional dan system cloud terdapat perbedaan mendasar yang menjadikan keduanya sebagai tolak ukur. Jelaskan perbedaan biaya dari kedua system tersebut!

BAB VI

IMPLEMENTASI CLOUD SYSTEM

TUJUAN PEMBELAJARAN

1. Mahasiswa mampu menjelaskan konsep virtualisasi pada cloud?
2. Mahasiswa mampu menjelaskan konsep *virtual private cloud*?
3. Mahasiswa mampu menjelaskan mengenai *virtual data center*?

Virtualisasi dan Cloud System adalah dua konsep yang saling berkaitan namun berbeda dalam tujuan dan implementasinya. Keduanya merupakan teknologi penting dalam komputasi modern, terutama untuk meningkatkan efisiensi, fleksibilitas, dan penghematan biaya dalam pengelolaan infrastruktur IT. Berikut adalah penjelasan dan perbandingan keduanya:

A. Virtualisasi

Virtualisasi adalah teknologi yang memungkinkan beberapa sistem operasi atau aplikasi berjalan pada satu server fisik dengan memanfaatkan mesin virtual (VM). Dengan virtualisasi, sumber daya perangkat keras seperti CPU, RAM, penyimpanan, dan jaringan dapat dibagi dan digunakan secara efisien oleh berbagai sistem atau aplikasi.

Jenis-jenis Virtualisasi:

1. Virtualisasi Server: Menggunakan hypervisor untuk membuat beberapa mesin virtual (VM) yang berjalan di atas satu server fisik. Setiap VM bertindak seperti komputer independen. Contoh: VMware, Hyper-V, KVM.
2. Virtualisasi Penyimpanan (Storage Virtualization): Menggabungkan beberapa perangkat penyimpanan fisik menjadi satu unit penyimpanan virtual yang dapat diakses secara terpusat. Contoh: SAN (*Storage Area Network*), NAS (*Network Attached Storage*).
3. Virtualisasi Jaringan (Network Virtualization): Memisahkan sumber daya jaringan fisik menjadi beberapa jaringan virtual yang dapat dikelola secara terpisah. Contoh: VLAN (*Virtual LAN*), SDN (*Software-Defined Networking*).

4. **Virtualisasi Desktop (Desktop Virtualization):** Menjalankan lingkungan desktop di mesin virtual, memungkinkan pengguna untuk mengakses desktop mereka dari mana saja melalui internet. Contoh: Citrix Virtual Apps and Desktops, VMware Horizon.

Manfaat Virtualisasi:

1. **Efisiensi Sumber Daya:** Mengoptimalkan penggunaan perangkat keras fisik dengan menjalankan beberapa VM di satu server.
2. **Biaya Lebih Rendah:** Mengurangi kebutuhan akan server fisik tambahan, sehingga mengurangi biaya pembelian perangkat keras dan pemeliharaan.
3. **Isolasi dan Keamanan:** Setiap VM terisolasi satu sama lain, sehingga masalah di satu VM tidak mempengaruhi VM lainnya.
4. **Skalabilitas:** Memungkinkan pengguna untuk menambah atau mengurangi VM sesuai kebutuhan tanpa harus menambah perangkat keras fisik.
5. **Pemulihan Bencana:** Virtualisasi memudahkan proses pencadangan dan pemulihan, karena VM dapat dipindahkan atau dipulihkan dengan lebih cepat.

Keterkaitan dengan Cloud yaitu virtualisasi adalah fondasi teknologi utama di balik layanan cloud computing. Dengan memvirtualisasikan sumber daya fisik, cloud provider dapat menyediakan layanan cloud secara lebih fleksibel dan efisien kepada pengguna.

B. Virtual Private Cloud

Virtual Private Cloud (VPC) adalah layanan cloud yang menyediakan lingkungan komputasi terisolasi dan aman di dalam infrastruktur cloud publik. VPC memungkinkan pengguna untuk menjalankan aplikasi, menyimpan data, dan mengelola jaringan dengan tingkat keamanan dan kontrol yang lebih tinggi dibandingkan dengan layanan cloud publik biasa, meskipun infrastruktur dasarnya masih dimiliki oleh penyedia cloud.

1. Karakteristik Utama Virtual Private Cloud (VPC)

a. Isolasi Jaringan

- VPC menciptakan lingkungan yang terpisah di dalam cloud publik menggunakan teknik virtualisasi jaringan. Pengguna dapat

menentukan topologi jaringan, subnet, dan segmen-segmen jaringan yang terisolasi untuk berbagai aplikasi atau layanan.

- Meskipun berbagi infrastruktur fisik dengan pelanggan lain, isolasi dilakukan pada tingkat jaringan sehingga setiap VPC sepenuhnya terpisah dari yang lain.

b. Kontrol Penuh atas Konfigurasi Jaringan

- Pengguna VPC memiliki kendali penuh atas konfigurasi jaringan seperti pengaturan alamat IP, subnet, gateway, dan firewall.
- Pengguna dapat menentukan aturan lalu lintas jaringan, mengkonfigurasi tabel routing, dan menentukan aturan firewall untuk membatasi akses ke sumber daya tertentu.

c. Keamanan Tingkat Tinggi

- VPC dilengkapi dengan mekanisme keamanan tingkat lanjut, seperti **Network Access Control Lists (NACL)** dan **Security Groups**, yang membantu pengguna mengatur izin akses dan melindungi data dari ancaman eksternal.
- VPC memungkinkan pengguna untuk mengatur **VPN (Virtual Private Network)** atau **Direct Connect** yang menghubungkan jaringan on-premises dengan VPC, memberikan koneksi yang lebih aman dan privat ke cloud.

d. Subnet Publik dan Privat

Di dalam VPC, pengguna dapat membuat **subnet publik** yang terhubung langsung ke internet dan **subnet privat** yang hanya dapat diakses melalui jaringan internal (VPN atau Direct Connect). Ini memungkinkan pengguna untuk menempatkan layanan yang memerlukan akses internet di subnet publik, sementara data sensitif tetap terlindungi di subnet privat.

e. Dukungan Layanan Cloud

VPC dapat digunakan dengan berbagai layanan cloud seperti penyimpanan, komputasi, dan basis data. Contoh: pengguna dapat mengatur **Instance EC2 (Elastic Compute Cloud)** di **Amazon Web**

Services (AWS) atau **Virtual Machines (VMs)** di **Google Cloud** di dalam VPCnya.

f. Konektivitas Hybrid

VPC sering kali digunakan dalam skenario **cloud hybrid**, di mana organisasi memiliki sebagian infrastruktur di cloud dan sebagian lagi di on-premises. Dengan VPC, jaringan on-premises dan VPC di cloud dapat dihubungkan secara aman menggunakan VPN atau koneksi langsung (misalnya AWS Direct Connect, Azure ExpressRoute).

2. Manfaat Virtual Private Cloud (VPC)

- a. **Keamanan yang Ditingkatkan.** VPC menawarkan keamanan lebih baik dibandingkan cloud publik tradisional. Pengguna dapat mengatur kebijakan akses yang ketat dan mengontrol siapa yang bisa mengakses sumber daya di dalam jaringan virtualnya.
- b. **Kontrol Jaringan yang Lebih Baik.** Pengguna memiliki kendali penuh atas konfigurasi jaringan, routing, dan firewall. Mereka dapat mengelola lalu lintas dan mengatur koneksi antara subnet sesuai kebutuhan aplikasi mereka.
- c. **Skalabilitas.** Seperti cloud publik, VPC memungkinkan pengguna untuk menskalakan sumber daya dengan cepat tanpa harus mengelola perangkat keras fisik. Namun, isolasi di VPC memastikan bahwa skalabilitas tersebut tidak mengorbankan keamanan.
- d. **Fleksibilitas dalam Integrasi.** VPC dapat diintegrasikan dengan jaringan on-premises, sehingga organisasi dapat membangun **cloud hybrid** yang memanfaatkan manfaat cloud publik sekaligus menjaga kontrol penuh atas infrastruktur lokal mereka.
- e. **Peningkatan Kinerja.** Karena isolasi jaringan dan kendali penuh atas konfigurasi, pengguna dapat mengoptimalkan VPC untuk memastikan performa aplikasi yang tinggi dan stabil.

3. Contoh Layanan VPC dari Penyedia Cloud

- a. **Amazon Virtual Private Cloud (Amazon VPC):**

- Menyediakan kontrol penuh atas jaringan virtual di AWS.
 - Mendukung pembuatan subnet publik dan privat.
 - Menawarkan fitur seperti VPN, peering VPC, dan koneksi Direct Connect.
- b. **Google Cloud VPC:**
- Menyediakan jaringan global yang memungkinkan pengelolaan jaringan secara terpadu di seluruh region.
 - Mendukung fitur subnet IP yang diatur secara otomatis dan manual, serta firewall yang dapat disesuaikan.
- c. **Microsoft Azure Virtual Network (VNet):**
- Menyediakan layanan VPC untuk jaringan virtual di Azure.
 - Mendukung peering jaringan, koneksi VPN, dan Azure ExpressRoute untuk koneksi privat antara data center on-premises dan Azure.

C. Virtual Data Center

Virtual Data Center (VDC) adalah sebuah konsep di mana sumber daya komputasi seperti server, penyimpanan, jaringan, dan aplikasi yang biasanya ada di dalam data center fisik, disediakan secara virtual menggunakan teknologi virtualisasi dan cloud computing. VDC memungkinkan organisasi untuk mengelola dan menggunakan infrastruktur IT dengan cara yang lebih fleksibel, hemat biaya, dan mudah disesuaikan, tanpa harus memiliki atau mengelola perangkat keras fisik secara langsung.

1. Karakteristik Virtual Data Center (VDC)
 - a. Virtualisasi Sumber Daya. Semua komponen dalam VDC (seperti server, penyimpanan, dan jaringan) di-virtualisasi sehingga pengguna dapat mengelolanya seolah-olah mereka adalah sumber daya fisik, meskipun mereka sebenarnya dijalankan di atas infrastruktur cloud atau virtual.
 - b. Skalabilitas dan Elastisitas. VDC menawarkan fleksibilitas yang besar untuk menambah atau mengurangi kapasitas sesuai kebutuhan organisasi. Infrastruktur dapat diperbesar dengan mudah tanpa harus

melakukan investasi besar pada perangkat keras fisik, sehingga sangat sesuai untuk lingkungan yang membutuhkan kemampuan untuk menangani beban kerja yang berubah-ubah.

- c. **Pengelolaan Terpusat.** Pengguna dapat mengelola semua sumber daya mereka dari satu antarmuka yang terpusat, seperti konsol manajemen cloud. Hal ini memudahkan organisasi untuk memantau kinerja, penggunaan, dan status infrastruktur secara real-time, serta mengelola layanan IT dengan lebih efisien.
 - d. **Integrasi dengan Infrastruktur Cloud dan Hybrid.** VDC sering kali diintegrasikan dengan cloud public untuk membuat arsitektur cloud hybrid. Ini memungkinkan perusahaan untuk menggabungkan data center lokal mereka dengan sumber daya cloud, sehingga dapat menjalankan aplikasi dan layanan dengan lebih fleksibel dan efisien.
 - e. **Keamanan dan Isolasi.** VDC menawarkan fitur keamanan tingkat lanjut yang memungkinkan organisasi untuk mengamankan infrastruktur mereka, baik di dalam maupun di luar cloud. Ini termasuk firewall virtual, enkripsi data, dan manajemen akses untuk memastikan bahwa sumber daya dan data tetap aman.
 - f. **Layanan On-Demand.** Seperti layanan cloud lainnya, VDC memberikan kemudahan dengan model on-demand di mana sumber daya komputasi dapat diakses dan digunakan kapan saja sesuai kebutuhan, serta pengguna hanya membayar sesuai penggunaan (pay-as-you-go).
2. **Manfaat Virtual Data Center (VDC)**
- a. **Pengurangan Biaya Operasional.** VDC menghilangkan kebutuhan akan investasi besar dalam perangkat keras fisik dan biaya pemeliharaan data center, seperti listrik, pendinginan, dan ruang fisik. Dengan menggunakan layanan cloud atau virtualisasi, organisasi hanya membayar sumber daya yang mereka gunakan.
 - b. **Fleksibilitas dan Skalabilitas.** Pengguna dapat menambah atau mengurangi kapasitas infrastruktur dengan cepat dan mudah sesuai

dengan kebutuhan bisnis. Hal ini sangat penting untuk perusahaan yang mengalami fluktuasi beban kerja atau yang ingin memperluas kapasitas mereka tanpa harus menambah perangkat keras fisik.

- c. Pemulihan Bencana (Disaster Recovery) yang Lebih Baik. Karena VDC berbasis virtual, pemulihan data dan aplikasi menjadi lebih cepat dan lebih mudah dibandingkan dengan infrastruktur fisik tradisional. Data dapat direplikasi dan disimpan di beberapa lokasi cloud untuk meningkatkan ketahanan dan ketersediaan.
 - d. Manajemen yang Efisien. Dengan antarmuka manajemen terpusat, administrator dapat memonitor, mengelola, dan mengoptimalkan sumber daya infrastruktur secara real-time. Hal ini memudahkan tim IT untuk mengatur dan mengelola infrastruktur tanpa harus menangani perangkat keras fisik secara langsung.
 - e. Keamanan yang Ditingkatkan. Meskipun berjalan di infrastruktur cloud atau virtual, VDC menyediakan fitur keamanan yang canggih, termasuk jaringan terisolasi, enkripsi data, serta manajemen akses yang granular. Ini memberikan keamanan yang kuat sambil tetap fleksibel.
 - f. Mobilitas yang Tinggi. Karena infrastrukturnya virtual, VDC memungkinkan aplikasi dan layanan dipindahkan dengan mudah antara lingkungan on-premises dan cloud. Ini memudahkan perusahaan untuk melakukan migrasi ke cloud atau mengadopsi arsitektur hybrid.
3. Komponen Virtual Data Center
 - a. Virtual Server (Compute). Server fisik digantikan oleh virtual machine (VM) atau container yang menjalankan berbagai sistem operasi dan aplikasi. Ini memungkinkan banyak VM dijalankan di satu server fisik untuk meningkatkan efisiensi sumber daya.
 - b. Virtual Storage. VDC menggunakan storage virtualization, yang menggabungkan banyak perangkat penyimpanan fisik menjadi satu entitas penyimpanan virtual yang dapat dikelola dan digunakan secara terpusat.

- c. Virtual Network. Virtual Network Functions (VNF) dan Software-Defined Networking (SDN) digunakan untuk mengelola jaringan di dalam VDC. Pengguna dapat mengatur dan mengkonfigurasi jaringan virtual, termasuk virtual firewall, load balancer, dan VPN, untuk memastikan keamanan dan kinerja jaringan.
- d. Virtual Security. VDC mencakup solusi keamanan virtual seperti firewall virtual, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), enkripsi data, dan kontrol akses, yang semuanya diatur secara virtual untuk melindungi sumber daya yang ada di VDC.

D. Latihan

a. Pilihan Ganda

1. Seorang administrator IT perlu meningkatkan kinerja infrastruktur tanpa menambah perangkat keras fisik. Administrator tersebut memilih menggunakan teknologi virtualisasi untuk mencapainya. Di antara pilihan berikut, manakah yang akan memberikan isolasi antar aplikasi di server, efisiensi sumber daya optimal, dan mendukung berbagai system operasi dalam satu server fisik?
 - a. Penggunaan server fisik tambahan tanpa virtualisasi
 - b. Penggunaan desktop virtualization untuk menjalankan aplikasi
 - c. Menggunakan hypervisor untuk menjalankan beberapa VM di satu server fisik
 - d. Mengkonfigurasi VLAN untuk mengisolasi jaringan aplikasi
 - e. Menggunakan network virtualization untuk mengelola lalu lintas jaringan
2. Dalam implementasi Virtual Private Cloud (VPC), keamanan jaringan menjadi prioritas utama bagi perusahaan yang ingin memanfaatkan VPC di cloud publik. Dengan menggunakan VPC, perusahaan ingin memastikan bahwa komunikasi antara infrastruktur on-premises dan VPC mereka di cloud berlangsung secara aman. Dari solusi berikut, manakah yang akan memberikan koneksi paling aman dan terkontrol antara kedua infrastruktur tersebut?

- a. Menggunakan subnet public tanpa konfigurasi keamanan tambahan
 - b. menggunakan VPN untuk menghubungkan on-premises ke VPC
 - c. Menggunakan VPC dengan akses langsung ke internet untuk seluruh layana
 - d. Membuat firewall virtual yang hanya mengontrol akses masuk
 - b. Menggunakan cloud storage untuk menyimpan data secara langsung tanpa isolasi jaringan
3. Saat menggunakan Virtual Private Cloud (VPC), administrator ingin memastikan bahwa aplikasi yang berada di subnet publik dapat mengakses internet, tetapi data sensitif tetap terlindungi di subnet privat. Manakah dari langkah-langkah berikut yang paling efektif dalam mencapai konfigurasi ini?
- a. Menempatkan semua data dan aplikasi di subnet publik untuk akses mudah
 - b. Menghubungkan seluruh subnet ke internet tanpa konfigurasi firewall
 - c. Memanfaatkan gateway internet untuk subnet publik dan menggunakan VPN untuk subnet privat
 - d. Mengisolasi seluruh subnet agar tidak ada akses ke internet
 - e. Menggunakan subnet privat dan membatasi akses internet melalui Network Access Control List (NACL)
4. Virtualisasi adalah teknologi kunci dalam infrastruktur modern. Mengapa penggunaan teknologi virtualisasi dapat membantu perusahaan dalam mengelola beban kerja yang fluktuatif? Jelaskan bagaimana virtualisasi server dan virtualisasi penyimpanan dapat bekerja bersama untuk mencapai tujuan tersebut.
- a. Mengurangi penggunaan server fisik dan meningkatkan penyimpanan
 - b. Menggabungkan sumber daya perangkat keras yang terbatas
 - c. Mengalokasikan sumber daya secara dinamis sesuai kebutuhan
 - d. Mengurangi kecepatan akses data
 - e. Membatasi penggunaan penyimpanan berbasis jaringan

5. VPC memungkinkan perusahaan membangun cloud hybrid yang memadukan jaringan on-premises dengan cloud publik. Bagaimana konektivitas hybrid ini dapat membantu organisasi meningkatkan fleksibilitas dan keamanan?
 - a. Dengan cara mengintegrasikan data center lokal secara langsung
 - b. Dengan meningkatkan jumlah subnet public
 - c. Dengan menggunakan firewall tambahan
 - d. Dengan menyediakan koneksi yang lebih aman melalui Direct Connect atau VPN
 - e. Dengan meningkatkan akses ke internet melalui jaringan virtual

b. Esai

Jawablah pertanyaan dibawah ini!

1. Virtualisasi dan cloud system adalah dua konsep teknologi penting yang saling berkaitan. Jelaskan keterkaitan cloud dengan virtualisasi!
2. Jelaskan jenis-jenis Virtualisasi beserta dengan contohnya!
3. Virtual private cloud dan virtual data center merupakan layanan cloud yang sama-sama menyediakan penyimpanan. Jelaskan perbedaan penyimpanan yang dimaksud dari kedua layanan cloud tersebut!

BAB VII

CLOUD SYSTEM: SECURITY

TUJUAN PEMBELAJARAN

1. Mahasiswa mampu menjelaskan konsep *cloud security*?
2. Mahasiswa mampu menjelaskan ancaman-ancaman pada *cloud security*?
3. Mahasiswa mampu menjelaskan *cloud security design principle*?

Keamanan merupakan salah satu perhatian utama dalam adopsi *cloud system* atau *cloud computing*. Meskipun *cloud computing* menawarkan banyak manfaat seperti skalabilitas, fleksibilitas, dan pengurangan biaya, ada sejumlah issue keamananyang perlu diperhatikan oleh organisasi saat menggunakan *cloud*. Pada bab ini akan dibahas mengenai keamanan dan issue keamanan yang terkait dengan *cloud system*.

A. Keamanan Cloud System (Cloud Security)

Cloud Security merujuk pada perlindungan data, aplikasi, dan infrastruktur di lingkungan *cloud* dari berbagai ancaman dan risiko keamanan. Dengan adopsi yang semakin meluas dari layanan *cloud*, penting bagi organisasi untuk memahami dan menerapkan langkah-langkah keamanan yang tepat untuk melindungi aset mereka di *cloud*. Berikut adalah aspek utama dari keamanan *cloud*:

1. Model Keamanan Shared Responsibility

Shared Responsibility Model adalah konsep kunci dalam keamanan *cloud*. Model ini membagi tanggung jawab keamanan antara penyedia layanan *cloud* dan pelanggan.

- a. Penyedia Cloud: Bertanggung jawab atas keamanan infrastruktur yang mendasari layanan *cloud*, termasuk server fisik, penyimpanan, jaringan, dan virtualisasi. Ini sering disebut sebagai "keamanan dari *cloud*."
- b. Pelanggan: Bertanggung jawab atas keamanan data, aplikasi, dan konfigurasi sistem yang berjalan di atas infrastruktur *cloud*. Ini mencakup kontrol akses, enkripsi data, dan pengaturan konfigurasi yang aman. Ini dikenal sebagai "keamanan di *cloud*."

2. Keamanan Data

Keamanan data di cloud mencakup perlindungan terhadap data baik saat istirahat (*data at rest*) maupun saat ditransmisikan (*data in transit*).

- a. Enkripsi: Data harus dienkripsi baik saat disimpan di cloud maupun saat dikirim melalui jaringan. Teknik enkripsi seperti AES (Advanced Encryption Standard) dan TLS (Transport Layer Security) digunakan untuk melindungi data dari akses tidak sah.
 - b. Backup dan Recovery: Implementasi strategi backup yang efektif untuk memastikan data dapat dipulihkan jika terjadi kehilangan data atau kerusakan.
3. Keamanan Akses dan Identitas
- a. Autentikasi Multi-Faktor (MFA): Menggunakan lebih dari satu metode verifikasi untuk memastikan bahwa hanya pengguna yang sah yang dapat mengakses sistem. Contoh termasuk kombinasi password dan token.
 - b. Manajemen Identitas dan Akses (IAM): Mengelola hak akses pengguna dan memastikan bahwa hanya individu yang memiliki izin yang tepat yang dapat mengakses data dan aplikasi tertentu.
4. Keamanan Jaringan
- a. Firewall Virtual: Menggunakan firewall virtual untuk memfilter lalu lintas jaringan dan melindungi sumber daya cloud dari akses yang tidak sah.
 - b. Virtual Private Network (VPN): Menciptakan koneksi yang aman antara pengguna dan sumber daya cloud melalui jaringan publik dengan enkripsi.
 - c. Intrusion Detection and Prevention Systems (IDPS): Memantau dan mendeteksi aktivitas yang mencurigakan atau tidak sah di jaringan cloud.
5. Keamanan Aplikasi
- a. Pengujian Keamanan Aplikasi: Melakukan penetration testing dan vulnerability scanning untuk menemukan dan memperbaiki kerentanan dalam aplikasi cloud.

- b. Pengelolaan Patch: Memastikan bahwa semua perangkat lunak dan aplikasi diperbarui dengan patch keamanan terbaru untuk mengurangi risiko eksploitasi kerentanan.
6. Keamanan Infrastruktur dan Konfigurasi
- a. Pengelolaan Konfigurasi: Mengatur dan memantau konfigurasi sistem cloud untuk memastikan bahwa semua pengaturan keamanan diimplementasikan dengan benar.
 - b. Automated Compliance: Menggunakan alat otomatis untuk memeriksa dan memastikan bahwa konfigurasi sesuai dengan kebijakan keamanan dan standar kepatuhan yang relevan.
7. Pemantauan dan Logging
- a. Monitoring: Memantau aktivitas dan performa sistem cloud secara real-time untuk mendeteksi anomali atau potensi ancaman.
 - b. Logging: Mencatat semua aktivitas di sistem cloud untuk audit dan investigasi, membantu dalam identifikasi dan respons terhadap insiden keamanan.
8. Kepatuhan dan Regulasi
- a. Kepatuhan terhadap Standar: Memastikan bahwa penyedia cloud dan organisasi mematuhi standar dan regulasi yang relevan, seperti GDPR, HIPAA, PCI-DSS, atau ISO/IEC 27001.
 - b. Audit Keamanan: Melakukan audit secara berkala untuk memastikan bahwa praktik keamanan mematuhi kebijakan dan peraturan yang berlaku.
9. Keamanan Kontrak dan Layanan
- a. Persetujuan Layanan (SLA): Memastikan bahwa perjanjian dengan penyedia cloud mencakup klausul keamanan yang memadai, termasuk tanggung jawab dalam hal pelanggaran data atau gangguan layanan.
 - b. Due Diligence: Melakukan penilaian keamanan terhadap penyedia cloud sebelum kontrak, termasuk evaluasi kebijakan keamanan, prosedur, dan riwayat kepatuhan mereka.
10. Manajemen Insiden

- a. Respons Insiden: Mengembangkan dan mengimplementasikan rencana respons insiden untuk mengatasi dan mengelola kejadian keamanan, termasuk identifikasi, mitigasi, dan pemulihan.
- b. Pelatihan dan Kesadaran: Melatih staf mengenai praktik keamanan terbaik dan kesadaran tentang potensi ancaman, seperti phishing dan serangan malware.

B. Ancaman Pada Cloud

Ancaman pada keamanan cloud mencakup berbagai risiko yang dapat mempengaruhi data, aplikasi, dan infrastruktur yang berada di lingkungan cloud. Berikut adalah beberapa ancaman utama yang dihadapi dalam keamanan cloud:

1. Ancaman Pada Infrastruktur

Ancaman pada infrastruktur cloud melibatkan berbagai risiko yang dapat mempengaruhi keberlangsungan dan keamanan lingkungan cloud. Infrastruktur cloud mencakup komponen-komponen fundamental seperti server, penyimpanan, jaringan, dan virtualisasi. Berikut adalah beberapa ancaman utama yang bisa mengancam infrastruktur cloud:

- a. Kelemahan dalam Virtualisasi. Virtualisasi adalah teknologi yang memungkinkan beberapa sistem operasi berjalan pada satu mesin fisik. Kelemahan dalam layer virtualisasi, seperti hypervisor, dapat memungkinkan penyerang untuk memanipulasi atau mengakses sistem lain yang berbagi sumber daya dengan mesin virtualnya. Contoh: Serangan VM Escape, di mana penyerang berhasil melarikan diri dari lingkungan virtual dan mendapatkan akses ke sistem fisik yang mendasarinya.
- b. Serangan Distributed Denial of Service (DDoS). Deskripsi: Serangan yang membanjiri sumber daya cloud dengan lalu lintas berlebihan untuk menghentikan atau memperlambat layanan, mengakibatkan downtime atau kinerja yang buruk. Contoh: Penyerang meluncurkan serangan DDoS untuk menargetkan aplikasi atau layanan yang di-host di cloud, menyebabkan gangguan pada layanan.

- c. Ancaman dari Pihak Ketiga. Deskripsi: Risiko yang terkait dengan integrasi layanan atau aplikasi pihak ketiga dengan infrastruktur cloud, yang dapat memperkenalkan kerentanannya sendiri. Contoh: Aplikasi pihak ketiga yang terintegrasi dengan layanan cloud dapat mengakses data atau konfigurasi sensitif, dan jika aplikasi tersebut memiliki kerentanan, ini dapat menambah risiko bagi infrastruktur cloud.
- d. Kesalahan Konfigurasi (Misconfiguration). Deskripsi: Konfigurasi yang salah dalam pengaturan infrastruktur cloud dapat menyebabkan keamanan yang lemah atau membuka celah untuk serangan. Contoh: Bucket penyimpanan yang dikonfigurasi untuk akses publik secara tidak sengaja, memungkinkan data sensitif diakses oleh siapa saja.
- e. Penurunan Performa (Performance Degradation). Deskripsi: Penurunan kinerja sistem cloud yang disebabkan oleh berbagai faktor, termasuk serangan DDoS, over-provisioning, atau kegagalan hardware. Contoh: Beban yang berlebihan pada server virtual dapat menyebabkan penurunan performa aplikasi, mengakibatkan pengalaman pengguna yang buruk.
- f. Kelemahan dalam Keamanan Jaringan. Deskripsi: Ancaman yang mempengaruhi keamanan jaringan cloud, termasuk serangan yang menargetkan komunikasi dan koneksi jaringan. Contoh: Serangan Man-in-the-Middle (MitM) yang dapat menangkap dan menganalisis data yang dikirim antara pengguna dan layanan cloud jika komunikasi tidak dikripsi dengan benar.
- g. Kepatuhan dan Regulasi (Compliance and Legal Risks) Deskripsi: Risiko terkait dengan kepatuhan terhadap standar dan regulasi yang berlaku di berbagai wilayah hukum dan industri. Contoh: Data pribadi yang disimpan di cloud tidak sesuai dengan regulasi seperti GDPR atau HIPAA, dapat menyebabkan denda dan masalah hukum.
- h. Ancaman dari Dalam (Insider Threats). Deskripsi: Risiko yang berasal dari karyawan, kontraktor, atau mitra yang memiliki akses sah ke sistem

cloud tetapi menyalahgunakan akses tersebut. Contoh: Karyawan yang dengan sengaja atau tidak sengaja mengakses atau mengubah data yang tidak seharusnya mereka akses.

2. Ancaman Pada Informasi

Ancaman terhadap informasi di cloud berfokus pada risiko yang dapat mempengaruhi kerahasiaan, integritas, dan ketersediaan data yang disimpan atau diproses di lingkungan cloud. Berikut adalah beberapa ancaman utama yang berhubungan dengan informasi di cloud:

- a. Pelanggaran Data (Data Breaches). Deskripsi: Akses tidak sah atau pengungkapan data sensitif kepada pihak ketiga yang tidak berwenang. Ini sering disebabkan oleh kerentanan dalam kontrol akses atau kelemahan dalam sistem keamanan. Contoh: Data pelanggan seperti informasi kartu kredit atau data medis diakses oleh peretas karena konfigurasi penyimpanan yang tidak aman.
- b. Kebocoran Data (Data Leaks). Deskripsi: Data secara tidak sengaja terekspos kepada publik atau pihak yang tidak berwenang. Kebocoran ini sering terjadi karena kesalahan konfigurasi atau pengaturan keamanan yang tidak memadai. Contoh: File konfigurasi yang berisi kredensial API dipublikasikan di repositori kode yang dapat diakses oleh siapa saja.
- c. Pencurian Identitas (Identity Theft). Deskripsi: Pihak tidak berwenang memperoleh informasi pribadi atau identitas untuk menyalahgunakan atau mencuri identitas seseorang. Contoh: Kredensial login yang dicuri melalui serangan phishing dapat digunakan untuk mengakses data pribadi dan melakukan penipuan.
- d. Ransomware. Deskripsi: Serangan di mana data dienkripsi oleh penyerang, dan korban diminta untuk membayar tebusan untuk mendapatkan kunci dekripsi. Contoh: Data bisnis penting di-enkripsi oleh ransomware, yang kemudian meminta pembayaran dalam bentuk cryptocurrency untuk mengembalikan akses.

- e. **Manipulasi Data (Data Tampering).** Deskripsi: Modifikasi data yang dilakukan oleh pihak yang tidak berwenang, baik untuk tujuan jahat atau sebagai bagian dari serangan. Contoh: Penyerang mengubah data transaksi dalam sistem akuntansi cloud untuk menutupi pencurian atau penipuan.
- f. **Penghapusan Data (Data Deletion).** Deskripsi: Penghapusan data oleh pihak yang tidak berwenang, yang dapat merusak integritas data atau mengakibatkan kehilangan data yang tidak dapat dipulihkan. Contoh: Data yang dihapus oleh penyerang setelah mendapatkan akses tidak sah ke sistem cloud, menyebabkan hilangnya informasi penting.

3. Ancaman Pada Akses Kontrol

Ancaman pada akses kontrol di lingkungan cloud berhubungan dengan risiko-risiko yang mempengaruhi pengelolaan dan pengaturan hak akses pengguna serta sistem untuk memastikan bahwa hanya pihak yang berwenang yang dapat mengakses atau mengelola sumber daya. Berikut adalah beberapa ancaman utama terkait akses kontrol di cloud:

- c. **Pencurian Kredensial (Credential Theft).** Deskripsi: Pencurian username dan password atau kredensial lainnya yang memungkinkan penyerang mendapatkan akses tidak sah ke sistem cloud. Contoh: Kredensial dicuri melalui serangan phishing, malware, atau eksploitasi kerentanan dalam sistem autentikasi.
- d. **Kelemahan dalam Autentikasi Multi-Faktor (MFA).** Deskripsi: Kelemahan atau kegagalan dalam implementasi MFA, yang seharusnya memberikan lapisan tambahan keamanan, tetapi tidak diterapkan atau dikonfigurasi dengan benar. Contoh: Implementasi MFA yang buruk, seperti penggunaan SMS untuk kode MFA yang dapat disadap atau diintersepsi.
- e. **Pengaturan Akses yang Salah (Misconfiguration of Access Control).** Deskripsi: Kesalahan dalam pengaturan hak akses, yang dapat menyebabkan individu yang tidak berwenang mendapatkan akses ke sumber daya atau data sensitif. Contoh: Bucket penyimpanan yang

dikonfigurasi untuk akses publik atau hak akses yang terlalu luas pada sumber daya cloud.

- f. Kelemahan dalam Manajemen Identitas dan Akses (IAM). Deskripsi: Kelemahan dalam sistem IAM yang mengelola hak akses dan identitas pengguna, yang dapat mengakibatkan akses yang tidak sah atau penyalahgunaan hak akses. Contoh: Hak akses pengguna yang tidak diperbarui secara teratur, seperti pengguna yang memiliki akses ke data sensitif setelah mereka seharusnya tidak lagi memiliki hak tersebut.
- g. Penggunaan Hak Akses yang Berlebihan (Excessive Permissions). Deskripsi: Pemberian hak akses yang lebih luas dari yang diperlukan kepada pengguna atau sistem, yang dapat meningkatkan risiko penyalahgunaan atau akses tidak sah. Contoh: Pengguna diberikan akses admin penuh pada sistem yang seharusnya hanya memerlukan akses baca-tulis.

C. Cloud Security Design Principle

Merancang keamanan untuk lingkungan cloud memerlukan pendekatan yang komprehensif dan proaktif, memastikan bahwa semua aspek dari infrastruktur, aplikasi, dan data dilindungi dari ancaman. Berikut adalah prinsip desain keamanan yang harus diperhatikan dalam merancang sistem keamanan cloud:

1. Penerapan Prinsip Kebutuhan-Tahu (Least Privilege)
 - a. Deskripsi: Berikan hak akses minimum yang diperlukan untuk pengguna atau sistem untuk menyelesaikan tugas mereka. Ini membantu mengurangi risiko jika kredensial atau akun pengguna dikompromikan.
 - b. Implementasi: Gunakan kontrol akses berbasis peran (RBAC) dan aturan akses yang ketat untuk memastikan bahwa pengguna hanya dapat mengakses sumber daya yang mereka butuhkan.
2. Keamanan dari Awal hingga Akhir (Security by Design)

- a. Deskripsi: Integrasikan keamanan dari awal desain hingga implementasi dan pemeliharaan sistem. Jangan menambahkan keamanan sebagai solusi tambahan setelah sistem sudah berjalan.
 - b. Implementasi: Lakukan threat modeling dan penilaian risiko selama fase desain dan pengembangan untuk mengidentifikasi dan mengatasi potensi kerentanan.
3. Segmentasi dan Isolasi (Segmentation and Isolation)
 - a. Deskripsi: Pisahkan sumber daya dan data ke dalam zona yang berbeda untuk mengurangi dampak jika terjadi pelanggaran. Gunakan isolasi antara lingkungan pengembangan, uji coba, dan produksi.
 - b. Implementasi: Gunakan Virtual Private Cloud (VPC), subnet, dan grup keamanan untuk mengatur akses dan komunikasi antar komponen sistem.
 4. Enkripsi Data (Data Encryption)
 - a. Deskripsi: Lindungi data dalam transit dan saat diam dengan enkripsi untuk mencegah akses tidak sah dan pencurian data.
 - b. Implementasi: Terapkan enkripsi end-to-end untuk data yang dikirim dan diterima melalui jaringan, serta enkripsi pada penyimpanan data.
 5. Otentikasi dan Otorisasi yang Kuat (Strong Authentication and Authorization)
 - a. Deskripsi: Gunakan mekanisme autentikasi yang kuat untuk memastikan bahwa hanya pengguna yang sah yang dapat mengakses sistem. Implementasikan otorisasi untuk mengontrol akses ke sumber daya.
 - b. Implementasi: Gunakan autentikasi multi-faktor (MFA), dan kelola identitas serta hak akses menggunakan sistem manajemen identitas (IAM) yang canggih.
 6. Pemantauan dan Audit (Monitoring and Auditing)
 - a. Deskripsi: Monitor aktivitas sistem dan data secara real-time untuk mendeteksi dan merespons insiden keamanan dengan cepat. Lakukan audit untuk memastikan kepatuhan dan integritas.

- b. Implementasi: Implementasikan solusi pemantauan dan logging yang komprehensif, dan lakukan audit keamanan secara berkala untuk mengevaluasi kebijakan dan kontrol yang ada.
- 7. Respon Insiden dan Pemulihan Bencana (Incident Response and Disaster Recovery)
 - a. Deskripsi: Siapkan rencana untuk merespons insiden keamanan dan mengatasi pemulihan bencana untuk meminimalkan dampak terhadap bisnis.
 - b. Implementasi: Kembangkan dan uji rencana respon insiden serta strategi pemulihan bencana, termasuk backup data dan pemulihan sistem.
- 8. Kepatuhan dan Regulasi (Compliance and Regulatory Requirements)
 - a. Deskripsi: Pastikan bahwa desain keamanan memenuhi standar industri dan regulasi yang berlaku, seperti GDPR, HIPAA, atau PCI DSS.
 - b. Implementasi: Tetapkan kebijakan dan prosedur untuk mematuhi persyaratan regulasi, dan lakukan audit kepatuhan untuk memastikan kesesuaian.
- 9. Manajemen Kerentanan (Vulnerability Management)
 - a. Deskripsi: Identifikasi, evaluasi, dan mitigasi kerentanan yang dapat dieksploitasi oleh penyerang. Pastikan bahwa semua sistem dan aplikasi diperbarui dengan patch keamanan terbaru.
 - b. Implementasi: Gunakan alat pemindaian kerentanan untuk secara rutin memeriksa sistem, dan tetapkan proses untuk mengelola dan menerapkan pembaruan keamanan.
- 10. Keamanan Rantai Pasokan (Supply Chain Security)
 - a. Deskripsi: Pertimbangkan keamanan dalam rantai pasokan, termasuk vendor dan layanan pihak ketiga yang terintegrasi dengan sistem cloud.
 - b. Implementasi: Evaluasi keamanan dan kepatuhan vendor dan layanan pihak ketiga, dan pastikan bahwa mereka mematuhi standar keamanan yang relevan.

11. Privasi Data (Data Privacy)

- a. Deskripsi: Lindungi data pribadi dan pastikan bahwa data dikumpulkan, disimpan, dan digunakan sesuai dengan kebijakan privasi dan hukum yang berlaku.
- b. Implementasi: Terapkan kontrol akses yang ketat, enkripsi, dan teknik anonymisasi untuk melindungi data pribadi.

12. Automasi dan Orkestrasi Keamanan (Security Automation and Orchestration)

- a. Deskripsi: Gunakan automasi untuk mengelola dan menanggapi ancaman dengan cepat dan efektif, serta orkestrasi untuk mengkoordinasikan berbagai kontrol keamanan.
- b. Implementasi: Implementasikan solusi automasi keamanan untuk deteksi dan respons ancaman, serta integrasikan berbagai alat dan sistem keamanan untuk efektivitas yang lebih baik.

13. Evaluasi dan Peninjauan Berkelanjutan (Continuous Evaluation and Review)

- a. Deskripsi: Lakukan evaluasi dan peninjauan berkelanjutan terhadap kontrol dan kebijakan keamanan untuk memastikan bahwa mereka tetap efektif dan relevan.
- b. Implementasi: Tinjau dan perbarui kebijakan dan prosedur keamanan secara berkala berdasarkan hasil audit, perubahan dalam ancaman, dan pembaruan teknologi.

D. Latihan

a. Pilihan Ganda

1. Manakah dari berikut ini yang tidak termasuk dalam langkah-langkah meningkatkan keamanan akses dan identitas di cloud?
 - a. Autentikasi multi-faktor (MFA)
 - b. Manajemen identitas dan akses (IAM)
 - c. Penggunaan password yang lemah

- d. Enkripsi data
 - e. Firewall virtual
2. Apa yang seharusnya dilakukan organisasi untuk memastikan data cloud tetap aman dari ancaman kehilangan atau kerusakan?
 - a. Menggunakan firewall fisik
 - b. Melakukan backup dan recovery secara rutin
 - c. Memastikan system cloud setelah digunakan
 - d. Menghapus data setelah disimpan
 - e. Menggunakan penyedia layanan cloud yang berbeda
 3. Bagaimana Teknik homomorphic encryption meningkatkan keamanan dalam komputasi cloud
 - a. Dengan memungkinkan data diproses tanpa harus mendekripsinya
 - b. Dengan mengenkripsi data hanya selama pengiriman
 - c. Dengan memperkuat firewall cloud
 - d. Dengan menyediakan dua lapisan enkripsi pada penyimpanan data
 - e. Dengan membatasi akses pengguna internal
 4. Dalam konteks shared responsibility model, apa tanggung jawab pelanggan dalam menggunakan layanan infrastructure as a service (IaaS)?
 - a. Mengelola keamanan fisik data center
 - b. Mengamankan aplikasi, data dan system operasi yang digunakan
 - c. Mengontrol seluruh infrastruktur jaringan
 - d. Melakukan audit regular pada perangkat keras
 - e. Menjamin akses jaringan fisik
 5. Bagaimana serangan side-channel memengaruhi keamanan data dalam lingkungan cloud berbasis virtualisasi
 - a. Menyusup ke jaringan melalui perangkat lunak enkripsi yang lemah
 - b. Mengeksploitasi kebocoran informasi dari sumber daya komputasi yang dibagi
 - c. Menginfeksi server cloud dengan malware
 - d. Menghapus data secara tidak sah melalui jaringan
 - e. Menyamar sebagai pengguna yang sah untuk mencuri data

b. Esai

Jawablah pertanyaan dibawah ini!

1. Jelaskan mengapa keamanan dalam sistem cloud menjadi hal yang sangat penting untuk diperhatikan!
2. Ancaman pada keamanan cloud mencakup berbagai resiko yang dapat mempengaruhi lingkungan cloud. Terdapat 3 Ancaman Utama yang dihadapi dalam keamanan cloud. Jelaskan ketiga ancaman tersebut!
3. Dalam merancang system keamanan cloud terdapat prinsip desain keamanan yang harus diperhatikan. Jelaskan bagaimana implementasi prinsip security by design!

DAFTAR PUSTAKA

- Armbrust, M., et al. (2010). "A View of Cloud Computing." *Communications of the ACM*, 53(4), 50-58.
- Amazon Web Services. (2021). *Overview of Amazon Web Services*. AWS Whitepapers.
- Bhowmik, Sandeep. (2017). "Cloud Computing". Cambridge University Press, India.
- Buyya, R., Broberg, J., & Goscinski, A. (2011). *Cloud Computing: Principles and Paradigms*. Wiley.
- Cisco Systems. (2020). *Networking Basics: What You Need To Know*. Cisco Networking Academy.
- Erl, T., Puttini, R., & Mahmood, Z. (2013). *Cloud Computing: Concepts, Technology & Architecture*. Prentice Hall.
- 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.
- Hurwitz, J., et al. (2012). *Cloud Computing For Dummies*. Wiley Publishing.
- Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson.
- Marinescu, D. C. (2013). *Cloud Computing: Theory and Practice*. Morgan Kaufmann.
- Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing* (Special Publication 800-145). National Institute of Standards and Technology.
- Raj, P., & Raman, A. C. (2017). *Big Data Analytics and Cloud Computing: Theory, Algorithms and Applications*. Springer.
- Reese, G. (2009). *Cloud Application Architectures: Building Applications and Infrastructure in the Cloud*. O'Reilly Media.

- Smith, J. (2020, August 10). What is cloud computing and how does it work? *TechRadar*. <https://www.techradar.com/news/what-is-cloud-computing>.
- Stallings, W. (2016). *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud*. Pearson Education.
- Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks* (5th ed.). Prentice Hall.
- Velte, A. T., Velte, T. J., & Elsenpeter, R. (2010). *Cloud Computing: A Practical Approach*. McGraw-Hill.

Cloud System

Knowledge Management

Buku ini membahas perkembangan dan konsep komputasi awan (*cloud system* atau *cloud computing*), yang telah mengubah cara individu dan bisnis mengelola data serta layanan teknologi. Dengan cloud, pengguna tidak perlu menyediakan infrastruktur fisik sendiri karena semua layanan bisa diakses melalui internet. Cloud computing menyediakan solusi yang lebih murah, fleksibel, dan efisien dibandingkan dengan sistem komputasi tradisional. Hal ini tercermin dalam tiga lapisan utama komputasi: infrastruktur, platform, dan aplikasi, yang saling terhubung untuk memberikan pengalaman komputasi yang optimal.

Cloud system dibangun di atas berbagai inovasi teknologi, seperti arsitektur mainframe, virtualisasi, dan revolusi komputer pribadi. Perusahaan besar seperti IBM, Amazon, dan Salesforce memainkan peran kunci dalam mengembangkan layanan cloud modern. Evolusi ini mempermudah pengguna untuk mengakses dan menggunakan layanan komputasi sesuai kebutuhan mereka tanpa harus berinvestasi besar dalam infrastruktur.

Buku ini akan menjelaskan konsep dari Cloud System atau Cloud Computing mulai dari sejarah, teknologi enablnya, manfaat dan tantangan, keamanan dan implementasinya. Buku ini juga melampirkan demo penggunaan cloud system pada platform Amazon Web Service.

Disusun Oleh:

Tim Pengampu Mata Kuliah

Dr. Valentino Aris, S.Kom., MM.

Hartoto, S.Pd., M.Pd.

Muh. Qardawi Hamzah, S.Pd., M.Si.

Support By

