RENCANA PEMBELAJARAN SEMESTER GANJIL 2019/2020
PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS ILMU KOMPUTER
UNIVERSITAS ESA UNGGUL

Mata Kuliah	:	Pemrosesan Data Tersebar	**Kode MK**	:	CPD121
Mata Kuliah Prasyarat	:	-	**Bobot MK**	:	3 sks
Dosen Pengampu	:	Hermansyah M.Kom.	**Kode Dosen**	:	7995
Alokasi Waktu	:	14 x E-Learning (Kuliah Daring)			
Capaian Pembelajaran	:	1. Mahasiswa memahami dan Mampu Menerapkan konsep pemrosesan sistem tersebar dalam sebuah kasus sederhana 2. Mahasiswa dapat mengkombinasikan penggunakan manajemen proyek, requirements analysis dan coding ke dalam pemrosesan sistem tersebar.			

SESI	KEMAMPUAN AKHIR	MATERI PEMBELAJARAN	BENTUK PEMBELAJARAN	SUMBER PEMBELAJARAN	INDIKATOR PENILAIAN
1	Mahasiswa mampu memahami kompetensi dasar dan indikator pencapai an mata kuliah Pemrosesan Data Tersebar	Sosialisasi Course Outline dan SAP Ruang Lingkup Pemrosesan Data Tersebar (DDP)	1. *Contextual Instruction (CI)* 2. *Problem Based Learning and Inquiry (PBL)*	1. Munawar, Course Hands Out, 2018	Mahasiswa mampu memahami latar belakang kenapa muncul sistem pemrosesan data tersebar serta bedanya dengan sistem terpusat dengan benar
2	Mahasiswa mampu memahami konsep pemrosesan data tersebar (DDP)	Distributed system (DDP) definition	*1. Contextual Instruction (CI)* *2. Problem Based Learning and Inquiry (PBL)*	1. van Steen ch 1 2. Colouris ch 1	Mahasiswa mampu : •Menjelaskan definisi DDP •Menjelaskan apa

			Media : kelas, komputer, LCD, whiteboard, web		saja yang termasuk kategori DDP serta karakteristiknya dengan benar
3	Mahasiswa mampu memahami arsitektur pada sistem DDP	Distributed system (DDP) definition	*1, Contextual Instruction (CI)* 2. *Problem Based Learning and Inquiry (PBL)* Media : kelas, komputer, *LCD, whiteboard, web*	1. Van Steen ch 1 2 Colouris ch 1	Mahasiswa mampu : • Menjelaskan definisi DDP • Menjelaskan apa saja yang termasuk kategori DDP serta karakteristiknya
4	Mahasiswa mampu memahami proses yang terjadi pada DDP	Processes of DDP	*1. Contextual Instruction (CI)* *2.Problem Based Learning and Inquiry (PBL)* *3.Case Study (CS)* *Media : kelas, komputer, LCD, whiteboard, web*	1. van Steen ch 3 2. Munawar, Course Hands Out, 2018	Mahasiswa dapat memahami proses yang terjadi di DDP dan konsekuensi migrasinya serta dapat mengaplikasikannya pada kasus mereka
5	Mahasiswa memahami mekanisme komunikasi di DDP	Communication in DDP	1. Contextual Instruction (CI) 2.Problem Based Learning and Inquiry (PBL) 3.Case Study (CS)	1. van Steen ch 4 2. Munawar, Course Hands Out, 2018 3. Colouris ch 4	Mahasiswa dapat memahami proses komunikasi yang terjadi antar layer di DDP dan dapat mengaplikasikann

			Media : kelas, komputer, LCD, whiteboard, web		ya dalam kasus mereka
6	Mahasiswa mampu memahami tata cara penamaan dan bagaimana pendistribusiannya di dalam DDP	Naming in DDP	*1 .Contextual Instruction (CI)* *2. Problem Based Learning and Inquiry (PBL)* Media : kelas, komputer, *LCD, whiteboard, web*	1. Contextual Instruction (CI) 2. Problem Based Learning and Inquiry (PBL) 3. Media : kelas, komputer, LCD, whiteboard, web	Mahasiswa dapat memahami penamaan DNS dan hierarki pendistribusiannya di DDP
7	Mahasiswa mampu memahami perlunya sinkronisasi akibat perbedaan posisi letak bumi	Synchronization	*1.Contextual Instruction (CI)* *2.Problem Based Learning and Inquiry (PBL)* *3.Case Study (CS)* Media : kelas, komputer, *LCD, whiteboard, web*	1. van Steen ch 6 2. Munawar, Course Hands Out, 2018	Mahasiswa dapat memahami implementasi sinkronisasi dalam penerapannya ke GPS dan konsekuensi tidak selalu tersedianya bandwith untuk komunikasi
8	Mahasiswa memahami perlunya replikasi pada sistem DDP	Conistency dan Replication	1.*Contextual Instruction (CI)* 2.*Problem Based Learning and Inquiry (PBL)* 3.*Case Study (CS)* 1. Media : kelas, komputer, *LCD, whiteboard, web*	1.van Steen ch 7 2.Munawar, Course Hands Out, 2018 3. Colouris ch 18	Mahasiswa dapat memahami perlunya consistensi dan replikasi dan bagaimana penerapan ke dalam kasus
9	Mahasiswa mampu memahami konsekuensi dari DDP	Fault Tolerance	1. *Contextual Instruction (CI)* 2.*Problem Based*	1.van Steen ch 8 2.Munawar, Course Hands Out, 2018	Mahasiswa menyadari konsekuensi dari

	adalah sistem saling ketergantungan		*Learning and Inquiry (PBL)* 3. *Case Study (CS)* Media : kelas, komputer, *LCD, whiteboard, web*		sistem saling ketergantungan akan berakibat kepada ketersediaan, keandalan, keamanan dan pemeliharaan sistem. Oleh karenanya perlu pengetahuan untuk antisipasi
10	Mahasiswa mampu memahami ancaman dan mekanisme pencegahan di sistem DDP	Security	1. Contextual Instruction (CI) 2. Problem Based Learning and Inquiry (PBL) 3. Case Study (CS) 4. Media : kelas, komputer, LCD, whiteboard, web	1.van Steen ch 9 2.Munawar, Course Hands Out, 2018 3. Colouris ch 11	Mahasiswa memahami berbagai macam ancaman di sistem DDP dan memahami penggunaan beberapa tool keamanan untuk pencegahan
11	Mahasiswa mengerti konsep obyek sistem terdistribusi dan mekanisme komunikasi diantara mereka	Distributed Object System	1. *Contextual Instruction (CI)* 2. *Problem Based Learning and Inquiry (PBL)* 3. *Case Study (CS)* 4. Media : kelas, komputer, *LCD,*	1. Van Steen ch 10 2. Munawar, Course Hands Out, 2018 3. Colouris ch 8	Mahasiswa mengerti konsep obyek terdistribusi dan mekanisme replikasi dan komunikasi diantara mereka.

			whiteboard, web		
12	Mahasiswa memahami mekanisme pertukaran file pada sistem DDP	Distributed File System	1. *Contextual Instruction (CI)* 2. *Problem Based Learning and Inquiry (PBL)* 3. *Case Study (CS)* Media : kelas, komputer, *LCD, whiteboard, web*	1. van Steen ch 11 2. Munawar, Course Hands Out, 2018 3. Colouris ch 12	Mahasiswa memahami beberapa teknik pertukaran file pada beberapa arsitektur sistem DDP
13	Mahasiswa memahami mekanisme komunikasi di sistem web pada DDP	Distributed Web System	1. *Contextual Instruction (CI)* 2. *Problem Based Learning and Inquiry (PBL)* 3. *Case Study (CS)* Media : kelas, komputer, *LCD,*	1.Van Steen ch 11 2. Munawar, Course Hands Out, 2018 3. Colouris ch 12	Mahasiswa memahami konsep client side, server side dan mekanisme komunikasi di sistem web pada DDP
14	Mahasiswa dapat memahami mekanisme koordinasi dan mengimplementasikan sistem DDP ke dalam kasus nyata	DIst Koordinasi in DDP Presentasi Tugas	1. *Contextual Instruction (CI)* 2. *Problem Based Learning and Inquiry (PBL)* 3. *Case Study (CS)* Media : kelas, komputer, *LCD, whiteboard, web*	1. Munawar, Course Hands Out, 2018	Mampu mengimplementasikan berbagai sistem DDP pada kasus nyata

EVALUASI PEMBELAJARAN

SESI	PROSE-DUR	BEN-TUK	SEKOR ≥ 77 (A / A-)	SEKOR ≥ 65 (B- / B / B+)	SEKOR ≥ 60 (C / C+)	SEKOR ≥ 45 (D)	SEKOR < 45 (E)	BOBOT

1	*Progress test* dan *Post test* (UTS)	Tes lisan	Menjelaskan 2 atau lebih indikator penilaian dengan benar	Menjelaskan 2 indikator penilaian dengan benar	Menjelaskan 1 indikator penilaian dengan benar	Menjelaskan 1 atau lebih indikator penilaian secara kurang tepat	Tidak mampu menjelaskan 1 indikator penilaian	5 %
2	*Post test* (UTS dan tugas *online*)	Tes tulisan	Menguraikan 2 atau lebih indikator penilaian dengan benar	Menguraikan 2 indikator penilaian dengan benar	Menguraikan 1 indikator penilaian dengan benar	Menguraikan 1 atau lebih indikator penilaian secara kurang tepat	Tidak mampu menguraikan 1 indikator penilaian	5 %
3	*Post test* (UTS dan tugas *online*)	Tes tulisan	Menganalisis 2 atau lebih indikator penilaian dengan benar	Menganalisis 2 indikator penilaian dengan benar	Menganalisis 1 indikator penilaian dengan benar	Menganalisis 1 atau lebih indikator penilaian secara kurang tepat	Tidak mampu menganalisis 1 indikator penilaian	5 %
4	*Post test* (UTS dan tugas *online*)	Tes tulisan	Menngidentifikasi 2 atau lebih indikator penilaian dengan benar	Menngidentifikasi 2 indikator penilaian dengan benar	Menngidentifikasi 1 indikator penilaian dengan benar	Menngidentifikasi 1 atau lebih indikator penilaian secara kurang tepat	Tidak mampu menngidentifikasi 1 indikator penilaian	5 %
5	*Post test* (Tugas dan tugas *online*)	Tes tulisan	Menyimpulkan 2 atau lebih indikator penilaian dengan benar	Menyimpulkan 2 indikator penilaian dengan benar	Menyimpulkan 1 indikator penilaian dengan benar	Menyimpulkan 1 atau lebih indikator penilaian secara	Tidak mampu menyimpulkan 1 indikator penilaian	10 %

						kurang tepat		
6	*Post test* (UTS dan tugas *online*)	Tes tulisan	Menggambarkan 2 atau lebih indikator penilaian dengan benar	Menggambarkan 2 indikator penilaian dengan benar	Menggambarkan 1 indikator penilaian dengan benar	Menggambarkan 1 atau lebih indikator penilaian secara kurang tepat	Tidak mampu menggambarkan 1 indikator penilaian	10 %
7	*Progress test* dan *Post test* (UTS dan tugas *online*)	Tes tulisan	Mengidentifikasi 2 atau lebih indikator penilaian dengan benar	Mengidentifikasi 2 indikator penilaian dengan benar	Mengidentifikasi 1 indikator penilaian dengan benar	Mengidentifikasi 1 atau lebih indikator penilaian secara kurang tepat	Tidak mampu mengidentifikasi 1 indikator penilaian	10 %
8	*Post test* (UAS dan tugas *online*)	Tes tulisan	Menyusun 2 atau lebih indikator penilaian dengan benar	Menyusun 2 indikator penilaian dengan benar	Menyusun 1 indikator penilaian dengan benar	Menyusun 1 atau lebih indikator penilaian secara kurang tepat	Tidak mampu menyusun n 1 indikator penilaian	5 %
9	*Post test* (UAS dan tugas *online*)	Tes tulisan	Membuat 2 atau lebih indikator penilaian dengan benar	Membuat 2 indikator penilaian dengan benar	Membuat 1 indikator penilaian dengan benar	Membuat 1 atau lebih indikator penilaian secara kurang tepat	Tidak mampu membuat indikator penilaian	5 %
10	*Post test* (UAS	Tes tulisan	Menjelaskan 2 atau lebih indikator	Menjelaskan 2 indikator	Menjelaskan 1 indikator	Menjelaskan 1 atau lebih	Tidak mampu menjelaskan	5 %

	dan tugas *online*)		penilaian dengan benar	penilaian dengan benar	penilaian dengan benar	indikator penilaian secara kurang tepat	1 indikator penilaian	
11	*Post test* (UAS dan tugas *online*)	Tes tulisan	Merumuskan 2 atau lebih indikator penilaian dengan benar	Merumuskan 2 indikator penilaian dengan benar	Merumuskan 1 indikator penilaian dengan benar	Merumuskan 1 atau lebih indikator penilaian secara kurang tepat	Tidak mampu merumuskan 1 indikator penilaian	5 %
12	*Post test* (UAS dan tugas *online*)	Tes tulisan	Menyusun 2 atau lebih indikator penilaian dengan benar	Menyusun 2 indikator penilaian dengan benar	Menyusun 1 indikator penilaian dengan benar	Menyusun 1 atau lebih indikator penilaian secara kurang tepat	Tidak mampu menyusun 1 indikator penilaian	10 %
13	*Post test* (Tugas dan tugas *online*)	Tes tulisan	Membuat 2 atau lebih indikator penilaian dengan benar	Membuat 2 indikator penilaian dengan benar	Membuat 1 indikator penilaian dengan benar	Membuat 1 atau lebih indikator penilaian secara kurang tepat	Tidak mampu membuat indikator penilaian	10 %
14	*Post test* (UAS dan tugas *online*)	Tes tulisan	Menggambarkan 2 atau lebih indikator penilaian dengan benar	Menggambarkan 2 indikator penilaian dengan benar	Menggambarkan 1 indikator penilaian dengan benar	Menggambarkan 1 atau lebih indikator penilaian secara kurang tepat	Tidak mampu menggambarkan 1 indikator penilaian	10 %

KOMPONEN PENILAIAN	
Kelas regular	Kelas parallel
1. Kehadiran : 10% 2. UTS : 30 % 3. UAS : 40% 4. Tugas : 20%	1. UTS : 30 % 2. UAS : 30% 3. Tugas-kuis : 20% 4. Tugas-online 20%

VERIFIKASI RPS	
	Jakarta, 11 Januari 2021
Mengetahui, Ketua Program Studi,	Dosen Pengampu,
M.Bahrul Ulum, S.Komm M.Kom.	Hermansyah M.Kom.

MODUL PMROSESAN DATA TERSEBAR

(PTI 611)

MODUL SESI 1.

PENGANTAR SISTEM TERDISTRIBUSI DAN OVERVIEW

DISUSUN OLEH

HERMANSYAH, SKom, M.Kom.

UNIVERSITAS ESA UNGGUL

2020

PENGANTAR SISTEM TERDISTRUSI DAN OVERVIW

A. Kemampuan Akhir Yang Diharapkan

http://repository.fue.edu.eg/xmlui/handle/123456789/3526

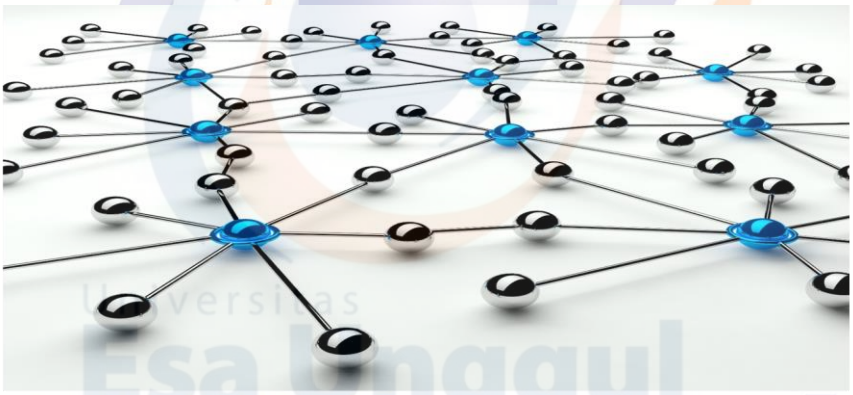
Setelah mempelajari modul ini, diharapkan mahasiswa mampu :

1. Mengertidan memahami pengertian dari PDT
2. Mengerti dan memahami Perbedaan antara jaringan computer dengan PDT
3. Mngerti dan Memahami Jenis-jenis dari PDT.

B. Uraian dan Contoh

1. Pengantar dan Overiew Pengolaan Data Terdistribusi

JARINGAN KOMPUTER VS PDT



Pengantar Sistem Terdistribusi & Overview

Jaringan Komputer adalah :

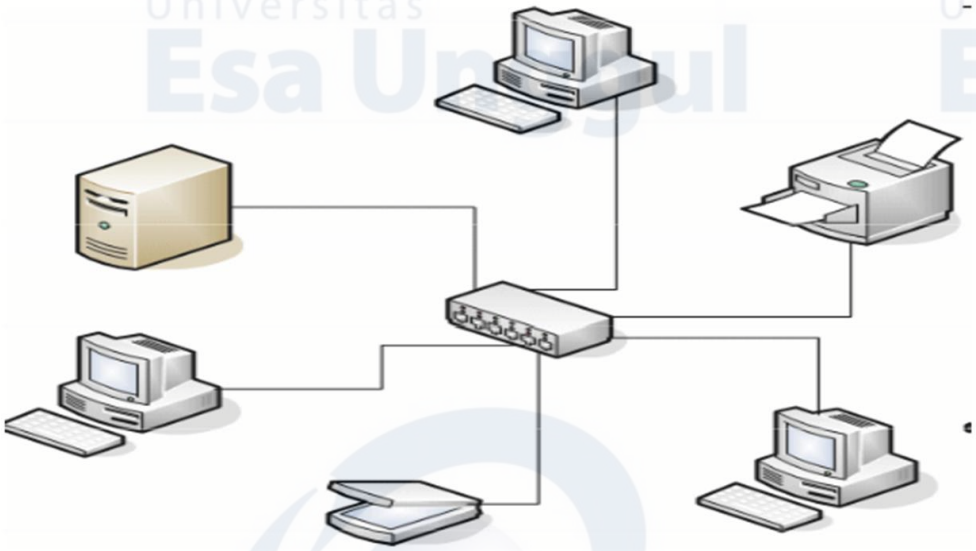
: Komputer otonom yang secara eksplisit terlihat (secara eksplisit teralamati)

- Dengan IP address masing-masing komputer

• **Sistem terdistribusi** : keberadaan beberapa komputer otonom bersifat transparan, sebagai satu kesatuan. (Tanembaum)

• Secara normal, setiap sistem terdistribusi mengandalkan layanan yang disediakan oleh jaringan komputer Berbasis TCP/IP

Jaringan komputer

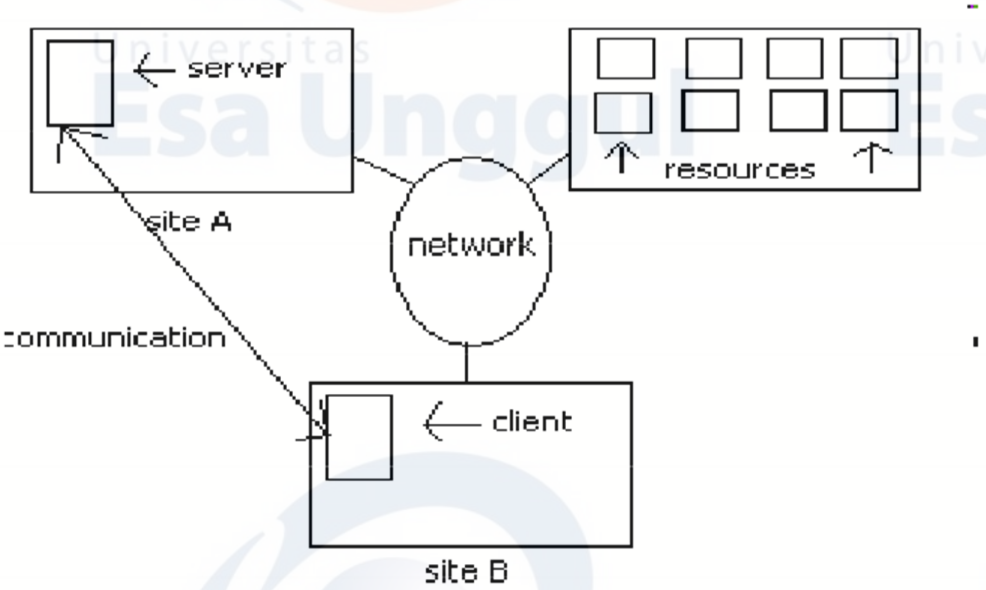


Sistem Terdistribusi

Satu sistem dimana beberapa komputer pada jaringan saling berkomunikasi, berkoordinasi, dan bekerja sama dengan cara saling bertukar pesan (messages)

- Komputer-komputer saling independen
• Memiliki memori dan prosesor sendiri
- Dihubungkan dalam jaringan komputer
• LAN / WAN
- Terlihat sebagai satu kesatuan
- Komputasi terintegrasi
- Dapat diterapkan pada middleware (Tanembaum

Ilustrasi



Scalability problems

(kemampuan untuk meningkatkan kinerja sistem)

Centralized services: single service for all requests

• Centralized data: single data point for all services

• Centralized algoritms: single computation for all requests

Contoh SistemTerdistribusi

• Internet = Interconnection Network

• Intranet Coorporation

• Mobile Computing

• Automated banking systems

• Tracking roaming cellular phones

• Global positioning systems

• Retail point-of-sale terminals

• Air-traffic control

Intranet

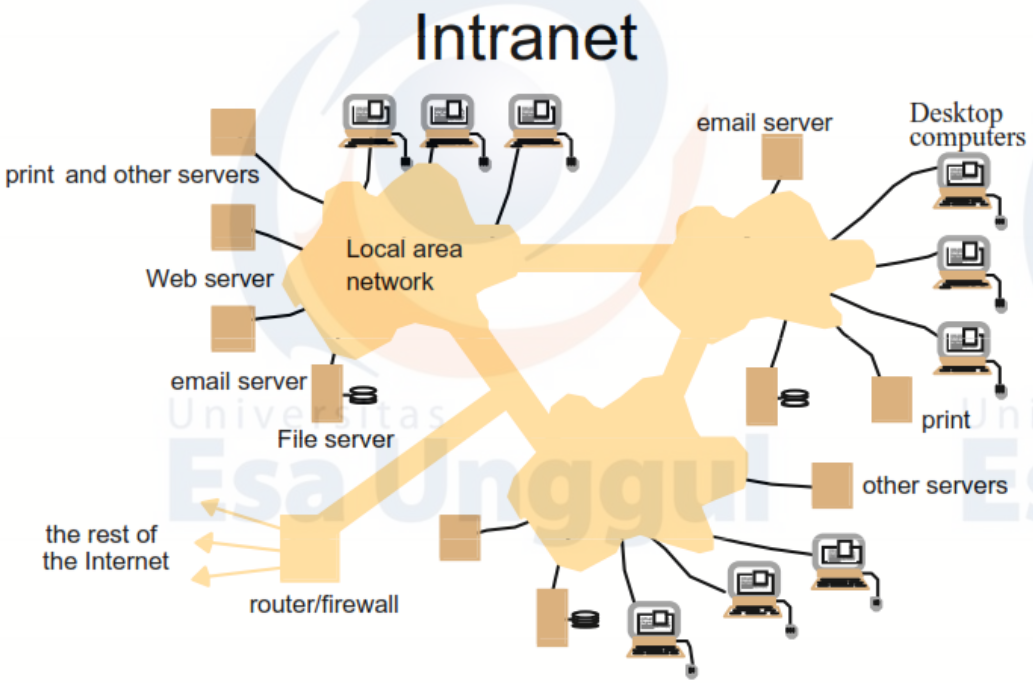
Intranet adalah sebuah jaringan privat yang menggunakan protokol-protokol Internet (TCP/IP), untuk membagi informasi rahasia perusahaan atau operasi dalam perusahaan tersebut kepada karyawannya.

• Bersifat internal (cth: web internal)

• Untuk membangun sebuah intranet, maka sebuah jaringan haruslah memiliki beberapa komponen yang membangun Internet, yakni protokol Internet (Protokol TCP/IP, alamat IP, dan protokol lainnya), klien dan juga server.

• Biasanya proprietary

• Terhubung ke internet (melalui firewall)



Uraian sub topik ke-1

2. Sistem Terdisribusi Multi Media

Sistem Terdistribusi Multimedia

Biasanya digunakan pada infrastruktur Internet

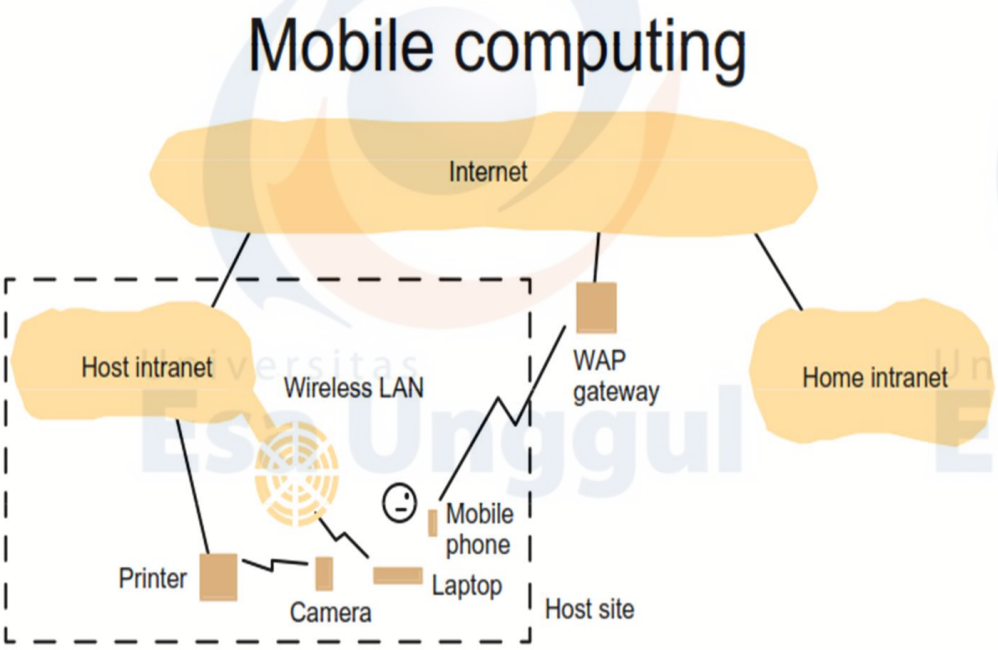
• Karakteristik

- Sumber data yang heterogen dan memerlukan sinkronisasi secara real time
- Video, audio, text
- Multicast (UDP based)
- Contoh:

• Teleteaching tools

• Video-conferencing

• Video and audio on demand



ATM

• Mesin ATM ada di cabang-cabang bank

• Klien dapat mengakses pada saat yg simultan bersamaan

- Mekanisme deadlock & sinkronisasi

• Sistem ATM akan menggunakan central-central office terdekatnya

- Relay mode

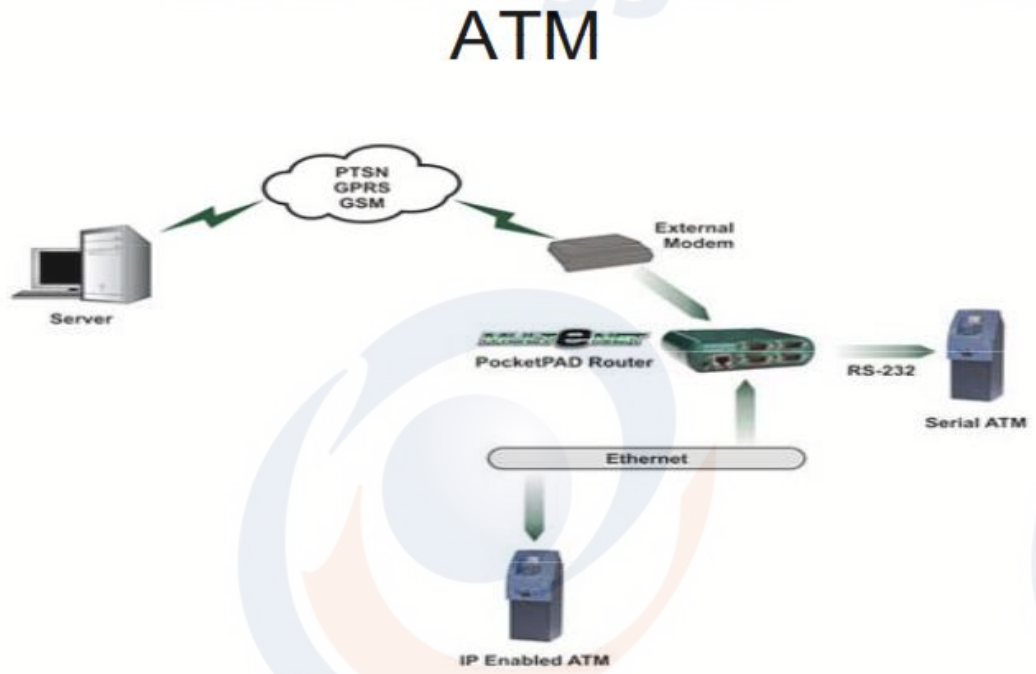
• Setiap central office akan menjadi backup bagi yang

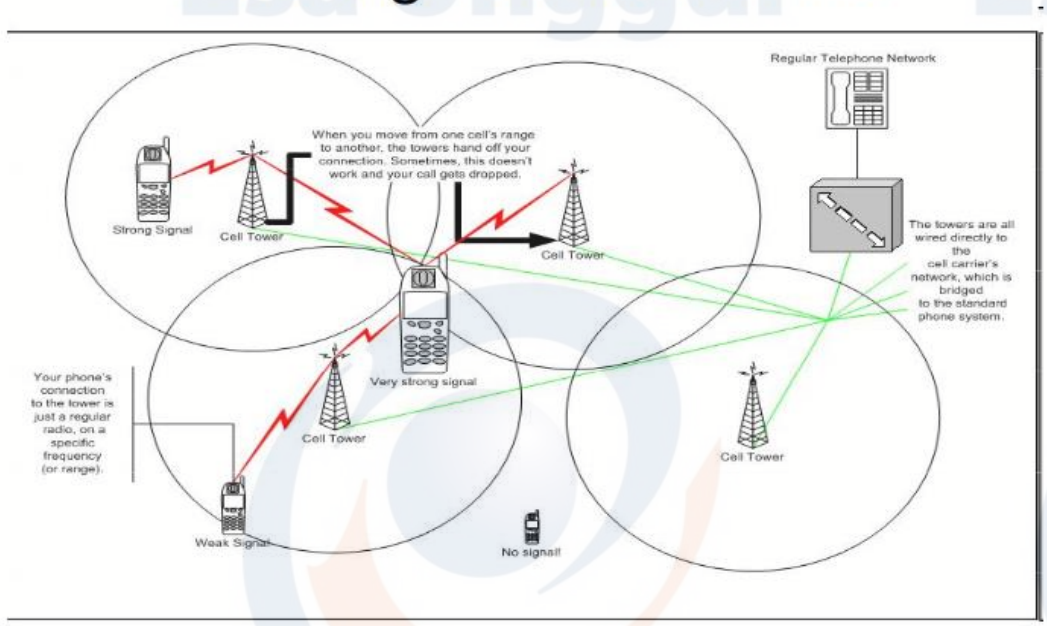
lainnya

- Replication

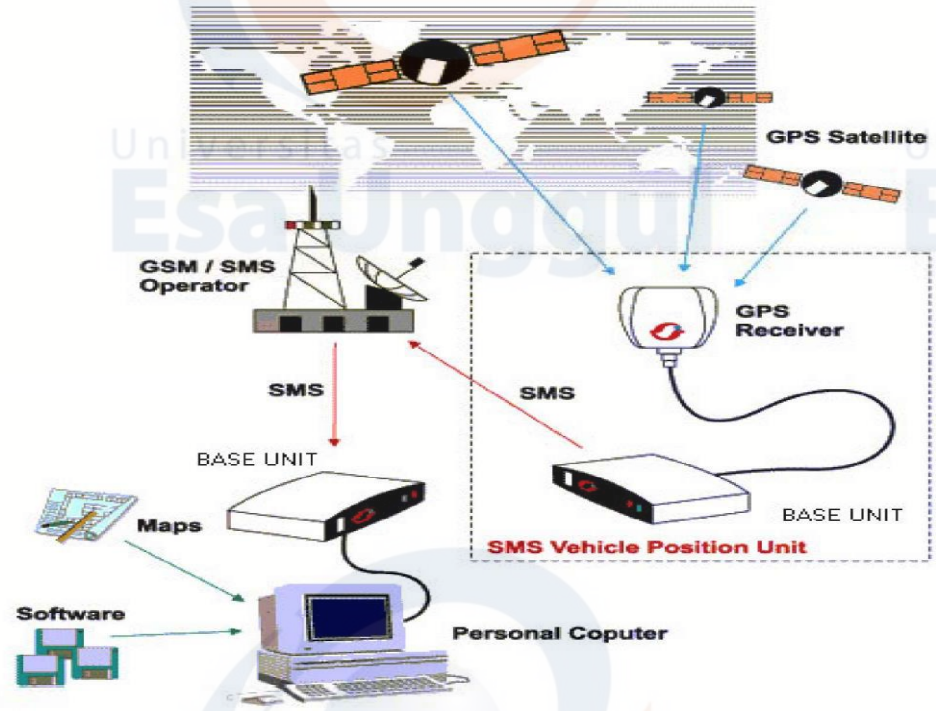
• Bagaimana menghandle transasksi? Keamanan? Network failure?

- Security





-



Contoh Sistem Terdistribusi yang lain

- • Sistem telepon
- - ISDN, PSTN
- • Manajemen jaringan
- - Administrasi resource jaringan
- • Network File System (NFS)
- - Arsitektur untuk mengakses sistem file melalui jaringan
- • WWW
- - Arsitektur client/server tebuka yang diterapkan di atas infrastruktur internet
- - Shared resources (melalui URL)

Alasan Sistem Terdistribusi

- • Resources sharing: sumber daya dapat digunakan secara bersama / bergantian
- • Distribusi fungsi: komputer memiliki kemampuan fungsi yang berbeda-beda

- - client/server
- - Host/terminal
- - Data gathering / data processing
- • Distribusi beban/keseimbangan :
- pemberian tugas ke prosesor secukupnya sehingga unjuk kerja seluruh sistem teroptimasi.

• Replikasi kekuatan pemrosesan : independent processors bekerja untuk pekerjaan yang sama

- Sistem terdistribusi terdiri dari kumpulan mikrokomputer yang memiliki kekuatan pemrosesan yang tidak dapat dicapai oleh superkomputer

- Mis: 10.000 CPU, masing-masing berjalan pada 50 MIPS (**Microprocessor without Interlocked Pipeline Stages)**, mencapai 500.000 MIPS,

- Maka satu perintah dijalankan dalam waktu 0.002 nsec

• Reliability : dalam sistem terdistribusi, apabila sebuah situs mengalami kegagalan, maka situs yang tersisa dapat melanjutkan operasi yang sedang berjalan. Hal ini menyebabkan reliabilitas sistem menjadi lebih baik.

- • Pemisahan fisik : sistem yang menggantungkan pada fakta bahwa komputer secara fisik terpisah (e.g., untuk mencapai kehandalan).
- • Ekonomis : kumpulan mikroprosesor menawarkan harga/unjuk kerja yang lebih baik dari pada mainframe
- • Fleksibilitas : komputer yang berbeda dengan kemampuan yang berbeda dapat di share antar user

Kesulitan

- • Software - bagaimana merancang dan mengatur software dalam Sistem Terdistribusi
- • Ketergantungan pada infrastruktur jaringan (world wide web
- • Kemudahan akses ke data yang di share, memunculkan masalah keamanan

Karakteristik Sistdm Terdistribusi

• **Concurrency** : Beberapa komputer dapat berjalan sekaligus dengan tugas yang berbeda

- Sinkronisasi dan koordinasi dengan message passing
- Sharing resources

• Contoh : WEB diakses oleh banyak orang

- Masalah umum dalam sistem concurrent

• Deadlock

• Komunikasi yang tidak handal

- **No global clock** : Pada sistem terdistribusi, tidak ada satu proses tunggal yang mengetahui global state sistem saat ini (disebabkan oleh concurrency)
- - Hal ini menyebabkan kesulitan dalam mensinkronkan waktu seluruh omputer/perangkat yang terlibat
- • **Independent failure** : kegagalan komputer/jaringan bisa terjadi kapan saja
- - Setiap komponen/perangkat dapat mengalami kegagalan namun komponen/perangkat lain tetap berjalan dengan baik.

Uraian sub topik ke-2

3. Tantangan Sistem Terdistribusi

Tantangan Sistem Terdistribusi

- • Heterogenity :
- - Infrastruktur jaringan
- - Hardware dan software (sistem operasi, perbedaan UNIX socket dan Winsock)
- - Bahasa pemrograman

- - Solusi: Perlu ada protokol yang standar, Middleware contoh : CORBA (Common Object Request Broker Architecture), Kode program universal, contoh : JAVA
- • Scalability : Sistem tetap efektif meskipun terdapat peningkatan resource dan pengguna secara signifikan

Tantangan

• **Openness**

- Memastikan sistem dapat diperluas dan mudah dalam pemeliharaan

• Mengikuti standard antarmuka

• Solusi: Adanya publikasi dari spesifikasi (RFC)

• **Security**

- Confidentiality (pencegahan terhadap hak akses oleh orang yang tidak berhak)

- Integrity (pencegahan terhadap perubahan data)

- Availability (pencegahan terhadap masalah ketersediaan, misalnya mencegah DDOS)

- • **Menghandle Kegagalan** : Kesalahan/Kegagalan bisa ditemukan/diperbaiki A.S.A.P dan mampu melakukan proses recovery
- - Pendeteksian, Toleransi dan Redudancy
- - Solusi: Replikasi, Load Balancing, Backup
- • **Konkurensi** : Banyak client yang mengakses banyak data dalam waktu yang bersamaan, sedangkan data harus tetap konsisten!
- - Menghindari masalah deadlock

Transparansi

- Transparency : Sistem terlihat sebagai satu kesatuan, bukan gabungan dari beberapa komponen
- Access transparency : memungkinkan resource lokal/ remote untuk diakses menggunakan operasi yg sama (tidak berbeda-beda)
- Location transparency : memungkinkan resources untuk diakses tanpa pengetahuan ttg jaringan fisik/lokasi (lokasi dan IP address).

- Concurrency transparency : memungkinkan beberapa proses untuk beroperasi secara konkuren menggunakan shared resources tanpa "mengganggu" mereka.
- Replication transparency : memungkinkan multiple instances dari resources untuk digunakan menaikan reliability dan performance tanpa pengetahuan pemrograman replikasi.

- **Failure transparency** : memungkinkan penyembunyian kegagalan, memperbolehkan users dan program aplikasi untuk menyelesaikan tugas mereka walaupun ada kegagalan komponen hardware / software.
- **Mobility transparency** : memungkinkan perubahan resources dan clients didalam sistem tanpa berefek pada operasi user dan program.
- **Performance transparency** : Memungkinka sistem untuk dikonfigurasi ulang untuk meningkatkan performa yang berubah secara cepat.
- **Scaling transparency** : memperbolehkan sistem dan aplikasi untuk diperluas tanpa mengubah struktur sistem atau algoritma aplikasi.

Pengembangan Lebih lanjut

- • Distributed Database
- - A logically interrelated collection of shared data (and a description of this data), physically
- distributed over a computer network
- - Penyimpanan data bisa dilakukan secara terdistribusi (tidak lagi tersentralisasi)
- - Menggunakan Replikasi dan Fragmentasi
- • Distributed Processing
- - Menggunakan RMI, RPC, atau .NET Remoting
- • Distributed Transactions

Distributed programming paradigms

• Client/server model

• Remote procedure calls

• Distributed File Systems
• Group communication and multicasts
• Distributed transactions
• Distributed object-based systems
• Publish-subscribe model
• Peer-to-peer model
• The Web

Uraian sub topik ke-n

C. Latihan

a. Apa perbedaan antara Jaringan Kompuetr dengan Pemrosesan Data Tersebar
b. Sebutkan contoh-contoh Pemrosesan Data Tersebar..?
c. Sebutkan Tantangan tantangan pada pemrosesan data tersebar.

D. Kunci Jawaban

a. Jawaban latihan soal ke-1

Perbedaan antara Jaringan komputer dengan pemrosesandata tersebar :

Jaringan Komputer adalah :

: Komputer otonom yang secara eksplisit terlihat (secara eksplisit teralamati)

- Dengan IP address masing-masing computer.

b. Jawaban latihan soal ke-2

Contoh contoh Pemrosesan Data Tesebar diantaranya :

- Jaringan Internet
- Jaringan Intranet
- Jaringan ekstranet
- Banking system
- Dll

c. Jawaban latihan soal ke-n

Tantangan dalamiplemnetasi Pemrosesan Data tersebar

- Heterogenity :
- - Infrastruktur jaringan
- - Hardware dan software (sistem operasi, perbedaan UNIX socket dan Winsock)
- - Bahasa pemrograman
- - Solusi: Perlu ada protokol yang standar, Middleware contoh : CORBA (Common Object Request Broker Architecture), Kode program universal, contoh : JAVA
- • Scalability : Sistem tetap efektif meskipun terdapat peningkatan resource dan pengguna secara signifikan

E. Daftar Pustaka

1. Couloris et. al. 2012. Distributed Systems Concepts and Design, Fifth Edition. Addison Wesley.
2. Van Steen and Tanenbaum, 2017. Distributed Systems: Prinsiples and Paradigms. 3e. Prentice-Hall

Link Jornal :

- https://ieeexplore.ieee.org/abstract/document/1646676
- https://komputasi.files.wordpress.com/2018/03/mvsteen-distributed-systems-3rd-preliminary-version-3-01pre-2017-170215.pdf

MODUL PEMROSESAN DATA TERSEBAR

(FTI 611)

MODUL SESI 2

DEFINISI PEMROSESAN DATA TERSEBAR

DISUSUN OLEH

HERMANSYAH S.Kom., M.Kom.

UNIVERSITAS ESA UNGGUL

2020

DEFINISI PEMROSESAN DATA TERSEBAR

A. Kemampuan Akhir Yang Diharapkan

Setelah mempelajari modul ini, diharapkan mahasiswa mampu :

1. Memahami dan mengerti Konsep Pemrosesan Data Tersebar
2. Memahami dan mengerti contoh implementasi DDP…?
3. Memahami Sistem Sensor pada DDP

B. Uraian dan Contoh

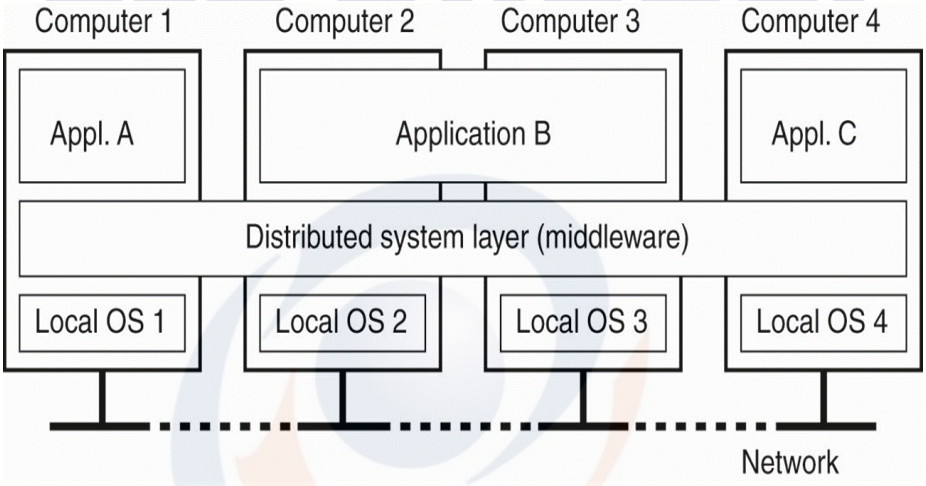
1. Definisi DDP...,,,?

Distributed Data Processing Definition

A distributed system is:

Cara untuk mempercepat pengolahan data atau informasi dengan mendistribusikan pekerjaan atau intruksi ke banyak komputer yang telah dipilih untuk memberi kekuatan pemrosesan yang lebih cepat.

Figure 1-1. Sistem terdistribusi yang diselenggarakan sebagai middleware. Lapisan middleware meluas ke beberapa mesin, dan menawarkan setiap aplikasi antar muka yang sama.



Tujuan dari komputasi terdistribusi

Adalah menyatukan kemampuan dari sumber daya (sumber komputasi atau sumber informasi) yang terpisah secara fisik, ke dalam suatu sistem gabungan yang terkoordinasi dengan kapasitas yang jauh melebihi dari kapasitas individual komponen-komponennya.

Scalability Problems

Concept	Example
Centralized services	A single server for all users
Centralized data	A single on-line telephone book
Centralized algorithms	Doing routing based on complete information

Figure 1-2. Examples of scalability limitations.

Akses : menyembunyikan perbedaan dalam representasi data dan suber daya yang rendah.

Lokasi : Sumber Daya yang tersembunyi

Migration : sumber Daya dapat berindah dari suatu lokasi ke lokasi yang lain secara tersembunyi

Relocation : secara tersembunyi Sumber daya dapat dpindahkan ke lokasi saad sedang digunakan.

Replication : Menyebunyikan sumber daya

Concurancy lain : menyembunyikan bahwa sumber daya dapat dibagikan oleh beberapa pengguna kompotitif

Failure ; Menyembunyikan kegagalan dan pemulihan sumber daya

Scalability Problems

Karekteristik dari Algoritma Desentralisasi

>Tidak ada mesin yang memiliki informasi lengkap tentang Mesin

>Mesin biasanya menbuat keoutusan hanya berdasarkan informasi lokal

>Kegagalan satu mesin tidak merusak algoritma anda

>tidak ada asumsi secara implisit bahwa ada jam secara global

Scaling Techniques (1)

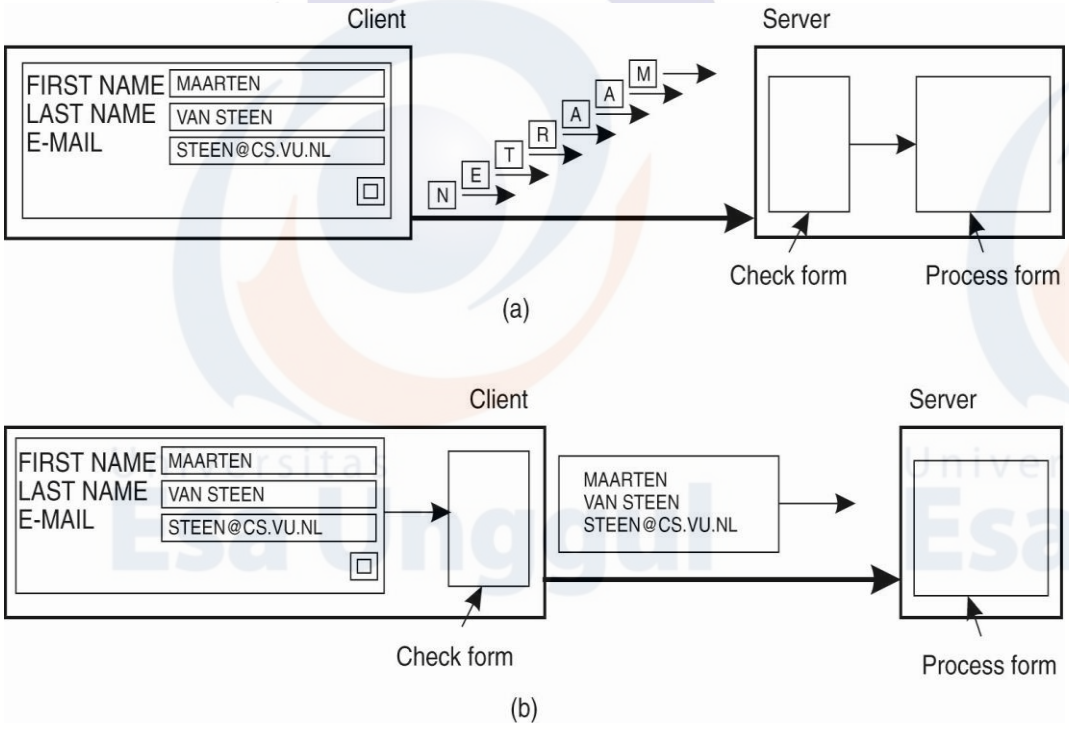


Figure 1-4. The difference between letting (a) a server or (b) a client check forms as they are being filled.

Scaling Techniques (2)

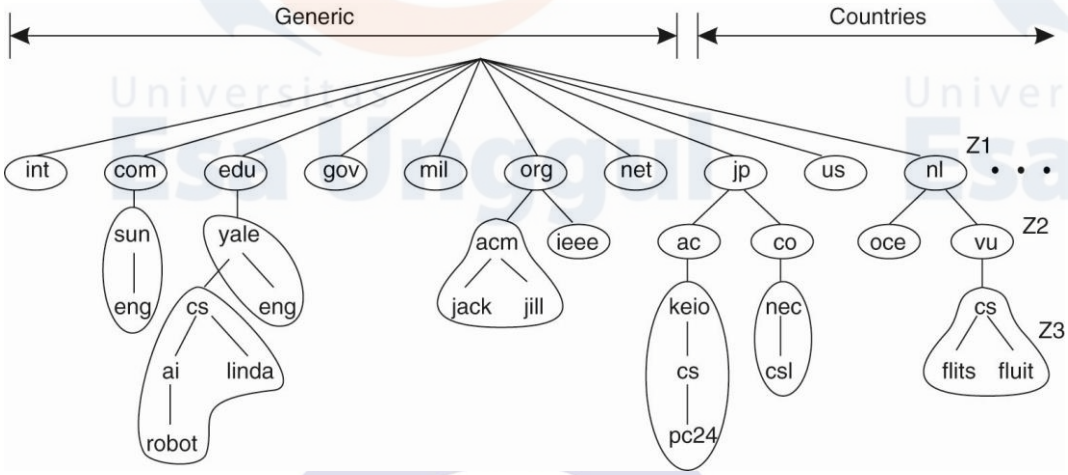


Figure 1-5. An example of dividing the DNS name space into zones.

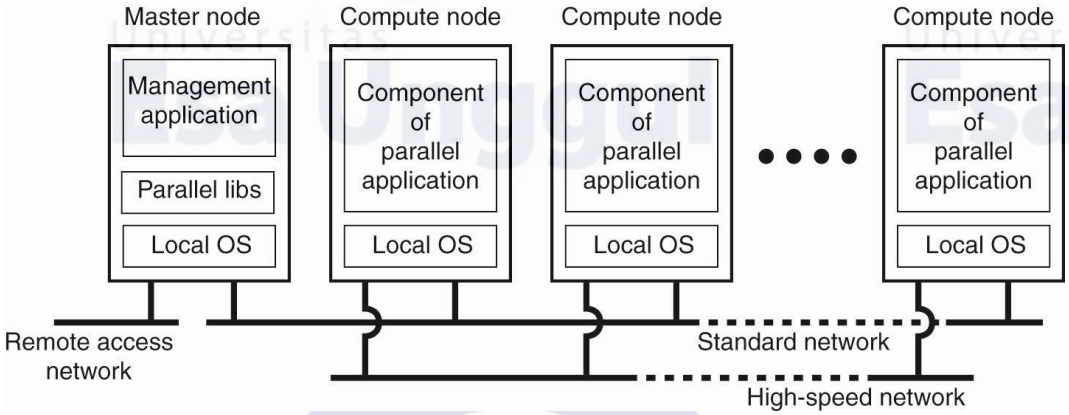
Pitfalls when Developing Distributed Systems

Jebakan saat Mengembangkan Sistem Terdistribusi:

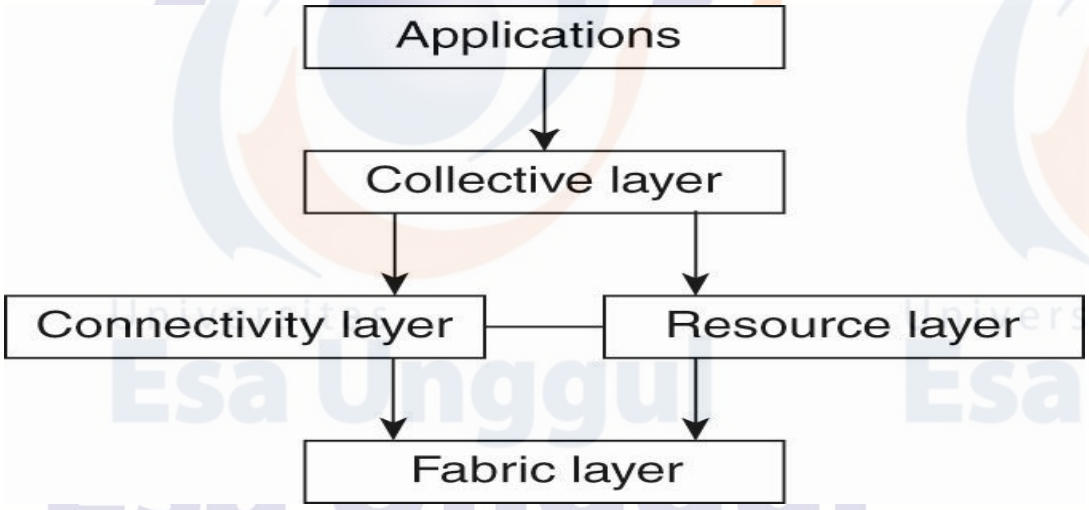
Ada beberapa hal dalam pengembangan Sistem Terdistribusi yag dapat menyebabkan anda terjebak dalam beberapa hal yang mungkin saja menjadikan kendala bagi anda nantinya ntuk itu anda perlu memperhatikan hal hal berikut :

- Jaringan yang handal
- Jaringan yang Aman.
- Jaringannya homogen.
- Topologi tidak berubah.
- Latensi adalah no
- Bandwidth tidak terbatas
- Biaya transportasi nol
- Ang yAda satu administrator.

Cluster Computing Systems



Grid Computing Systems



Transaction Processing Systems (1)

Figure 1-8. Example primitives for transactions.

Primitive	Description
BEGIN_TRANSACTION	Mark the start of a transaction
END_TRANSACTION	Terminate the transaction and try to commit
ABORT_TRANSACTION	Kill the transaction and restore the old values
READ	Read data from a file, a table, or otherwise
WRITE	Write data to a file, a table, or otherwise

Transaction Processing Systems (2)

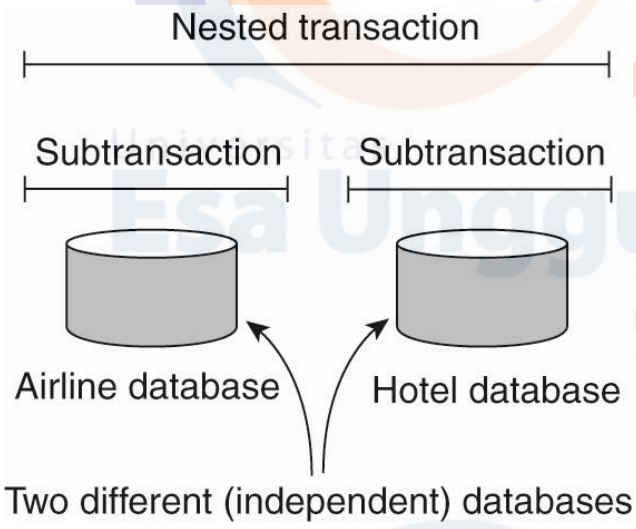
Sifat karakteristik transaksi :

- Atomic: Bagi dunia luar, transaksi itu terjadi secara terpisah.
- Consistent: Transaksi tidak melanggar invarian sistem

Isolated: Transaksi bersamaan tidak saling mengganggu

Durable: Setelah transaksi dilakukan, perubahan itu bersifat permanen.

Transaction Processing Systems (3)



Transaction Processing Systems (4)

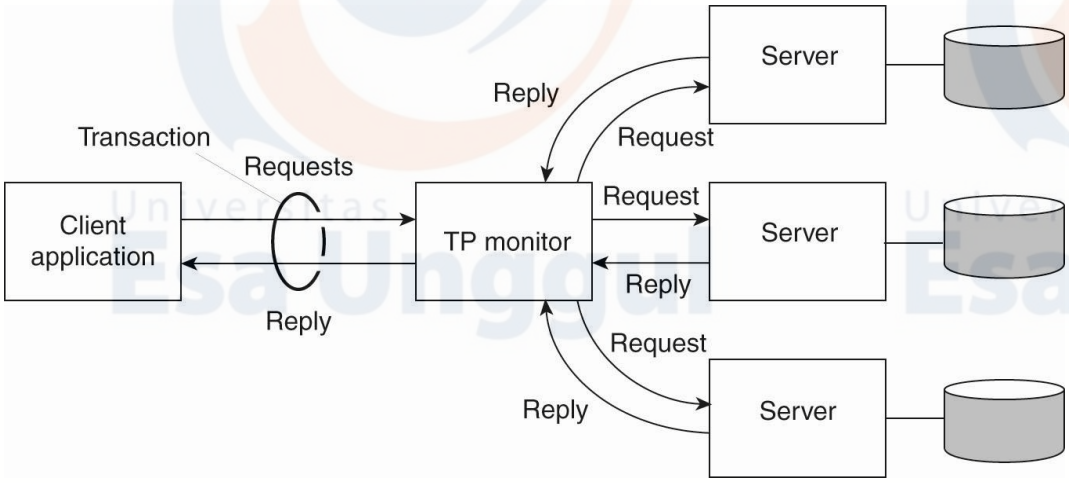
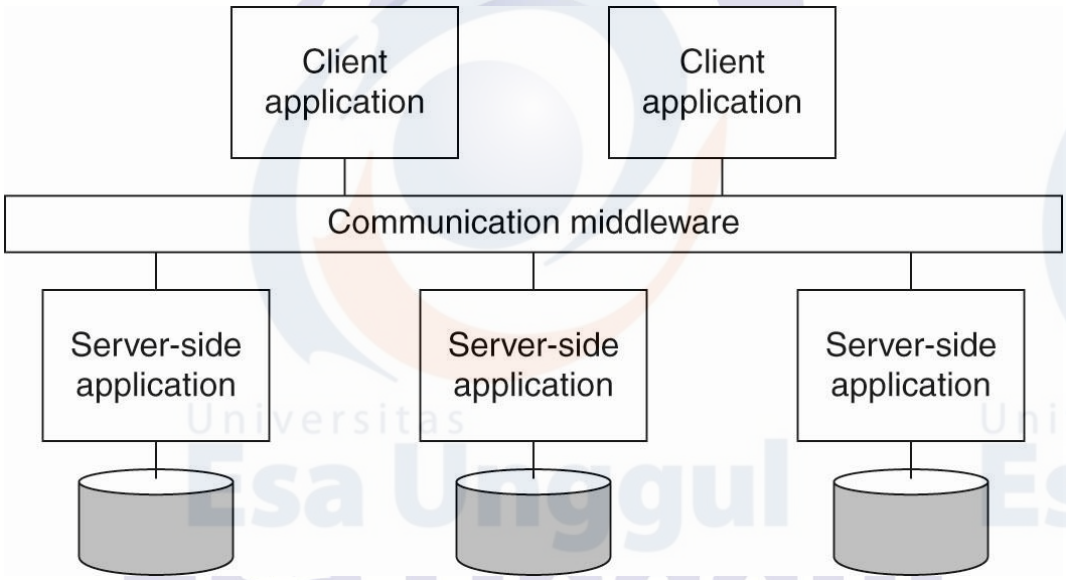


Figure 1-10. The role of a TP monitor in distributed systems.

Enterprise Application Integration



Uraian sub topik ke-1

2. Sub sub topik ke-2

Distributed Pervasive Systems

Requirements for pervasive systems

.Rangkulah perubahan kontekstual

- Dorong komposisi ad hoc.
- Mengakui berbagi sebagai default.

Electronic Health Care Systems (1)

Pertanyaan yang harus diajukan untuk sistem perawatan kesehatan:

- Di mana dan bagaimana data yang dipantau disimpan
- Bagaimana kita bisa mencegah hilangnya data penting?
- Infrastruktur apa yang dibutuhkan untuk menghasilkan dan menyebarkan peringatan?
- Bagaimana dokter dapat memberikan umpan balik online?

Bagaimana ketahanan ekstrim dari sistem pemantauan dapat direalisasikan?

Masalah keamanan dan bagaimana kebijakan yang tepat dapat ditegakkan?

Electronic Health Care System

Figure 1-12. Monitoring a person in a pervasive electronic health care system, using (a) a local hub or

(b) a continuous wireless connection

Jaringan Sensor

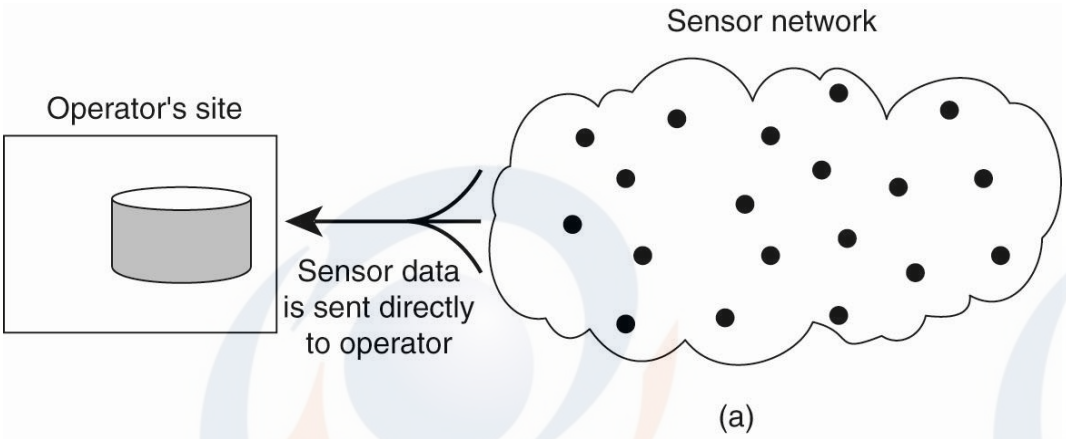
Pertanyaan tentang sensor network

- Bagaimana kita (secara dinamis) mengatur pohon efisien dalam jaringan sensor?

. agregasi hasil terjadi? Bisakah itu dan Bagaimana ikendalikan?

- Apa yang terjadi ketika tautan jaringan gagal?

Sensor Networks (2)



Sensor Networks (3)

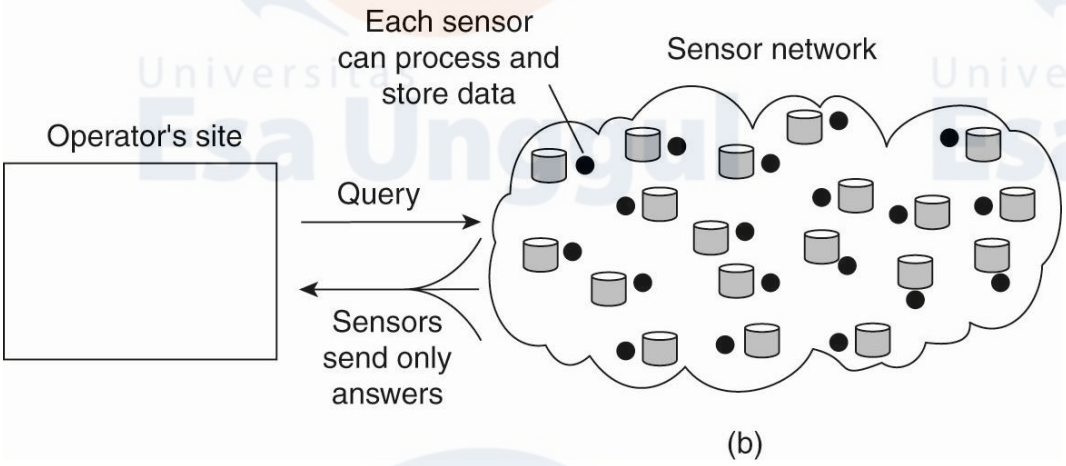


Figure 1-13. Organizing a sensor network database, while storing and processing data … or (b) only at the sensors.

Jaringan Sensor Nirkabel atau dalam banyak literatur disebut Wireless Sensor Network (WSN) adalah sebuah jaringan yang menghubungkan perangkat-perangkat seperti sensor node, router dan sink node (Muhamad Fajar). Perangkat

ini terhubung secara ad-hoc dan mendukung komunikasi multi-hop. Istilah ad-hoc merujuk pada kemampuan perangkat untuk berkomunikasi satu sama lain secara langsung tanpa memerlukan infrastruktur jaringan seperti router atau akses point. Sedangkan multi-hop yaitu istilah yang merujuk pada komunikasi beberapa perangkat yang melibatkan perangkat antara (intermediate), multi-hop melibatkan perangkat antara seperti router untuk meneruskan sebuah paket dari satu node ke node lain dalam jaringan.

Banyak aplikasi yang bisa dilakukan menggunakan jaringan sensor nirkabel, misalnya pengumpulan data kondisi lingkungan, security monitoring, dan node tracking scenarios . Sebuah aplikasi pengumpulan data lingkungan kanonik adalah salah satu penelitian dimana ilmuwan ingin mengumpulkan pembacaan beberapa sensor dari satu set poin dalam suatu lingkungan selama periode waktu tertentu untuk mendeteksi tren dan saling ketergantungan. Para ilmuwan ini ingin mengumpulkan data dari ratusan titik yang tersebar di seluruh daerah dan kemudian menganalisis data secara offline.

Peningkatan jumlah aplikasi Wireless Sensor Network membutuhkan delay jaringan yang rendah. Penelitian saat ini di bidang WSN terutama terkonsentrasi pada bagaimana mengoptimalkan efisiensi energi dengan kurang memperhatikan masalah delay jaringan. Beberapa rancangan WSN baru ditargetkan pada aplikasi yang memerlukan delay transfer data yang rendah dan keandalan yang tinggi. WSN termasuk jaringan transfer data multihop dengan delay rendah dan hemat energi. Usianya bisa mencapai beberapa tahun dengan baterai kecil. Node-node saling berkomunikasi menggunakan biaya dan daya yang rendah pada frekuensi radio. Jaringan ini telah diterapkan pada aplikasi sistem keamanan di rumah sakit.

Arsitektur WSN

Terdapat dua macam topologi wireless sensor network, yaitu tipe kluster dan tipe flat. Topologi jaringan kluster pada gambar 1. Pada topologi ini, node-node sensor diatur dalam susunan secara hierarki sehingga terdapat tiga macam node, yaitu child node, cluster head, dan parent node. Cluster head berfungsi sebagai

pengatur beberapa child node dalam aplikasinya. Beberapa cluster head menjadi anggota dari sebuah parent node.

Sedangkan untuk topologi jaringan flat hanya terdapat dua macam node secara fungsional, yaitu sensor/source node dan sink node. Semua sensor node dalam sistem mengirim data ke satu tujuan akhir, yaitu sink node. Proses pertukaran data dilakukan secara nirkabel. Frekuensi yang dipilih adalah salah satu alokasi frekuensi bebas pada ISM Bands. Alokasi frekuensi ISM lain yang tersedia adalah 315, 868, 915, dan 2400 MHz.

Berbagai jenis Node dalam WSN

Node dalam WSN seringkali juga disebut sebagai “mote”. Pada dasarnya adalah sebuah komputer (hasil dari evolusi komputer saat ini), walaupun bentuk dan kemampuannya tidak seperti umumnya komputer yang kita gunakan saat ini karena kemampuan yang masih terbatas dan ukurannya yang cukup kecil (smart dust), tetapi fungsi mereka seperti komputer pada umumnya dan tentu saja semakin hari kemampuannya pun semakin meningkat. Mote dilengkapi alat pemroses (CPU), memori,sejumlah antarmuka Input/Output yang dapat diprogram (terintegrasi pada mikrokontroller), transceiver untuk komunikasi radio, sumber daya energi yang umumnya menggunakan baterai, dan beberapa peralatan tambahan yang dapat disertakan sesuai kebutuhan. Gambar 4. Memperlihatkan komponen utama penyusun sebuah mote.

Fungsi dan kemampuan mote berbede-beda, berikut beberapa jenis mote dalam WSN.

Sensor node: yaitu node yang berfungsi untuk membaca data lingkungan atau objek yang dipantau.Untuk keperluan pembacaan atau penginderaan, node ini dilengkapi dengan satu atau beberapa perangkat sensor. Dari kemampuannya, node ini dapat dibagi menjadi dua jenis. Pertama, Node dengan kemampuan standar (Mis: Proyek Hydra), dan kedua yaitu Node yang telah dilengkapi fasilitas yang lebih kaya seperti CCD camera, wireless LAN, logger, Webserver, dsb (Mis: Proyek FieldServer). Node jenis kedua ini juga mampu melakukan komputasi yang lebih kompleks dibanding jenis pertama.

Router: yaitu node yang berfungsi untuk meneruskan paket data dari sebuah node ke node lain. Node ini berguna untuk keperluan komunikasi multi-hop. Dalam aplikasi nyata, kita dapat memprogram sebuah Sensor Node bertindak sebagai router.

Sink Node: yaitu node yang berfungsi untuk mengumpulkan data penginderaan dari Sensor Node, kemudian meneruskannya ke perangkat atau sistem lain, seperti ke database server untuk penyimpanan. Selain untuk mengumpulkan data dari sensor node, sink juga berfungsi sebagai penyebar paket dari perangkat atau sistem lain ke WSN, misalnya untuk keperluan pemrograman atau konfigurasi ulang sensor node secara remote

C. Latihan

a. Sebutkan Tujuan dari DDP..?
b. Sebutkan karateristik dari DDP …?
c. Apa yang dimaksud dengan sensor Network …?

D. Kunci Jawaban

a. Jawaban latihan soal ke-1

Tjuan dari DDP adalah :

Adalah menyatukan kemampuan dari sumber daya (sumber komputasi atau sumber informasi) yang terpisah secara fisik, ke dalam suatu sistem gabungan yang terkoordinasi dengan kapasitas yang jauh melebihi dari kapasitas individual komponen-komponennya.

b. Jawaban latihan soal ke-2

Tidak ada mesin yang memiliki informasi lengkap tentang Mesin

- Mesin biasanya menbuat keoutusan hanya berdasarkan informasi lokal
- Kegagalan satu mesin tidak merusak algoritma anda
- tidak ada asumsi secara implisit bahwa ada jam secara global

c. Jawaban latihan soal ke-n

sebuah jaringan yang menghubungkan perangkat-perangkat seperti sensor node, router dan sink node. Perangkat ini terhubung secara ad-hoc dan mendukung komunikasi multi-hop.

E. Daftar Pustaka

1. Couloris et. al. 2012. Distributed Systems Concepts and Design, Fifth Edition. Addison Wesley.
2. Van Steen and Tanenbaum, 2017. Distributed Systems: Prinsiples and Paradigms. 3e. Prentice-Hall

Link :

http://www.businessdictionary.com/definition/distributed-data-processing-DDP.html

https://cds.cern.ch/record/1056310/files/0132392275_TOC.pdf

MODUL PEMROSESAN DATA TERSEBAR

(PTI 611)

MODUL SESI 3

ARSITEKTUR PEMROSESAN DATA TERSEBAR

DISUSUN OLEH

HERMANSYAH, S.Kom., M.Kom.

UNIVERSITAS ESA UNGGUL

2020

MODEL ARSITEKTUR PEMROSESAN DATA TERDI

A. Kemampuan Akhir Yang Diharapkan

Setelah mempelajari modul ini, diharapkan mahasiswa mampu :

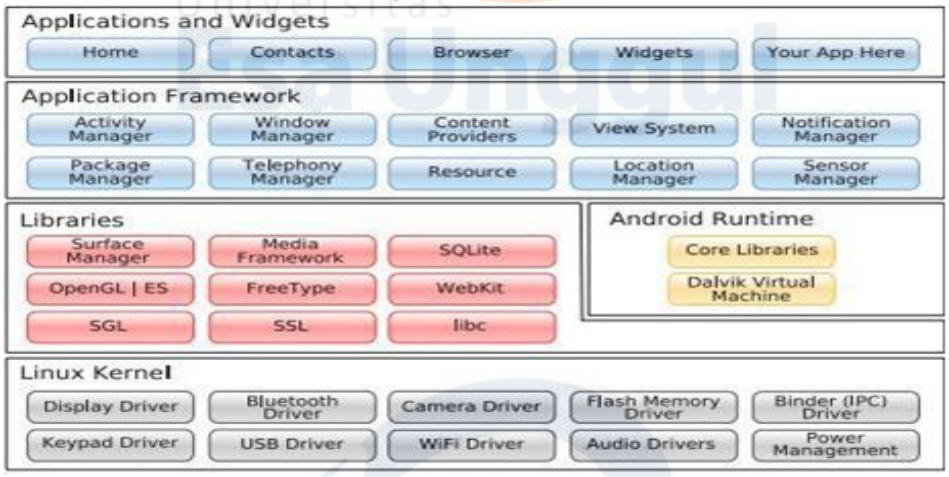
1. Memahami dan mengerti Arsitektur Pengolahan Data Terdistribusi
2. Memahami dan mengerti berbagai jenis arsitektur Pemrosesan Data Tersebar.
3. Memahami dan mengerti Collaborative arsitektur dalam pengolahan data tersebar

B. Uraian dan Contoh

1. Arsitektur Sistem Pemrosesan Data Tersebar.

Arsitektur Sistem Terdistribusi

Arsitektur Definisi: Suatu rancangan untuk penyusunan komponenkomponen suatu sistem, dimana rancangan tersebut mengidentifikasi komponen serta fungsi masing-masing komponen, konektifitas antar komponen serta pemetaan fungsionalitas komponen.



Model Arsitektur Sistim terdistribusi

Arsitektur Logis (Software architecture)

- Organisasi logika dari komponen-komponen perangkat lunak
- Komponen yang dimaksud berupa unit modular berupa interface yang dapat diproses di sistem yang berbeda
- RPC (remote prosedure call), message passing
- Jenis Model arsitektur logis (style)
- Layered architectures
- Object-base architectures
- Data-Center architectures
- Event-based architectures
- Arsitektur Fisik (System architecture)
- Peletakan mesin
- Peletakan komponen perangkat lunak pada mesin sesungguhny a

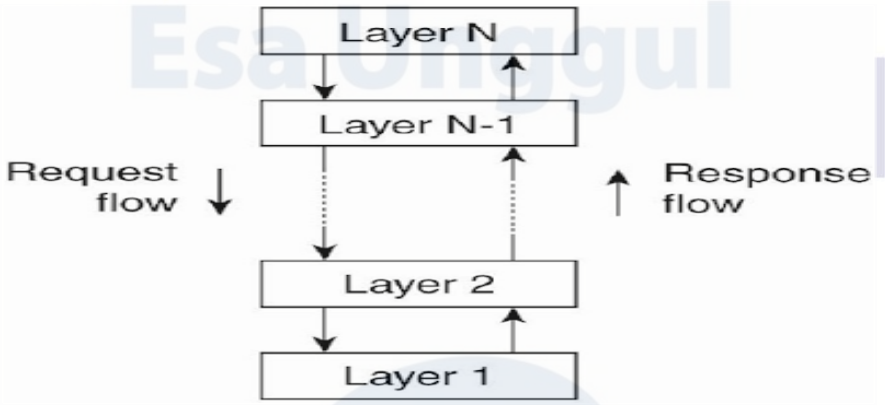
Layered Architectures

Komponen-komponen pada Layered architectures diorganisasi dalam bentuk lapisan-

lapisan (layer) fungsi dan service Contoh:

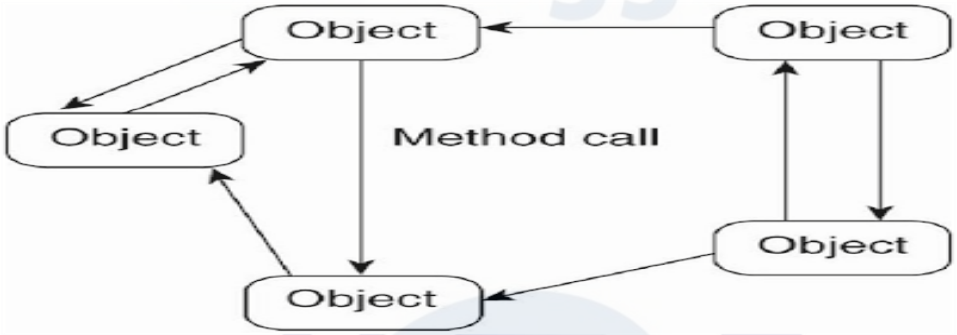
• - Operating system (windows, linux)

- Network Protocol (OSI, TCP/IP)

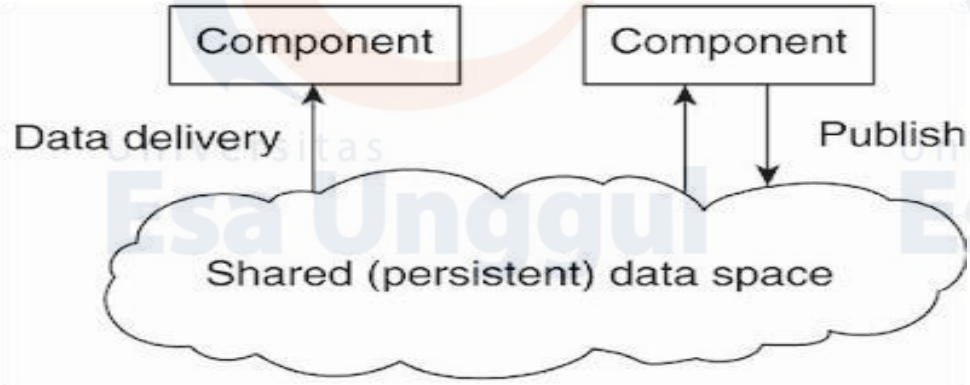


Object-base Architectures

Object-base architectures menggambarkan setiap objek melakukan koresponden dengan komponen, dan komponen ini terkoneksi melalui mekanisme procedure call. Bentuk T.



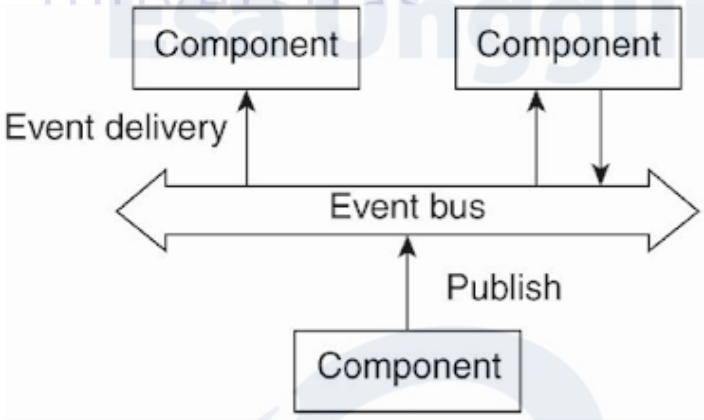
Data-center Architectures



Data center dapat dipandang sebagai gudang data (data warehouse) yang berfungsi sebagai sistem pengelolaan data mulai dari pengumpulan, pengolahan, penyimpanan hingga penemuan kembali data, serta mampu pula memberikan dukungan dalam pengambilan keputusan. Sebagai contoh adalah sistem tersebar berbasis web.

Event-based Architectures

Proses EBA pada dasarnya berdasarkan propagasi event. Proses mengeluarkan event setelah Middleware memberikan kepastian hanya proses itu saja yang bisa di subcribe untuk event yang diterima. Keuntungan EBA adalah proses bersifat loosely coupled.



System Architecture

Centralized Architectures (Client-Server)

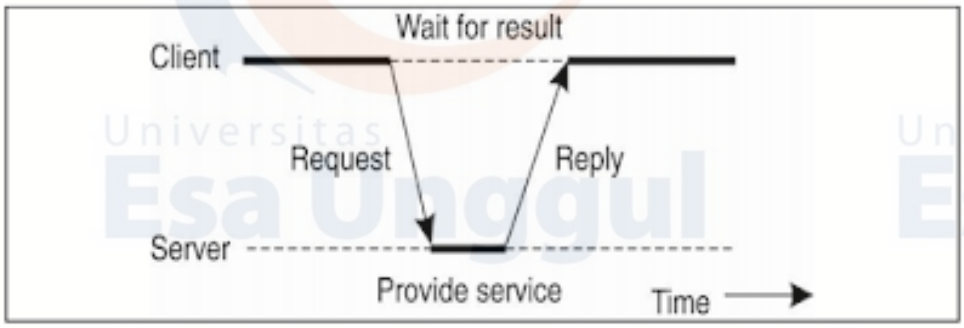
- Application Layering
- Multi-tiered Architectures

Decentralized Architectures

- Structured P2P (Peer-to-Peer) Architectures
- Unstructured P2P Architectures
- Topology Management of Overlay Networks
- Superpeers

Hybrid Architectures

- Edge-Server Systems
- Collaborative Distributed Systems

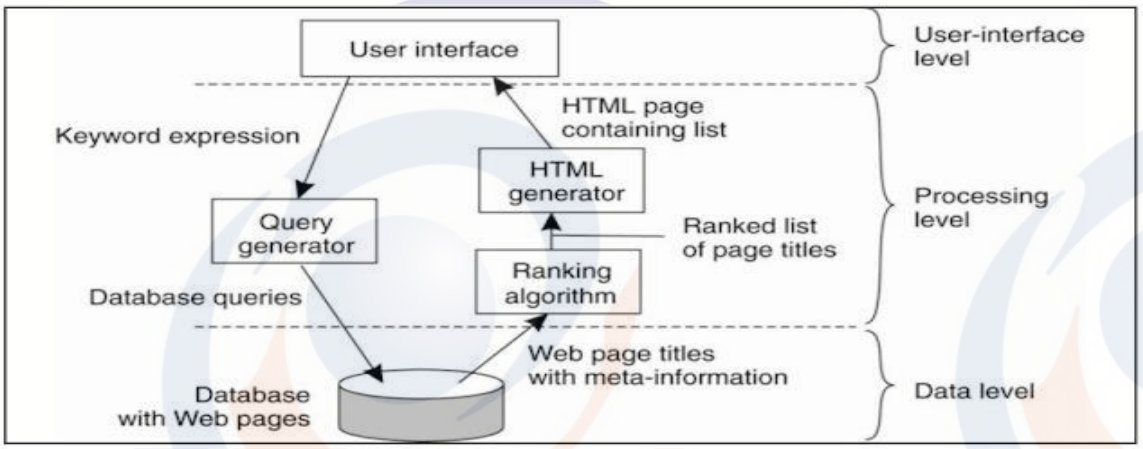


Client server unggul dalam kecepatan dan mendukung jaringan besar. Kekurangan terdapat pada sisi setup yang cukup komplek, biaya tinggi dan membutuhkan sumberdaya manusia yang handal untuk mengelola. Pada model client server, terdapat perilaku yang biasa disebut requestreply behavior

Application Layering

Model client server seiring perkembangannya mengundang perdebatan mengenai perbedaan antara client dan server itu sendiri. Pada umumnya client server architecture ditujukan untuk keperluan user access ke database, maka dari itu layered architectural style dibagi menjadi:

- user-interface level (display management)
- processing level (applications)
- data level (actual data that is being acted on)



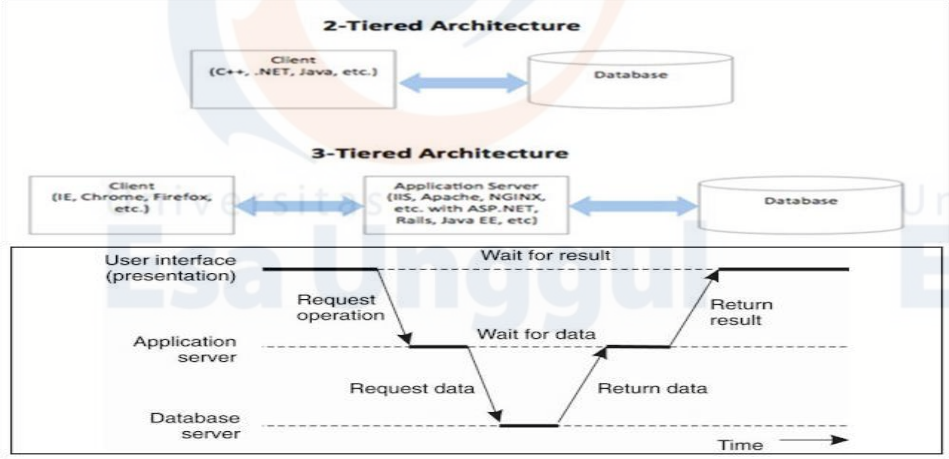
The simplified organization of an Internet search engine into hree different layers.

Multitier Architecture

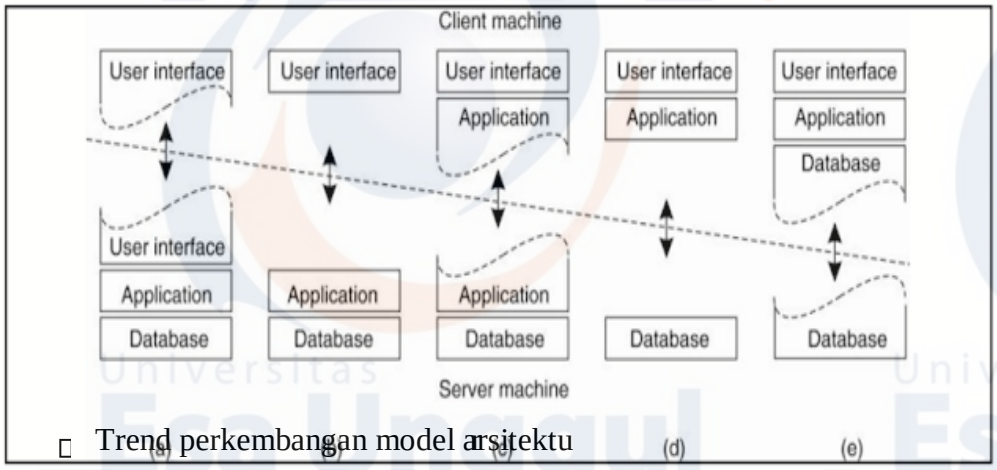
2 tier architecture

Pengorganisasian paling simple dimana terdiri atas 2 type mesin

- Client yang berisi implementasi program pada user-interface level
- Server yang berisi implementasi program pada proses dan data level



1. 3 tier architecture
2. Pada keperluan khusus, kadang server juga perlu bertindak sebagai client
3. Pada arsitektur ini, program pada processing level tidak hanya terdapat pada server yang terpisah, bahkan dapat terdistribusi pada client dan server mesin



- Trend perkembangan model arsitektu

Ringkasan

1. Perbedaan tier berkaitan dengan aplikasi logis organisasi.
2. Disebut sebagai vertical distribution dimana karakteristik tipe ini adalah menempatkan secara logis komponen yang berbeda pada mesin yang berbeda juga.
3. Memiliki vertical distribution dapat membagi secara logis maupun fisik dalam beberapa mesin yang berbeda, dimana masing-masing mesin dapat menjalankan fungsi khusus atau tergabung pada sebuah grup untuk fungsi tertentu

Uraian sub topik ke-1

2. Decentralied Arschitecture

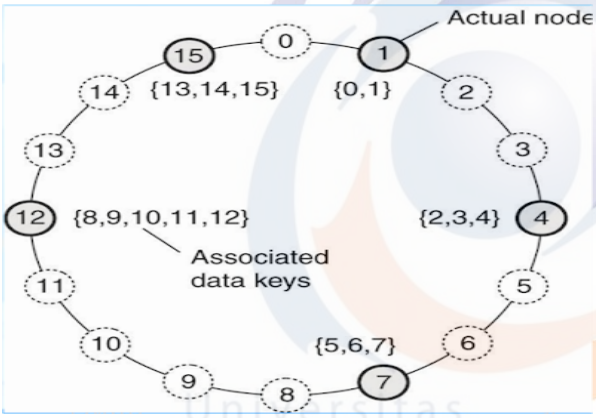
Decentralized Architecture

• Disebut sebagai Horizontal distribution

• Pada arsitektur ini, secara fisik terpisah namun secara logis memiliki fungsi level yang sama (equivalent), dimana setiap mesin memproses bagiannya sendiri kemudian melakukan balancing terhadap hasil proses.

• Nama lain Peer-to-peer architecture

Peer-to-peer architecture



Perkembangan P2P arsitektur tidak lepas dari pertanyaan

1. Bagaimana organisasi proses dalam jaringan
2. Sebuah proses tidak dapat berhubungan secara langsung dengan proses lain di jaringan.

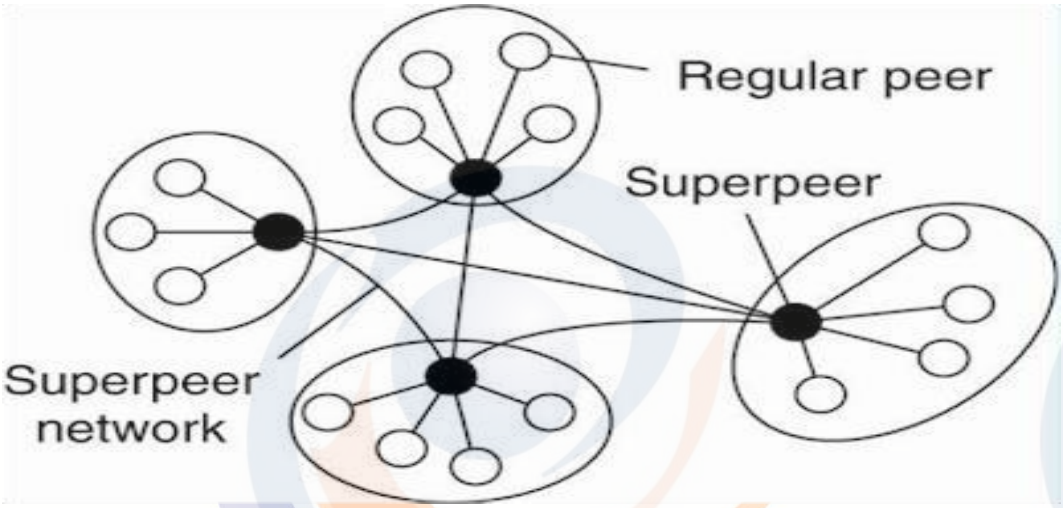
2. Diperlukan sebuah pesan khusus untuk komunikasi proses

1. Structured peer-to-peer architecture : Dalam struktur ini lapisan jaringan di bangun menggunakan deterministic procedure, seperti menggunakan distributes hash table (DHT).

o Unstructured peer-to-peer architecture : Dalam struktur ini menugaskan sebagian besar pada algoritma secara acak untuk membangun lapisan jaringan. Pada intinya setiap node mendata jaringan node neighboor, tetapi data node tersebut di tempuh dengan proses acak sederhana.

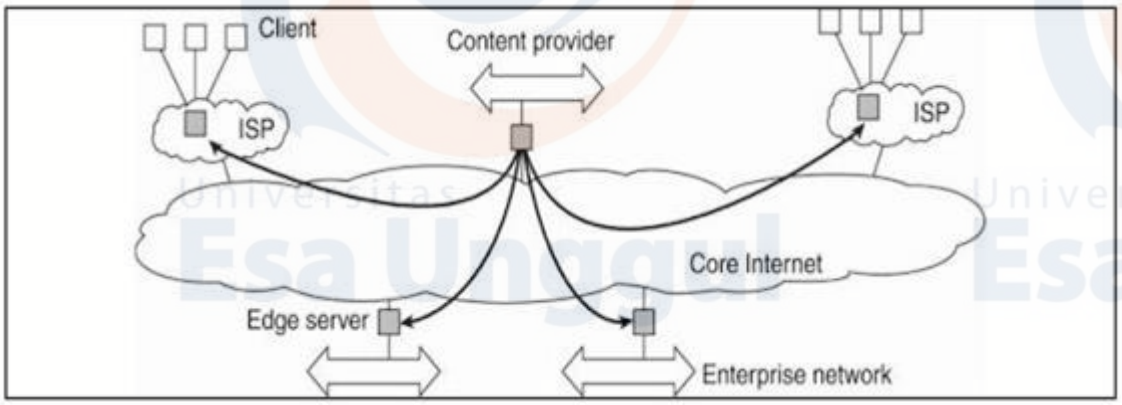
o Topology Management of Overlay Networks : Walaupun pada structured dan unstrustured peer-to-peer System cukup jelas, namun dalam beberapa kasus masih belum lengkap. Satu kunci dari observasi adalah kehati-hatian dari proses pertukaran dan pemilihan entries dari pandangan parsial dimana topologi tertentu dapat dibangun dan dijaga konektivitasnya.

- **Superpeers**



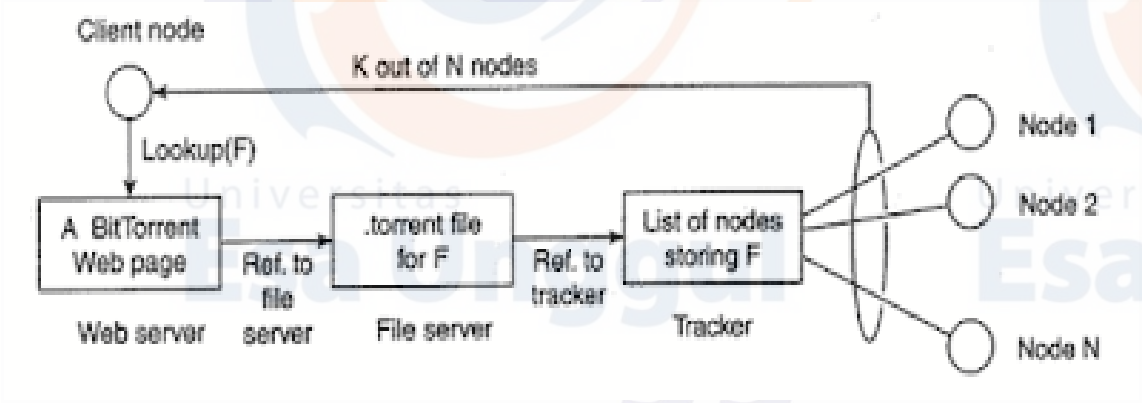
Hybrid Architecture

1. Edge-Server Systems
2. Sistem ini dibangun di jaringan internet dimana server di tempat kan pada edge (tepi) dari jaringan.
3. Tujuan Edge server adalah melayani content (isi), pada saat proses filtering dan fungsi transcoding



Collaborative Distributed Systems

1. Bentuk lainnya adalah CBS ini dibangun dari beberapa jaringan sistem tersebar yang ada.
2. Konsep sama dengan BitTorrent file-sharing system
3. Component dapat redirect client untuk akses server lain, analisa pola akses client, memanage replication data

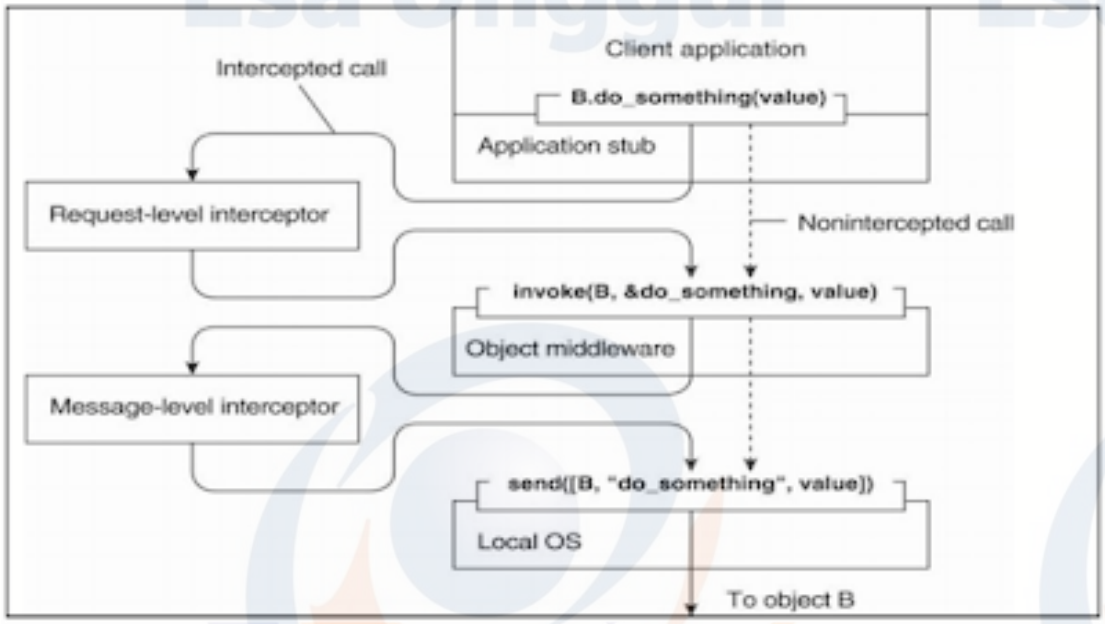


Architecture Versus Middleware

1. Tidak membahas perbandingan Arsitektur dan Middleware
2. Middleware mengikuti bentuk arsitektur yang ada.
3. Middleware dan aplikasi menangani kebutuhan berbeda namun nantinya tetap dibutuhkan solusi dimana middleware mudah untuk di konfigurasi, disesuaikan dan di kostumisasi sesuai kebutuhan aplikasi.

Interceptors

1. Interceptors merupakan perangkat lunak yang memecah aliran pengendalian dan mengijinkan kode lain untuk di eksekusi/proses.
2. Interceptors sangat baik untuk menyediakan proses transparency dari Replication dan Performance



General Approaches to Adaptive Software

1. Kebutuhan akan penyesuaian terhadap lingkungan aplikasi di sistem tersebar adalah perubahan secara terus menerus.
2. Perubahan ini sebagai hasil dari mobility, quality-of-service networks, kerusakan hardware, dan battery drainage dll.
3. Konsep ini disebut sebagai adaptive software
4. McKinley et al. (2004) membagi 3 teknik dasar menuju adaptive system

1. Separation of concerns:
2. Computational reflection
3. Component-based design (stand-alone)

Uraian sub topik ke-2

3. Sub sub topik ke-n

Uraian sub topik ke-n

C. Latihan

a. Latihan soal ke-1

Berikan Penjelasan apa yang dimaksud dengan arsitektur dari DDP…?, dan sebutkan beberapa Arsiektur Distributed Data Processing anda ketahui …?

b. Latihan soal ke-2

Jelaskan apa yang dmaksud dengan centralisai data prosesing dan paperbedaan nyadengan DDP….?

c. Latihan soal ke-n

D. Kunci Jawaban

a. Jawaban latihan soal ke-1

Arsitektur Definisi: Suatu rancangan untuk penyusunan komponenkomponen suatu sistem, dimana rancangan tersebut mengidentifikasi komponen serta fungsi masing-masing komponen, konektifitas antar komponen serta pemetaan fungsionalitas komponen.

Ada beberapa model arsiektur atara lain :

- Layered Architectures
- Object-base Architectures
- Data-center Architectures
- Event-based Architectures
- Hybrid Architectures

b. Jawaban latihan soal ke-2

Data Tersentralisasi :

Dalam sistem pengolahan data tersentralisasi operasi-operasi pengolahan data dilaksanakan oleh suatu bagian yang terpisah dalam struktur organisasi yang sering disebut bagian pengolahan data elektronik (Elektronic Data Processing/EDP), atau dapat juga dilakukan oleh :

- Suatu biro jasa yang merupakan suatu perusahaan terpisah di luar organisasi dan memberikan bermacam-macam pelayanan pengolahan data
- Fasilitas – fasilitas pembagian waktu bersama (timesharing) yang dibeli atau disewa dari suatu perusahaan
- Suatu susunan manajemen fasilitas dimana suatu perusahaan mengambil alih pelaksanaan operasi data dalam organisasi tersebut

Bentuk pengolahan data tersentralisasi dalam struktur organisasi mempunyai faktor pendukung antara lain :

- Penghematan khusus dalam hardware dan pengadaan personalia
- Penghematan karena meniadakan pengembangan sistem yang ganda
- Manfaat karena standarisasi
- Manfaat karena sistem yang seragam

Perbedaan yang pasi adalah

- Kalau pengolahan data tercentralisasi, maka penglahan data dilakukan secara terpusat disuatu lokasi tertentu.
- Kalau pengolahan dtata terdistribusi maka penglahan data dilakukan secara tersebar pada masing masing lokasi tertentu.

E. Daftar Pustaka

1. Couloris et. al. 2012. Distributed Systems Concepts and Design, Fifth Edition. Addison Wesley.
2. Van Steen and Tanenbaum, 2017. Distributed Systems: Prinsiples and Paradigms. 3e. Prentice-Hall

Link journal :

https://www.amazon.co.uk/Distributed-Systems-Principles-Paradigms-United/dp/0130888931

MODUL PEMROSESAN DATA TERSEBAR

(PTI-611)

MODUL SESI KE-4

PROSES DALAM PROSES DATA TERSEBAR

DISUSUN OLEH

HERMANSYAH S.Kom., M.K.om.

UNIVERSITAS ESA UNGGUL

2020

PROSES DALAM DATA TERDISTRIBUSI

A. Kemampuan Akhir Yang Diharapkan

Setelah mempelajari modul ini, diharapkan mahasiswa mampu :

1. Memahami konsep proses dalam pengolahan data terdistribusi
2. Mengetahui konsekwensi Migrasinya serta dapat mengaplikasinya pada kasus kasus.
3. Sub kompetensi ke-n

B. Uraian dan Contoh

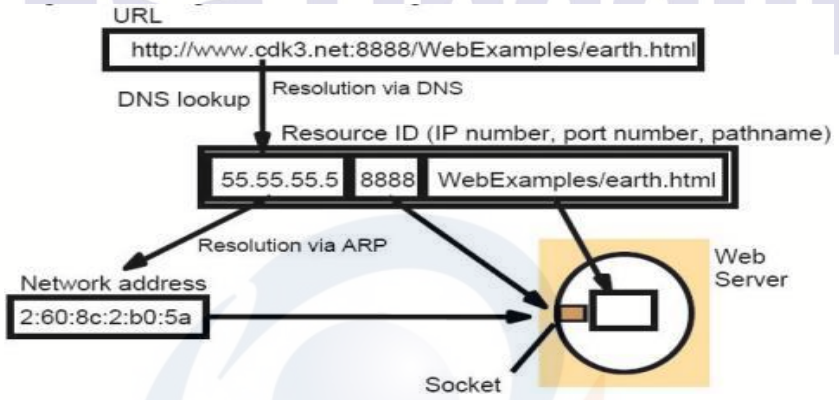
1. Sub sub topik ke-1

Processes

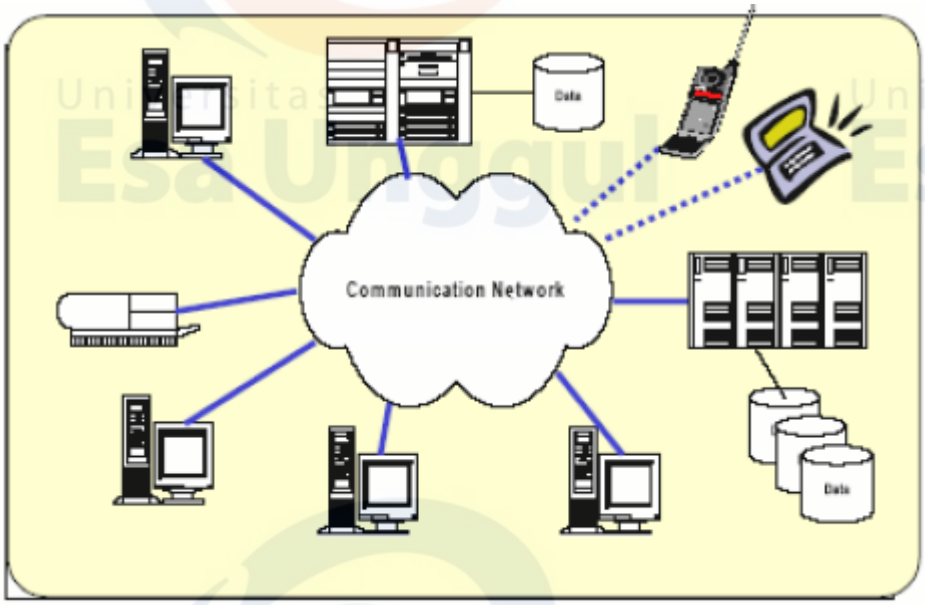
Proses Dalam Sistem Terdistribusi

• Proses dalam sistem terdistribusi dijalankan secara bersamaan (execute concurrently) dimana proses berinteraksi untuk bekerjasama dalam mencapai tujuan yang sama dan mengkoordinasikan aktifitas dan pertukaran informasi yaitu pesan yang dikirim melalui jaringan komunikasi.

Struktur Sistem Terdistribusi dapat dilihat pada gambar dibawah ini:



Gmbar 4,1. Names Servis ati Distributed Data Processing



Gambar 4.2. Jaringankomunikasu

Dalam sistem terdistribusi prosesor yang dimiliki bervariasi, dapat berupa small microprocessor, workstation, minicomputer, dan lain sebagainya. Sebenarnya ada beberapa hal mendasar yang membedakan antara jaringan komputer yang merupakan dasar dari konsep sistem terdistribusi dengan sistem terdistribusi itu sendiri yaitu komputer otonom yang secara eksplisit terlihat, sedangkan pada sistem terdistribusi komputer otonom transparan dan juga memiliki lebih banyak masalah dibanding dengan jaringan komputer.

B. Karakteristik Sistem Terdistribusi

Ada tiga karakteristik sistem terdistribusi antara lain sebagai berikut:

1. Concurrency of components

Pengaksesan suatu komponen/sumber daya (segala hal yang dapat digunakan bersama dalam jaringan komputer, meliputi H/W dan S/W) secara bersamaan. Contoh: Beberapa pemakai browser mengakses halaman web secara bersamaan

2. No global clock

Hal ini menyebabkan kesulitan dalam mensinkronkan waktu seluruh komputer/perangkat yang terlibat. Dapat berpengaruh pada pengiriman pesan/data, seperti saat beberapa proses berebut ingin masuk ke critical session.

3. Independent failures of components

Setiap komponen/perangkat dapat mengalami kegagalan namun komponen/perangkat lain tetap berjalan dengan baik.

Hal ini menyebabkan kesulitan dalam mensinkronkan waktu seluruh komputer/perangkat yang terlibat. Dapat berpengaruh pada pengiriman pesan/data, seperti saat beberapa proses berebut ingin masuk ke critical session.

Sistem terdistribusi dibangun untuk mencapai tujuan-tujuan yang ingin dicapai, diantaranya :

1. Untuk memberikan akses bagi pengguna untuk dapat mengembangkan sumber daya sistem.
2. Peningkatan kecepatan komputasi.
3. meningkatkan availibilitas atau ketersediaan dan reliabilitas data

Dalam penggunaanya sistem terdistribusi sangat diperlukan karena:

1Performance : Sekumpulan prosesor dapat menyediakan kinerja yang lebih tinggi daripada komputer yang terpusat

22. Distribution : Banyak aplikasi yang terlibat, sehingga lebih baik jika dipisah dalam mesin yang berbeda (contoh: aplikasi perbankan, komersial)

1. Reliability : Jika terjadi kerusakan pada salah satu mesin, tidak akan mempengaruhi kinerja system secara keseluruhan

2. Incremental Growth : Mesin baru dapat ditambahkan jika kebutuhan proses meningkat

3. Sharing Data/Resource : Segala hal yang dapat digunakan bersama dalam jaringan komputer. Meliputi hardware (e.g. disk, printer, scanner), juga software (berkas, basis data, obyek data).

4. Communication : Menyediakan fasilitas komunikasi antar manusia.

Uraian sub topik ke-1

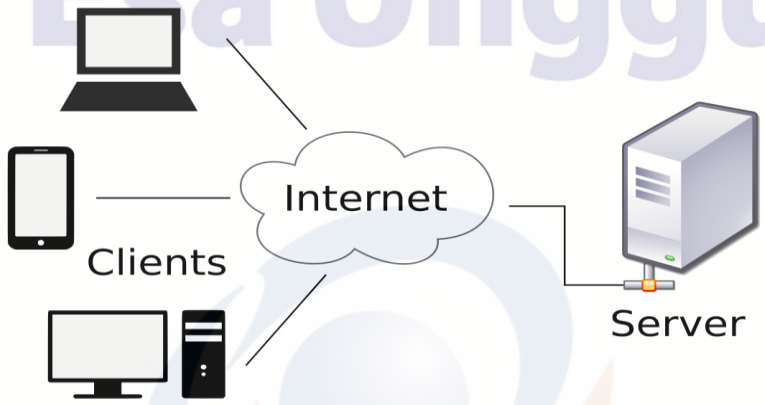
2. Model Sistem Terdistribusi

D. Model Sistem Terdistribusi

Dalam pelaksanaannya sistem terdistribusi memiliki berbagai bentuk (model), yaitu :

1. Sistem client - server

Merupakan bagian dari model sistem terdistribusi yang membagi jaringan berdasarkan pemberi dan penerima jasa layanan. Pada sebuah jaringan akan didapatkan: file server, time server, directory server, printer server, dan seterusnya. \



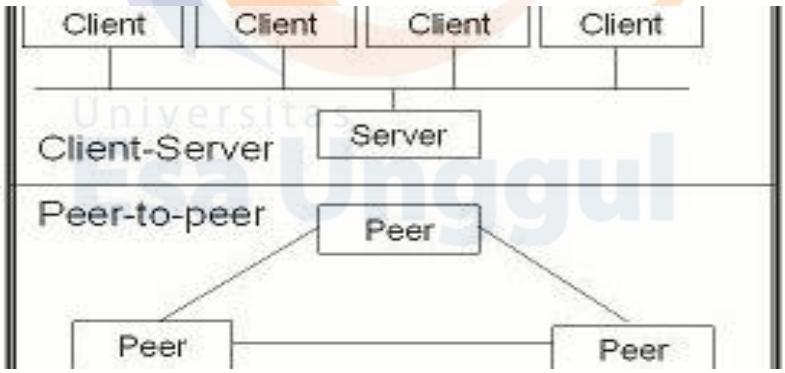
Gambar 4,3, Model Client Server

2. Sistem point to point

Merupakan bagian dari model sistem terdistribusi dimana system dapat sekaligus berfungsi sebagai client maupun server.

Gambar 4.4. sistem pont to point

3. Sistem terkluster



Gambar 4.5. Sistem Terkluster

Adalah gabungan dari beberapa sistem individual (komputer) yang dikumpulkan pada suatu lokasi, saling berbagi tempat penyimpanan data (storage), dan saling terhubung dalam jaringan lokal (Local Area Network). Sistem kluster memiliki persamaan dengan sistem paralel dalam hal menggabungkan beberapa CPU untuk meningkatkan kinerja komputasi. Jika salah satu mesin mengalami masalah dalam menjalankan tugas maka mesin

lain dapat mengambil alih pelaksanaan tugas itu. Dengan demikian, sistem akan lebih handal dan fault tolerant dalam melakukan komputasi.

E. Alasan Membangun Sistem Terdistribusi

Ada empat alasan utama untuk membangun sistem terdistribusi, yaitu:

1. Resource Sharing

Dalam sistem terdistribusi, situs-situs yang berbeda saling terhubung satu sama lain melalui jaringan sehingga situs yang satu dapat mengakses dan menggunakan sumber daya yang terdapat dalam situs lain. Misalnya, user di situs A dapat menggunakan laser printer yang dimiliki situs B dan sebaliknya user di situs B dapat mengakses file yang terdapat di situs A

2. Computation Speedup

Apabila sebuah komputasi dapat dipartisi menjadi beberapa subkomputasi yang berjalan bersamaan, maka sistem terdistribusi akan mendistribusikan subkomputasi tersebut ke situs-situs dalam sistem. Dengan demikian, hal ini meningkatkan kecepatan komputasi (computation speedup)

3. Reliability

Dalam sistem terdistribusi, apabila sebuah situs mengalami kegagalan, maka situs yang tersisa dapat melanjutkan operasi yang sedang berjalan. Hal ini menyebabkan reliabilitas sistem menjadi lebih baik

4, Communication

Ketika banyak situs saling terhubung melalui jaringan komunikasi, user dari situs-situs yang berbeda mempunyai kesempatan untuk dapat bertukar informasi.

Selain itu ada beberapa alasan lain membangun sistem terdistribusi, yakni :

- Distribusi fungsi : Komputer memiliki kemampuan fungsi yang berbeda-beda (client/server, Host/terminal, Data gathering / data processing)

- Distribusi beban/keseimbangan : Pemberian tugas ke prosesor secukupnya sehingga unjuk kerja seluruh sistem teroptimasi

- Replika Kekuatan : Kumpulan PC memiliki kekuatan yang lebih besar dari super computer

F. Permasalahan Sistem Terdistribusi

Masalah dengan sistem terdistribusi yang dapat dimunculkan antara lain berkaitan dengan :

- ✓ Software - bagaimana merancang dan mengatur software dalam Distribusi Sistem
- ✓ Ketergantungan pada infrastruktur jaringan
- ✓ Kemudahan akses ke data yang di share, memunculkan masalah keamanan

Dalam setiap penggunaan suatu sistem, banyak sekali ditemui permasalahan - permasalahan yang muncul, begitu juga dengan sistem terdistribusi. Selain permasalahan-permasalahan yang akan dihadapi terdapat tantangantantangan dalam sistem terdistribusi

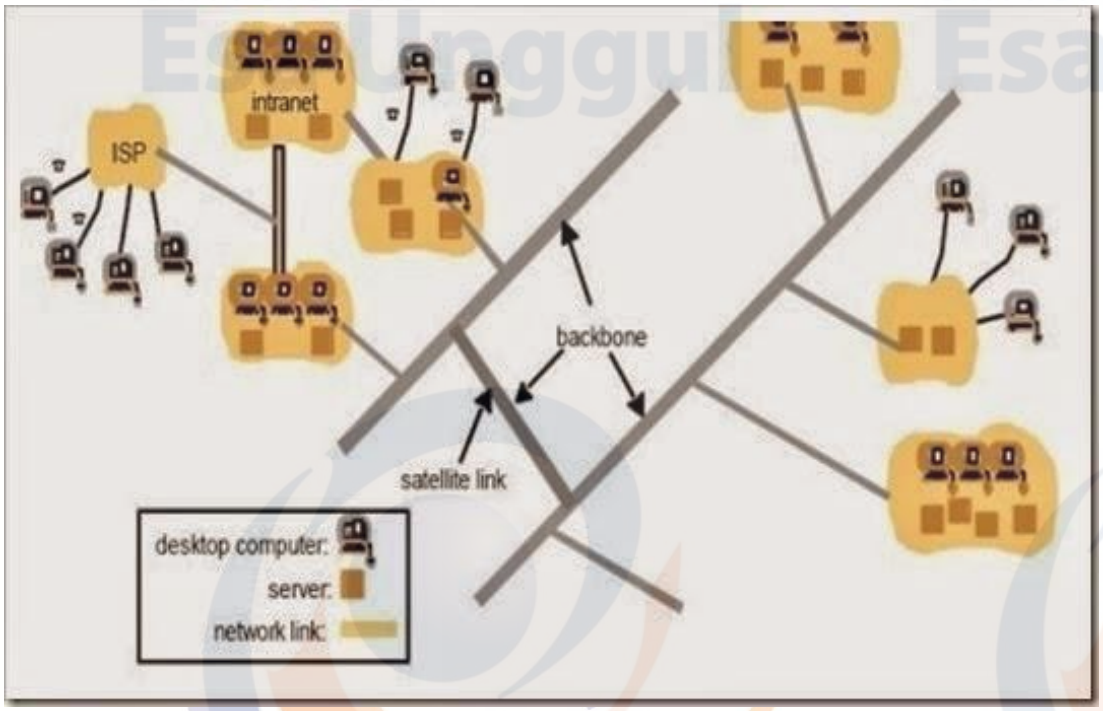
G. Contoh dari sistem terdistribusi

1. Internet

Pengertian Internet

Internet adalah sebuah jaringan yang menghubungkan komputer satu sama lain yang menggunakan standar sistem global Transmission Control Protocol atau Internet Protocol Suite (TCP/IP) sebagai protokol pertukaran sehingga kita bisa saling berkomunikasi, berinteraksi, dan saling bertukar informasi meski dalam jarak yang jauh.

Merupakan suatu bentuk jaringan global yang menghubungkan komputer denga satu sama lainnya, yang dapat *berkomunikasi* dengan media IP sebagai protokol



Gambar 4.6. Sistem Internet

2. Intranet

Pengertian Intranet

Selain Internet ada juga yang namanya Intranet, Intranet adalah jaringan pribadi (Private Network) yang mengunakan internet untuk saling berbagi dan bertukar informasi di dalam jaringan lokal contohnya adalah: Perusahaan, Kantor, Sekolah Universitas DLL.

Intranet juga termasuk ke dalam salah satu jaringan LAN (Local Area Network) yang hanya bisa mencakup wilayah kecil.

- Jaringan yang teradministrasi secara lokal
- Biasanya proprietary
- Terhubung ke internet (melalui firewall)
- Menyediakan layanan internal dan eksternal

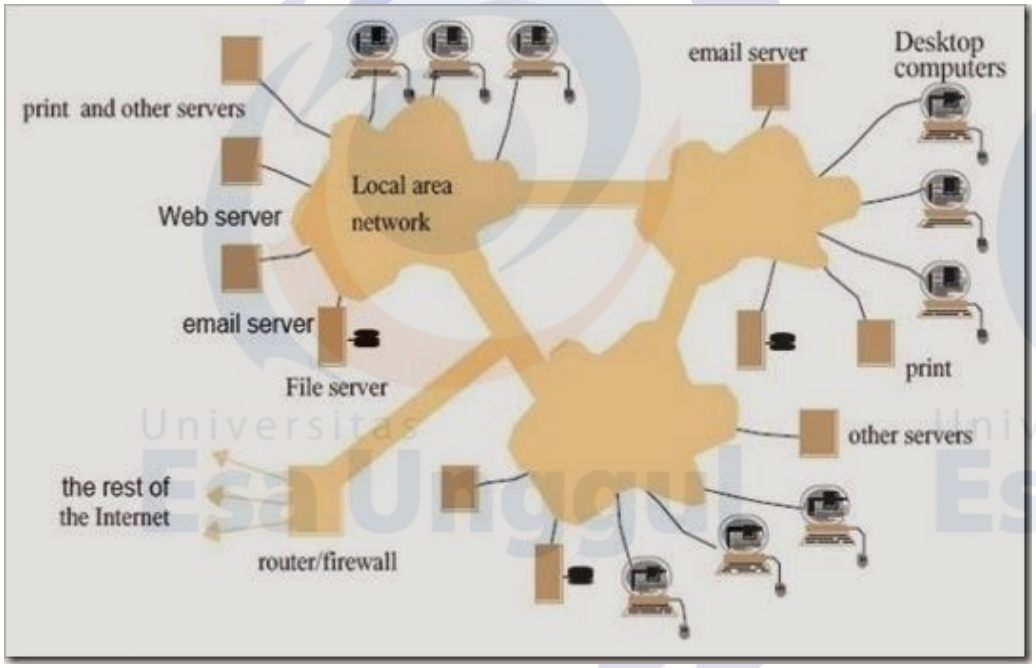
3. Perbedaan Antara Internet dan Intranet

Internet :

- Jaringan yang sangat Luas (Internasional Bahkan Sedunia)
- Memiliki Jaringan yang Kuat
- Perkembangan yang Sangat Pesat
- Bisa di akses kapan saja dan dimana saja

Intranet:

- Jaringan yang kecil dan sempit (hanya mencakup wilayah lokal)
- Perkembangannya yang lambat
- Biasa digunakan oleh perkantoran, sekolah, universitas, rumah sakit, dll



Gamba 4,7 Sistem Intranet

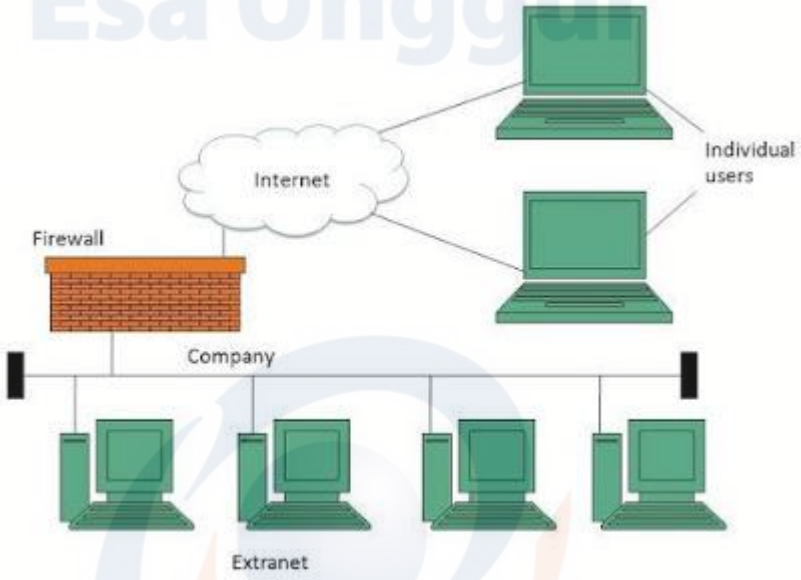
3. Ekstranet

Apa itu Extranet ?

Extranet atau Ekstranet adalah jaringan pribadi yang menggunakan protokol internet dan sistem telekomunikasi publik untuk membagi sebagian informasi

bisnis atau operasi secara aman kepada penyalur (supplier), penjual (vendor), mitra (partner), pelanggan dan lain-lain.

Extranet merujuk ke jaringan dalam sebuah organisasi, menggunakan internet untuk terhubung ke orang luar dalam cara yang terkontrol. Ini membantu untuk berhubungan bisnis dengan pelanggan dan penyalur mereka dan karena itu memungkinkan bekerja secara kolaboratif.

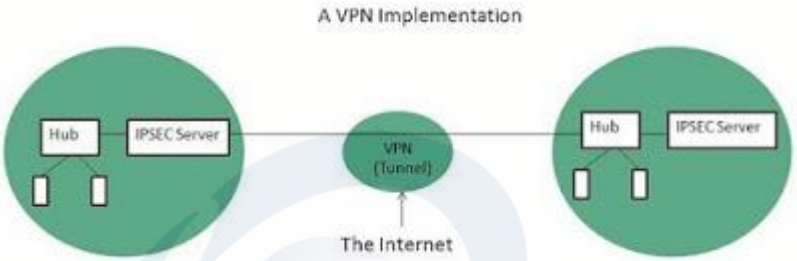


Gambar 4.9 Eksternet

Implementasi Exreanet

Extranet diimplementasikan sebagai jaringan pribadi Virtual / *Virtual Private Networt* (**VPN**) karena menggunakan internet untuk menyambung ke organisasi perusahaan dan selalu ada ancaman bagi keamanan informasi. **VPN** menawarkan jaringan aman infrastruktur masyarakat (**Internet**).

**VPN adalah singkatan dari Virtual Private Network, yaitu jaringan pribadi (bukan untuk akses umum) yang menggunakan medium nonpribadi (misalnya internet) untuk menghubungkan antar remote-site secara aman.*



Gambar 4.10 Contoh Implementasi Ekstrane

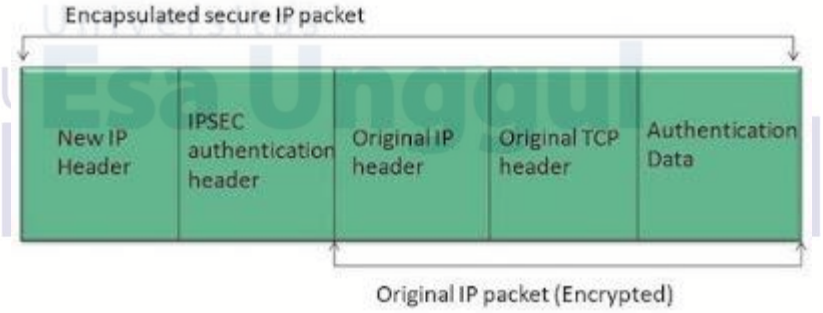
Kunci Utama pada Extranet

- Paket dirumuskan di batas jaringan di router keluhan **IPSEC**.
- Menggunakan kunci enkripsi untuk merangkum paket dan alamat IP juga.
- Paket yang diterjemahkan hanya oleh **IPSEC** keluhan router atau server.
- Pesan yang dikirim melalui **VPN** melalui tunnel **VPN** dan proses ini dikenal sebagai tunneling.

VPN menggunakan **Internet Protocol Security Architecture (IPSEC)** untuk memberikan keamanan transaksi dengan menambahkan lapisan keamanan tambahan untuk protokol **TCP/IP**. Lapisan ini dibuat oleh encapsulating paket **IP** untuk paket IP baru seperti yang ditunjukkan pada diagram berikut:

*IPSec (singkatan dari IP Security) adalah sebuah protokol yang digunakan untuk mengamankan transmisi datagram dalam sebuah internetwork berbasis TCP/IP. IPSec mendefiniskan beberapa standar untuk melakukan enkripsi data dan juga integritas data pada lapisan kedua dalam DARPA Reference Model (internetwork layer)

*TCP/IP (singkatan dari Transmission Control Protocol/Internet Protocol) yang diterjemahkan menjadi Protokol Kendali Transmisi/Protokol Internet, yang merupakan gabungan dari protokol TCP (Transmission Control Protocol) dan IP (Internet Protocol) sebagai sekelompok protokol yang mengatur komunikasi data dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan internet yang akan memastikan pengiriman data sampai ke alamat yang dituju



Gambar 4.11. Ip Packet

Manfaat Extranet

Extranet membuktikan untuk menjadi model sukses untuk semua jenis bisnis baik besar maupun kecil. Berikut adalah beberapa keuntungan dari extranet untuk karyawan, penyalur (supplier), mitra bisnis, dan pelanggan:

Tabel 4.1. Tabel Kuntungan Ekstranet

Masalah pada Extranet

Terpisah untuk keuntungan yang ada juga beberapa masalah terkait dengan **extranet**. Permasalahan ini dibahas di bawah ini:

Hosting
Halaman **extranet** akan diselenggarakan yaitu yang akan menjadi tuan rumah halaman **extranet**. Dalam konteks ini ada dua pilihan:

- Meng-host di server Anda sendiri.
- Host dengan Internet Service Provider (ISP) dengan cara yang sama sebagai halaman web.

Tapi hosting **extranet** halaman di server Anda sendiri memerlukan koneksi internet bandwidth tinggi yang sangat mahal.

Keamanan
Keamanan *firewall* tambahan diperlukan jika Anda meng-host halaman extranet di server Anda sendiri yang menghasilkan mekanisme keamanan yang kompleks dan meningkatkan beban kerja.

Accessing Issues
Informasi tidak dapat diakses tanpa koneksi internet. Namun, informasi dapat diakses di **Intranet** tanpa koneksi internet.

Postingan Terkait : Pengertian Intranet Manfaat dan Perbedaan Intranet dan Internet

Penurunan interaksi
Ini mengurangi face dengan interaksi face dalam bisnis yang mengakibatkan kurangnya komunikasi antara pelanggan, mitra usaha dan penyalur (supplier).

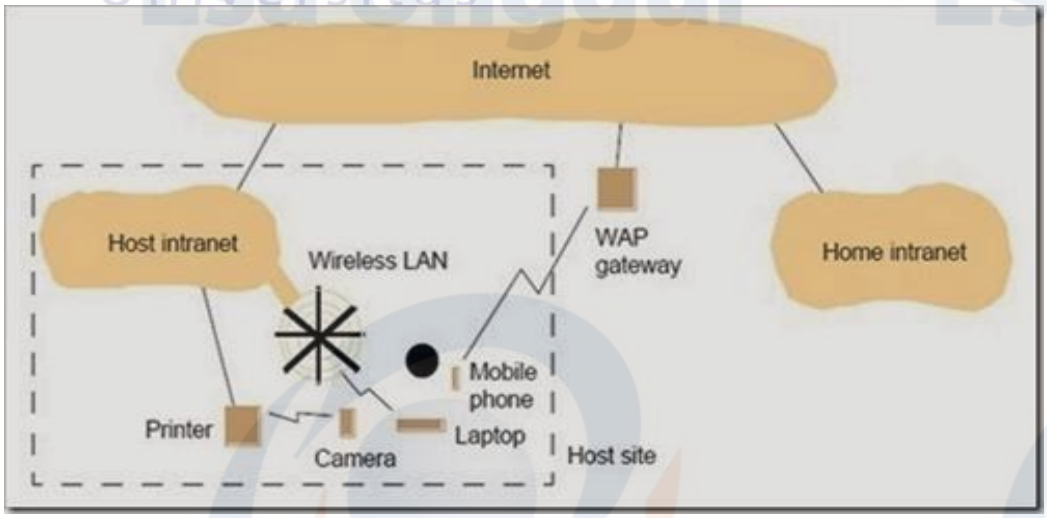
Extranet vs Intranet

Tabel berikut menunjukkan perbedaan antara Intranet dan Extranet:

Extranet	Intranet
Jaringan internal yang dapat diakses secara eksternal.	Jaringan internal yang tidak dapat diakses secara eksternal
Extranet adalah ekstensi dari Intranet perusahaan	Hanya terbatas pada pengguna perusahaan.
Untuk terbatas eksternal komunikasi antara pelanggan	penyalur (supplier) dan mitra bisnis. Hanya untuk komunikasi dalam perusahaan

***Tabel 4.2. Perbedaan Extranet dengan* Internet**

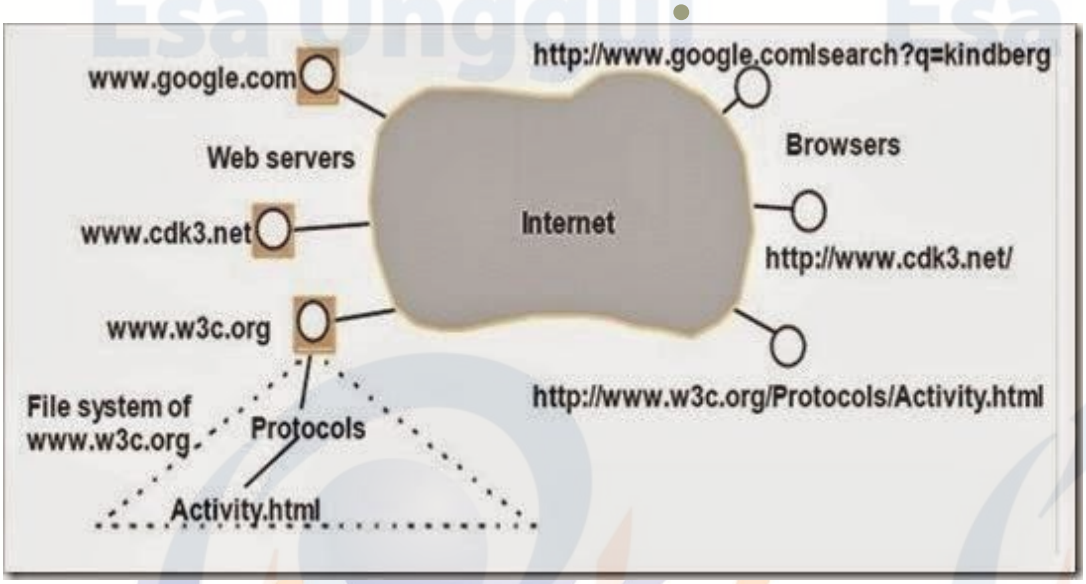
4. ***Mobile dan sistem komputasi ubiquitous***
    - Sistem telepon Cellular (e.g., GSM) Resources dishare : frekuensi radio, waktu transmisi dalam satu frekuensi, bergerak
    - Komputer laptop, ubiquitous computing
    - Handheld devices, PDA, etc



Gambar 4,11 Internet

4. World wide web

- Arsitektur client/server tebuka yang diterapkan di atas infrastruktur internet
- Shared resources (melalui URL)



Gambar 4.12. Sistem WWW.

Uraian sub topik ke-2

C. Latihan

a. Jelaskan Tentag Proses dalam data Terdistribusi
b. Sebutkan alasan Membangun sistem terdisbusi…?
c. Sebutkan beberapa contoh implementasi PDT ..?

D. Kunci Jawaban

a. Proses oengolahan Data Terdistribusi.

Proses dalam sistem terdistribusi dijalankan secara bersamaan (execute concurrently) dimana proses berinteraksi untuk bekerjasama dalam mencapai tujuan yang sama dan

mengkoordinasikan aktifitas dan pertukaran informasi yaitu pesan yang dikirim melalui jaringan komunikasi

b. Jawaban latihan soal ke-2

i. Resource Sharing
ii. Computation Speedup
iii. Reliability
iv. Communication

c, Contoh mplementasi PDT

- Internet
- Intranet
- Mobile dan sistem komputasi ubiquitous
- World wide web

A. Daftar Pustaka

1. Couloris et. al. 2012. Distributed Systems Concepts and Design, Fifth Edition. Addison Wesley.
2. Van Steen and Tanenbaum, 2017. Distributed Systems: Prinsiples and Paradigms. 3e. Prentice-Hall

Link :

https://www.goodreads.com/book/show/405614.Distributed_Systems

https://www.goodreads.com/search?q=process+in+distributed+data+processing&qid=pNFFKZD0Uu

MODUL PEMROSESAN DATA TERSEBAR

(FTI 611)

MODUL SESI 5

KOMUNIKASI

DISUSUN OLEH

HERMNSYAH S,Kom., M.Kom.

UNIVERSITAS ESA UNGGUL

2020

KOMUNIKASI DALAM SISTEM TERDISTRIBUSI

A. Kemampuan Akhir Yang Diharapkan

Setelah mempelajari modul ini, diharapkan mahasiswa mampu :

1. Memahami dan mengerti Konsep Komuniksi pada Pemrosesan Data tersebar.
2. Memahami dan mengerti Jenis-jenisKomunikasi serta protocol komunikasi
3. Sub kompetensi ke-n

B. Uraian dan Contoh

1. Komunikasi dalam Sistem Terdisribusi

Uraian sub topik ke-1

Komunikasi dalam Sistem Terdistribusi

Komunikasi adalah suatu proses penyampaian informasi (pesan, ide, gagasan) dari satu pihak kepada pihak lain. Pada umumnya, komunikasi dilakukan secara lisan atau verbal yang dapat dimengerti oleh kedua belah pihak. Dimana proses komunikasi dapat dilakukan kepada orang, kelompok, organisasi dan masyarakat menciptakan, dan menggunakan informasi agar terhubung dengan lingkungan dan orang lain.Komunikasi memiliki komponen-komponen yang menjadikan komunikasi berjalan dengan baik, komponen tersebut yaitu:

• Pengirim atau komunikator (sender) adalah pihak yang mengirimkan pesan kepada pihak lain.

• Pesan (message) adalah isi atau maksud yang akan disampaikan oleh satu pihak kepada pihak lain.

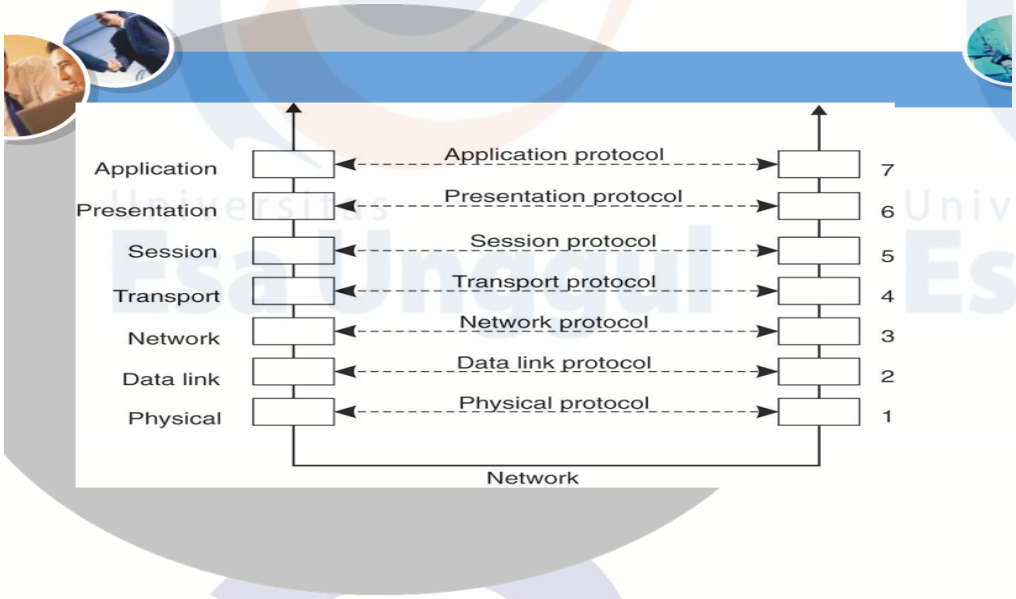
• Saluran (channel) adalah media dimana pesan disampaikan kepada komunikan. dalam komunikasi antar-pribadi (tatap muka) saluran dapat berupa udara yang mengalirkan getaran nada/suara.

• Penerima atau komunikate (receiver) adalah pihak yang menerima pesan dari pihak lain

• Umpan balik (feedback) adalah tanggapan dari penerimaan pesan atas isi pesan yang disampaikannya.

• Protokol adalah sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan,komunikasi, dan perpindahan data antara dua atau lebih titik komputer. Protokol dapat diterapkan pada perangkat keras, perangkat lunak atau kombinasi dari keduanya. Pada waktu itu, komunikasi antar komputer dari vendor yang berbeda adalah sangat sulit dilakukan, karena mengunakan protokol dan format data yang berbeda-beda. Sehingga International Standards Organization (ISO) membuat suatu arsitektur komunikasi yang dikenal sebagai Open System Interconnection

(OSI) model yang mendefinisikan standar untuk menghubungkan komputer-komputer dari vendor-vendor yang berbeda. Model-OSI tersebut terbagi atas layer-layer, yaitu: Layered Protocols



Gambar 5.1 Lapisan OSI

1. Physical Layer
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application.

TCP / IP (Transmition Control Protocol / Internet Protocol)

TCP / IP adalah protocol yang digunakan di jaringan global karena memiliki sistem pengalamatan yang baik dan memiliki sistem pengecekan data. saat ini terdapat 2 versi TCP/IP yang berbeda dalam sistem penomoran, yaitu IPv4 (32 bit) dan IPv6 (128 bit).

Remote Procedure Call (RPC) adalah sebuah metode yang memungkinkan kita untuk mengakses sebuah prosedur yang berada di komputer lain. Untuk dapat melakukan ini sebuah server harus menyediakan layanan remote procedure. Pendekatan yang dilakuan adalah sebuah server

membuka socket, lalu menunggu client yang meminta prosedur yang disediakan oleh server. Bila client tidak tahu harus menghubungi port yang mana, client bisa me- request kepada sebuah matchmaker pada sebuah RPC port yang tetap. Matchmaker akan memberikan port apa yang digunakan oleh prosedur yang diminta client.

RPC masih menggunakan cara primitif dalam pemrograman, yaitu menggunakan paradigma procedural programming. Hal itu membuat kita sulit ketika menyediakan banyak remote procedure. RPC menggunakan socket untuk berkomunikasi dengan proses lainnya. Pada sistem seperti SUN, RPC secara default sudah ter- install kedalam sistemnya, biasanya RPC ini digunakan untuk administrasi sistem. Sehingga seorang administrator jaringan dapat mengakses sistemnya dan mengelola sistemnya dari mana saja, selama sistemnya terhubung ke jaringan.

Langkah-langkah dalam RPC

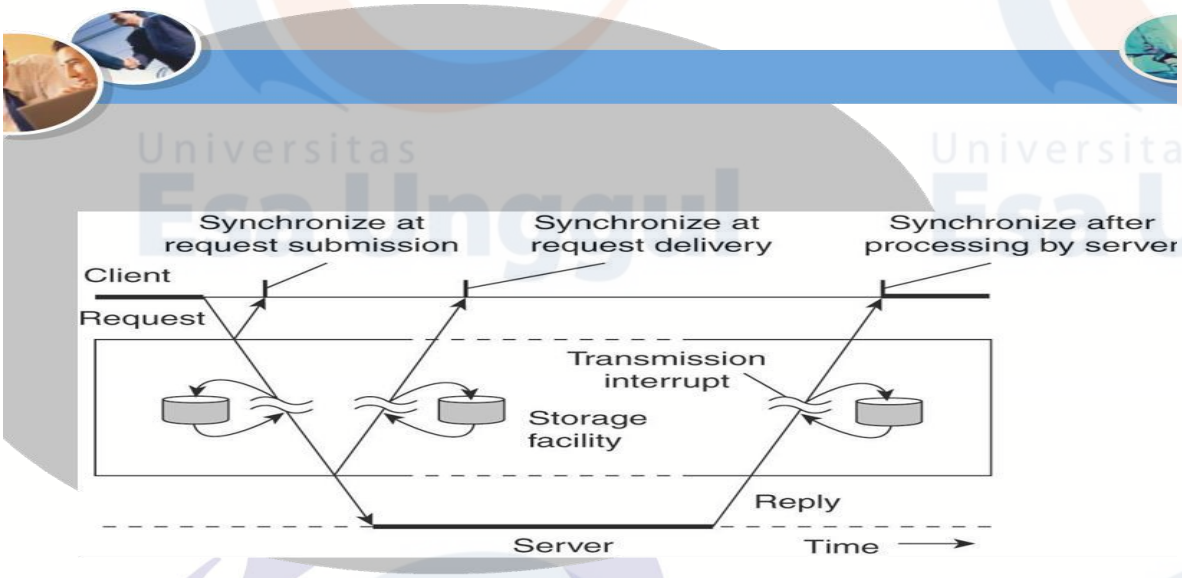
1. Klien memanggil prosedur stub lokal. Prosedur Stub akan memberikan parameter dalam suatu paket yang akan dikirim ke jaringan. Proses ini disebut sebagai marshalling.
2. Fungsi Network pada O/S (Operating system - Sistem Operasi) akan dipanggil oleh stub untuk mengirim suatu message.
3. Kemudian Kernel ini akan mengirim message ke sistem remote. Kondisi ini dapat berupa connectionless atau connection-oriented.
4. Stub pada sisi server melakukan proses unmarshals pada paket yang dikirim pada nakan etwork.
5. Stub pada server kemudian mengeksekusi prosedur panggilan lokal.

6. Jika eksekusi prosedur ini telah selesai, maka eksekusi diberikan kembali ke stub pada server.
7. Stub server akan melakukan proses marshals lagi dan mengirimkan pesan nilai balikan (hasilnya) kembali ke jaringan.
8. Pesan ini akan dikirim kembali ke klien.
9. Stub klien akan membaca message ini dengan menggunakan fungsi pada jaringan.
10. Proses unmarshalled kemudian dilakukan pada pesan ini dan nilai balikan akan diambil untuk kemudian diproses pada proses lokal. Proses tersebut akan dilakukan berulang-ulang (rekursif) dalam pengeksekusian RPC dalam suatu remote system

2. Type Komunikasi

Ada beberapa macam type komunikasi yang dapat kita lakukanm diantaranya adalah :

1. **Komunikasi Sinkron (Serentak) /SsyncronousYiitu komunikasi secara langsung atau biasa disebut komunikasi secara online realtime.**
2. **Komunikasi Asinkron (Tidak Serentak)/Asyncronous Yaitu komunikasi secara online tidak realtime**



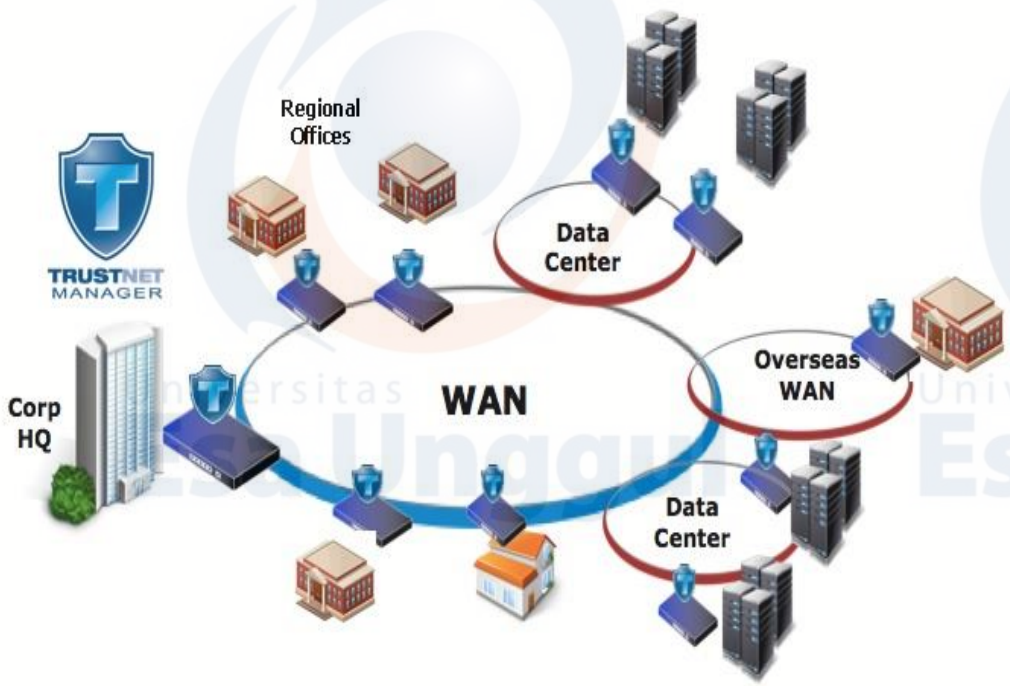
Gambar 5.2. Gambar pola pengiriman data Syncronous

Pengertian dari Asynchronous

Komunikasi online Tidak Langsung atau Asynchronous adalah mediasi computer dan layanan dari dalam terlaksanakannya komunikasi yang di lakukan secara tunda, dengan menggunakan media seperti e-mail, forum, dan membaca dan menulis dokumen online melalui World Wide Web.Asynchronous adalah Proses komunikasi data yang tidak terikat dengan waktu tetap, proses transformasi data kecepatannya cukup relatif dan tidak tetap.Metode komunikasi data serial dari suatu perangkat ke perangkat lainnya. Data dikirimkan perbit dalam satuan waktu. Tiap simbol yang dikirimkan mempunyai start bit dan stop bit, untuk melakukan singkronisasi dari suatu device pengirim dan penerima. Interval waktu yang terjadi antara satu karakter dengan karakter lainnya dapat bervariasi atau bermacam-macam.Transmisi asinkron digunakan apabila pengiriman data dilakukan satu karakter setiap kali pengiriman. Transmisinya dilakukan dengan cara memberikan bit awal (start bit)pada setiap awal pengiriman karakter dan diakhiri dengan bit akhir (stop bit).

Pengertian dari Synchronous

Komunikasi online **Langsung** atau Synchronous adalah mediasi computer dan layanan daring dalam terlaksanakannya komunikasi yang di lakukan secara langsung, dengan menggunakan media seperti Video Call dan Chat.Istilah yang digunakan pada bidang komunikasi atau sistem operasi untuk suatu kejadian yang terjadi pada waktu bersamaan dengan rate yang sama, dan kejadian ini terjadi berkelanjutan dan dapat diprediksi.Merupakan suatu pengiriman data yang dikirim dengan kecepatan tinggi dan data yang dikirim pada block, dimana setiap block data akan dicek ulang oleh : Block Check Character (BCC). Transmisi ini digunakan untuk transmisi data dengan kecepatan yang tinggi.



Gambar 5.3. Komunikasi secara Syncronous

Perbedaan antara Synchronous dan Asynchronous

Synchronous

proses pengirim dan penerima diatur sedemikian rupa sehingga memiliki pengaturan yang sama, sehingga dapat diterima dan dikirim denan baik. umumnya pengaturan ini didasarkan pada waktu

dalam mengirimkan sinyal. waktu ini diatur oleh denyut listrik secara periodik yang disebut *clock* . dengan kata lain synchronous adalah sistem operasi untuk kejadian yang terjadi pada waktu bersamaan, berkelanjutan dan dapat diprediksi. contoh: chating.

Asynchronous

proses komunikasi data yang tidak tergantung dengan waktu yang tetap. proses transformasi data kecepatanya. cukup relatif dan tidak tetap. metode komunikasi serial dari satu perangkat ke perangkat lainnya. data dikirimkan perbit persatuan waktu. tiap simbol yang dikirimkan mempunyai start bit dan stop bit, untuk melakukan sinkronisasi dari suatu device pengirim dan penerima. interval yang terjadi antar satu karakter dengan karakter lainnya dapat bervariasi. asynchronous merupakan operasi yang tidak bergantung waktu.

CONTOH dari Synchronous dan Asynchronous

- Perbedaan antara synchronous dengan asynchronous yang terutama tergantung dari ada tidaknya jeda antara pertukaran pesan dan fleksibilitas waktu antar pengguna komunikasi tersebut.

Synchronous

Proses pengirim dan penerima diatur sedemikian rupa sehingga memiliki pengaturan yang sama, sehingga dapat diterima dan dikirim denan baik. umumnya pengaturan ini didasarkan pada waktu dalam mengirimkan sinyal. waktu ini diatur oleh denyut listrik secara periodik yang disebut clock . dengan kata lain synchronous adalah sistem operasi untuk kejadian yang terjadi pada waktu bersamaan, berkelanjutan dan dapat diprediksi. contoh: chating

Keuntungan dan Kerugian

Apa keuntungan dan kerugian yang dihadirkannya?

Meskipun jenis komunikasi ini memiliki keuntungan besar, sehingga cakupan popularitasnya, penyalahgunaannya dapat menyebabkan serangkaian kelemahan. Di antara kelebihan dan kekurangan komunikasi sinkron adalah:

1. Keuntungan

Keuntungan utama adalah sebagai berikut.

Ini memungkinkan kita menghasilkan komunikasi atau dialog dengan orang lain dimanapun mereka berada , yang memungkinkan komunikasi instan di tingkat internasional.

Mengaktifkan pelestarian file interaksi

Ini memungkinkan penyimpanan informasi visual atau auditori yang dipertukarkan.

Memungkinkan kerja tim tanpa orang harus bertemu di tempat yang sama .

Ini adalah ruang pertemuan dan memfasilitasi interaksi antara orang-orang dengan minat yang sama.

2. Kekurangan

Di antara kerugian yang terkait dengan komunikasi sinkron.

- Dalam hal komunikasi tertulis, kurangnya konteks atau ketidakmampuan untuk memahami nada orang lain dapat menyebabkan kesalahpahaman atau kebingungan.
- Kurangnya aturan interaksi atau kurangnya pertimbangan Ini dapat menyebabkan kejenuhan orang tersebut. Yang mungkin merasa harus menjawab setiap saat.
- Membutuhkan pembaruan konstan seiring kemajuan teknologi

- Itu dapat menghasilkan ketergantungan dan kebutuhan untuk tetap berhubungan dengan orang lain

Gambar 5.4 : Komunikasi Syncronous

Asynchronous

Pproses komunikasi data yang tidak tergantung dengan waktu yang tetap. proses transformasi data kecepatanya. cukup relatif dan tidak tetap. metode komunikasi serial dari satu perangkat ke perangkat lainnya. data dikirimkan perbit persatuan waktu. tiap simbol yang dikirimkan mempunyai start bit dan stop bit, untuk melakukan sinkronisasi dari suatu device pengirim dan penerima. interval yang terjadi antar satu karakter dengan karakter lainnya dapat bervariasi. asynchronous merupakan operasi yang tidak bergantung waktu.Asynchronous sering disebut juga sebagai Asynchronous Transfer Mode (ATM). mode ini paling sering digunakan dalam mengirimkan dan menerima data antar 2 alat. pada mode ini berarti clock yang digunakan oleh kedua alat tidak bekerja selaras satu

dengan yang lainnya. dengan demnikian data harus berisikan informasi tambahan yang mengijinkan kedua lata kapan menyetujui kapan pengiriman alat dilakukan. contoh: modem, mesin fax, TCP/IP, mail, buletin board, dll.

C. Latihan

a. Jelaskan pengertian Komunikasi dan sebutkan jenis jeninya

b. Sebutkan apa itu protokol dan jelaskan layer layernya.

c. Latihan soal ke-n

D. Kunci Jawaban

a. Jawaban latihan soal ke-1

Komunikasi adalah suatu proses penyampaian informasi (pesan, ide, gagasan) dari satu pihak kepada pihak lain. Pada umumnya, komunikasi dilakukan secara lisan atau verbal yang dapat dimengerti oleh kedua belah pihak. Dimana proses komunikasi dapat dilakukan kepada orang, kelompok, organisasi dan masyarakat menciptakan, dan menggunakan informasi agar terhubung dengan lingkungan dan orang lain.Komunikasi memiliki komponen-komponen yang menjadikan komunikasi berjalan dengan baik,

Jenis jenis Komunikasi :

-Komunikasi secara Syncronous

-Komunikasi secaa Ansyncronous

b. Jawaban latihan soal ke-2

Potokol OSI dengan 7 Layer

1. Physical Layer
2. Data Link
3. Network
4. Transport
5. Session

6. Presentation
7. Application.

c. Jawaban latihan soal ke-n

D. Daftar Pustaka

1. Couloris et. al. 2012. Distributed Systems Concepts and Design, Fifth Edition. Addison Wesley.
2. Van Steen and Tanenbaum, 2017. Distributed Systems: Prinsiples and Paradigms. 3e. Prentice-Hall

Link :

https://www.goodreads.com/book/show/405614.Distributed_Systems

https://www.goodreads.com/search?q=process+in+distributed+data+processing&qid=pNFFKZD0Uu

MODUL PEMROSESAN DATA TERSEBAR

(PTI-611)

MODUL SESI 6

NAME SERVICE

DISUSUN OLEH

HERMANSYAH S.Kom., M.Kom.

UNIVERSITAS ESA UNGGUL

2020

PENGERTIAN NAME SERVICE

A. Kemampuan Akhir Yang Diharapkan

Setelah mempelajari modul ini, diharapkan mahasiswa mampu :

1. Memahami tata cara penamaan dan pendistribusiannya dalam DDP
2. Mahasiswa dapat memahami penamaan DNS dan hierarki pendistribusiannya di DDP

B. Uraian dan Contoh

1. Pengertian Name Service

NAME SERVICE

Pengertian Name Service

Name Service dalam Sistem Terdistribusi merupakan layanan penamaan yang berfungsi untuk menyimpan *naming context*, yakni kumpulan *binding* nama dengan objek, tugasnya untuk me-*resolve* nama.

Pengaksesan *resource* pada sistem terdistribusi memerlukan:

- Nama *resource* (untuk pemanggilan),
- Alamat (lokasi *resource* tsb),
- Rute (bagaimana mencapai lokasi tsb).

Name Service memiliki konsentrasi pada aspek penamaan dan pemetaan antara nama & alamat, bukan pada masalah rute, yang dibahas di Jaringan Komputer. *Resource* yang dipakai dalam *Name Service* adalah: komputer, layanan, *remote object*, berkas, pemakai.

Contoh penamaan pada aplikasi sistem terdistribusi:

– URL untuk mengakses suatu halaman web.

– Alamat e-mail utk komunikasi antar pemakai.

Name Resolution, Binding, Attributes

***Name resolution*:**

Nama ditranslasikan ke data ttg *resource/object* tsb.

***Binding*:**

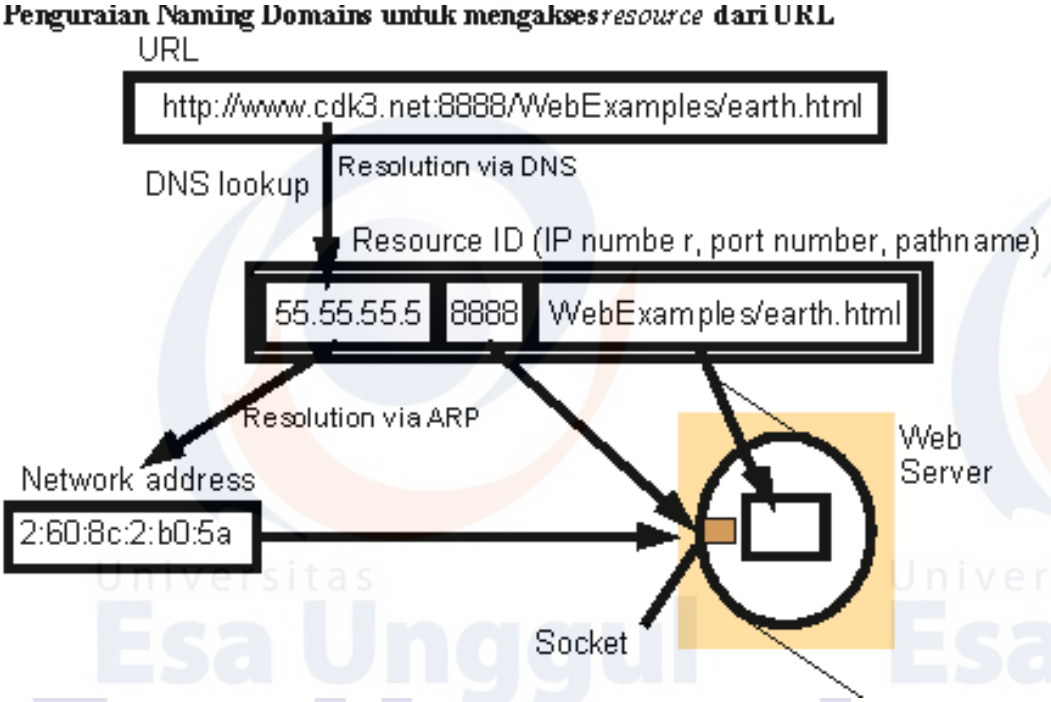
Asosiasi antara nama & obyek.

Biasanya nama diikat (*bound*) ke *attributes* dr suatu obyek.

***Address*:** atribut kunci dari sebuah entitas dalam sistem terdistribusi

***Attribute*:** nilai suatu *object property*.

Penguraian Naming Domains untuk mengakses *resource* dari URL



Tujuan Penamaan

Identifikasi

- Seorang pemakai menginginkan obyek/layanan A, bukan obyek/layanan B.

Memungkinkan terjadinya *sharing*

- Lebih dari satu pemakai dapat mengindentifikasikan *resource* dengan nama yang sesuai (tidak harus nama yang sama).

Memungkinkan *location independence:*

- Perubahan lokasi tidak menuntut perubahan nama, asalkan lokasi tidak menjadi bagian dari nama *resource* tsb.

Memberikan kemampuan keamanan (*security)*

- Jika sebuah nama dipilih secara acak dari himpunan besar *interger*, maka nama tsb hanya bisa diketahui dari *legitimate source*, bukan dari menebak. Jadi jika seseorang mengetahui nama obyek tsb, maka dia memang diberitahu, karena sulit sekali menebak nama tsb.

Domain Name System

Domain Name System merupakan sebuah name service sebagai standart penamaan pada Internet. Hal itu ditemukan oleh Mockapertis (1987) untuk menggantikan skema penamaan original, dimana semua hal dilakukan oleh satu central master file dan di download oleh FTP untuk semua computer yang membutuhkannya.

Database DNS diterapkan dengan sistem partitioning yang terbagi-bagi dalam suatu zone berdasar domainnya dan letak geografis. Top level organizational domain (biasa disebut generic domains) yang digunakan saat ini antara lain :

- DNS merupakan sistem berbentuk database terdistribusi yang akan memetakan/mengkonversikan nama host/mesin/domain ke alamat IP (Internet Protocol) dan sebaliknya dari alamat IP ke nama host yang disebut dengan reverse-mapping.
- Penggunaan :
  - Untuk memetakan nama mesin misal www.univrab.ac.id ke alamat IP misal 202.154.187.5
  - Untuk routing e-mail, telnet, ftp, web, dan lain-lain.

DNS sebagai jembatan

- Manusia lebih mudah untuk mengingat nama daripada alamat IP dengan panjang 32 bit itu.
- Komputer menggunakan alamat IP untuk berkomunikasi dan berinteraksi.

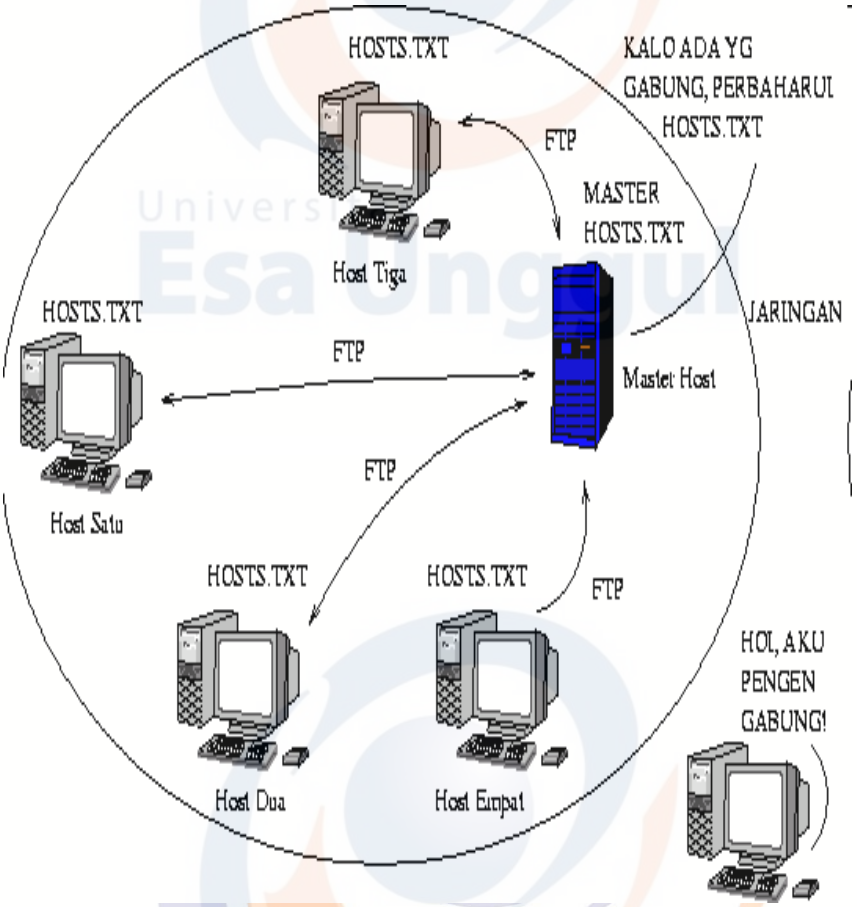
- DNS tidak diperlukan jika kita bisa mengingat ratusan, ribuan, bahkan jutaan alamat IP di Internet.

Uraian sub topik ke-1

2. History DNS

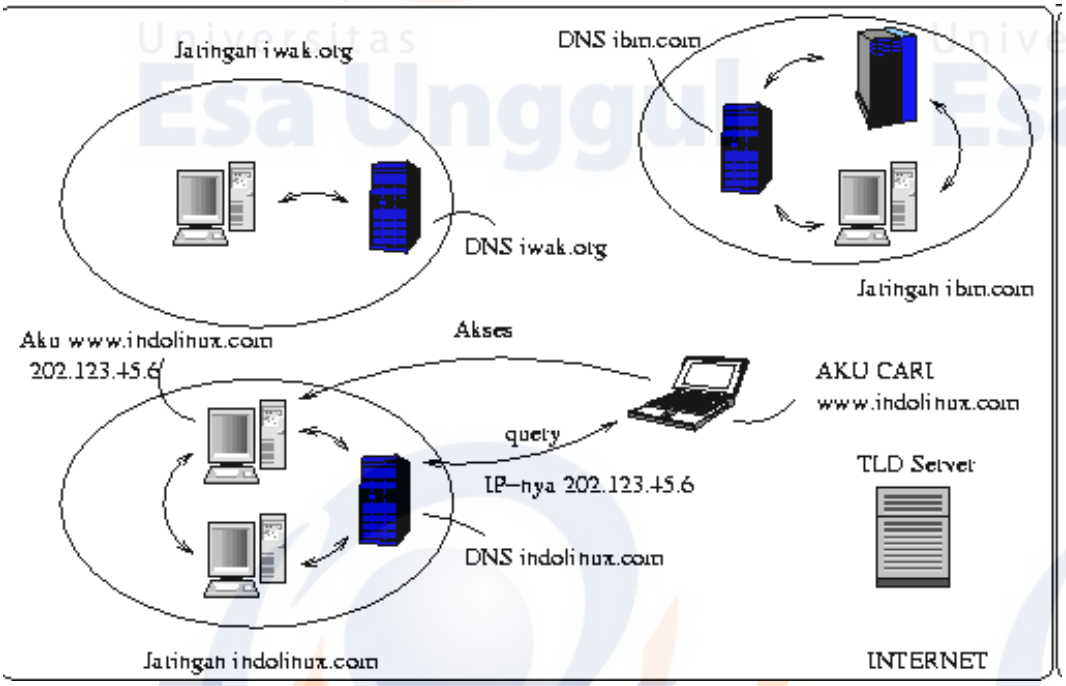
History

- Sebelum adanya DNS, tahun 1970-an ARPAnet menggunakan pemetaan dengan bentuk tabel host pada berkas HOSTS.TXT
- HOSTS.TXT berisi nama host dan alamat IP serta pemetaannya dari seluruh mesin/komputer yang terhubung dalam jaringan.
- Ketika ada komputer lain yang terhubung ke jaringan ARPAnet maka masing-masing komputer dalam jaringan tersebut harus memperbaharui berkas HOSTS.TXT-nya.
- Cara meng-update berkas HOSTS.TXT dengan menggunakan ftp setiap satu atau dua minggu sekali.
- Masalah ketika jaringan menjadi semakin besar. Kesulitan meng-update isi berkas HOSTS.TXT karena jumlah nama mesin/komputer yang dituliskan sudah terlalu besar dan tidak efisien.



- Muncul ide untuk membuat sistem database terdistribusi yang mempunyai data mengenai pemetaan nama host ke alamat IP dan sebaliknya.
- Dengan adanya pendistribusian database nama host dan alamat IP, maka tiap organisasi yang memiliki jaringan di dalam domain tertentu hanya bertanggung jawab terhadap database informasi pemetaan nama host dan alamat IP pada jaringannya saja yang biasa disebut zone.
- Administrasi domain tersebut dilakukan secara lokal tetapi informasi itu dapat diakses oleh semua komputer di Internet.
- Karena sifat database yang terdistribusi ini, maka dibutuhkan suatu mekanisme pengaksesan informasi bagi host lain pada database yang terdistribusi untuk menemukan informasi host atau jaringan yang dipunyai oleh suatu organisasi.
- Dan pada tahun 1984, Paul Mockapetris mengusulkan sistem database terdistribusi ini dengan Domain Name System (DNS) yang dideskripsikan

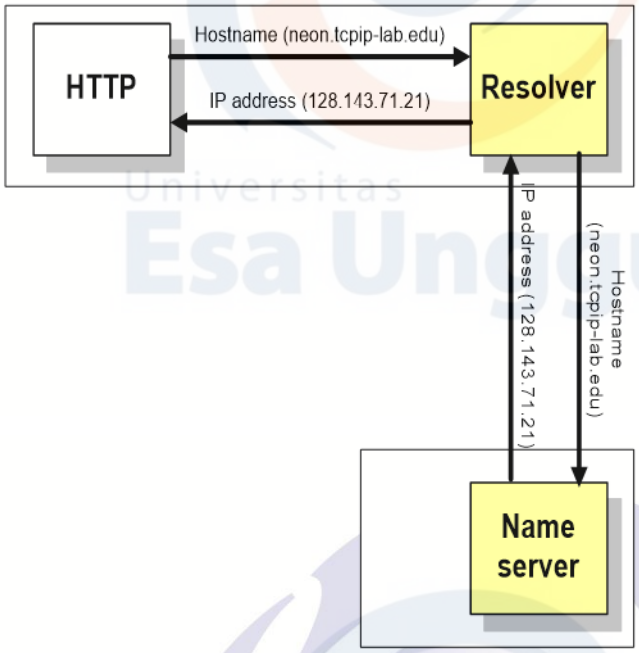
dalam RFC 882 dan 883. Sistem ini digunakan sampai sekarang pada jaringan khususnya Internet.



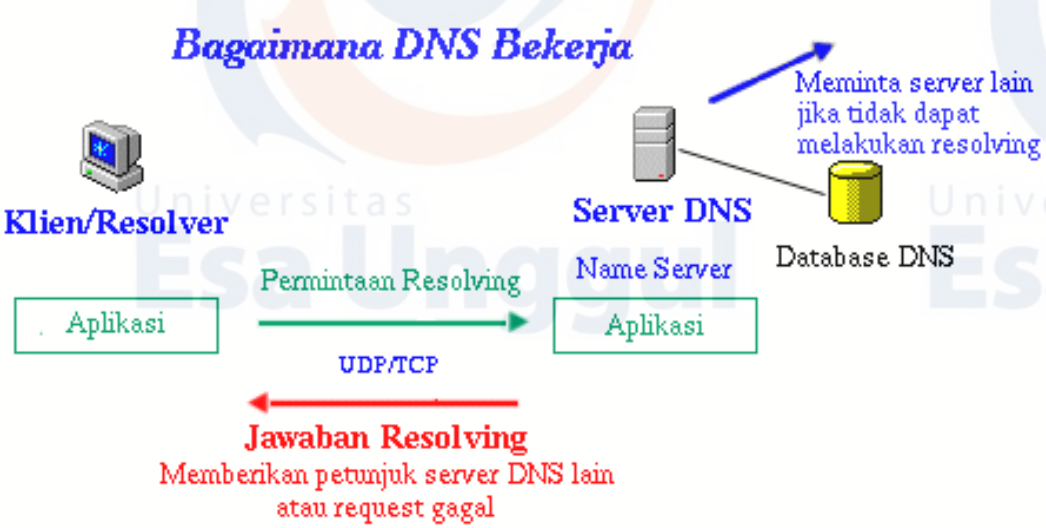
Resolver and name server

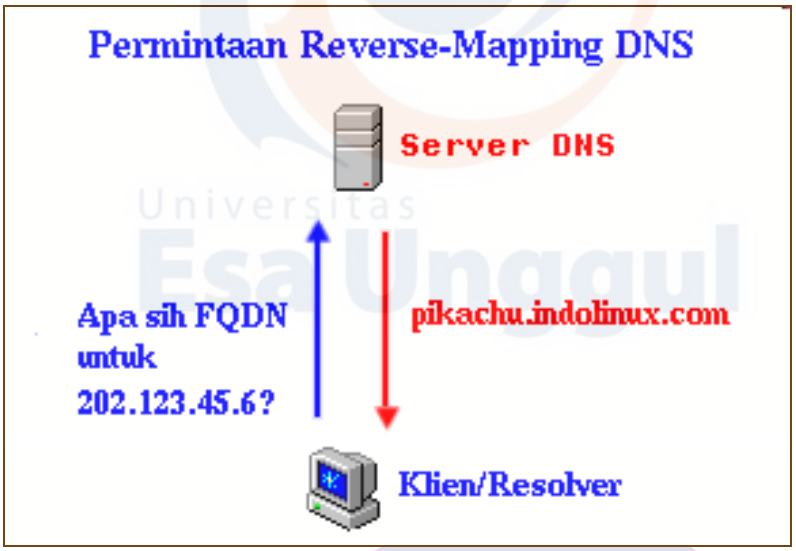
1. Sebuah program aplikasi pada host yang mengakses domain system disebut sebagai **resolver**
2. Resolver mengontak DNS server, yang biasa disebut name server
3. DNS server mengembalikan IP address ke resolver yang meneruskan ke aplikasi yang membutuhkan IP address

- Reverse lookups are also possible, i.e., find the hostname given an IP address


HTTP
Hostname (neon.tcpip-lab.edu)
IP address (128.143.71.21)
Resolver
IP address (128.143.71.21)
Hostname (neon.tcpip-lab.edu)
Name server

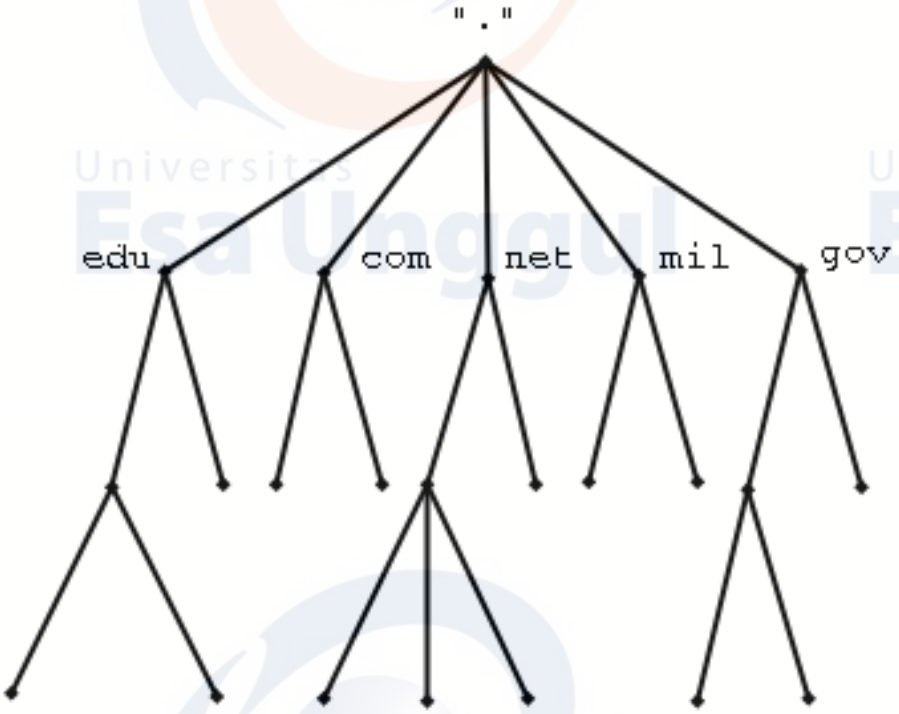
Kerja DNS

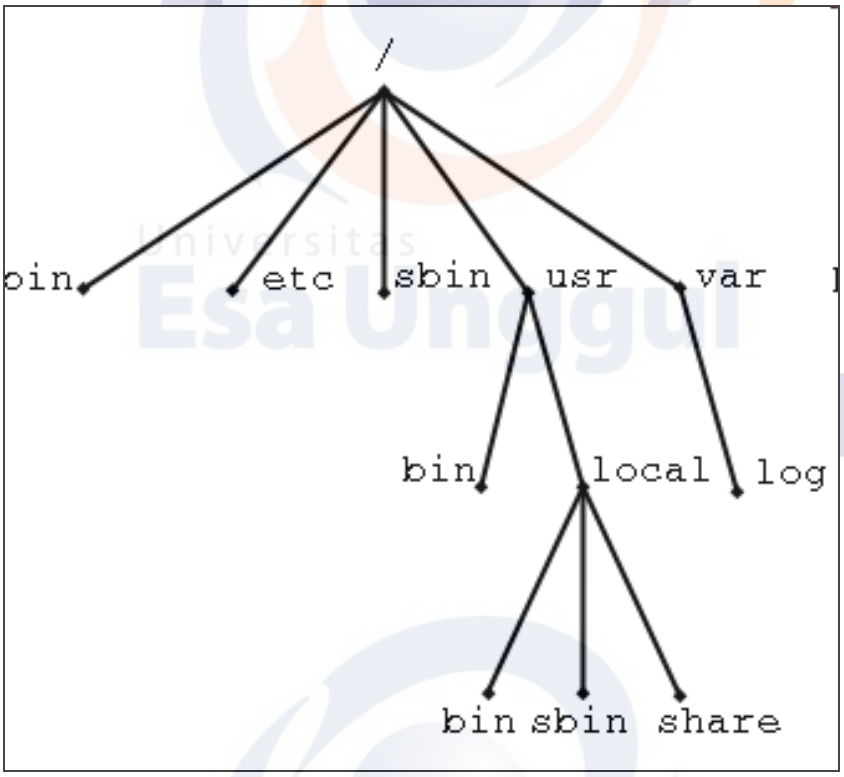

Bagaimana DNS Bekerja
Meminta server lain jika tidak dapat melakukan resolving
Klien/Resolver
Server DNS
Database DNS
Name Server
Permintaan Resolving
Aplikasi
Aplikasi
UDP/TCP
Jawaban Resolving
Memberikan petunjuk server DNS lain atau request gagal



Struktur

- Struktur database DNS mirip dengan sistem-berkas/filesystem UNIX yaitu berbentuk hierarki atau pohon.
- Tingkat teratas pada DNS adalah root yang disimbolkan dengan titik/dot (.) sedangkan pada sistem berkas UNIX, root disimbolkan dengan slash (/).
- Setiap titik cabang mempunyai label yang mengidentifikasikannya relatif terhadap root (.).
- Tiap titik cabang merupakan root bagi sub-tree/tingkat bawahnya.
- Tiap sub-tree merupakan domain dan dibawah domain terdapat sub-tree lagi bernama subdomain.
- Setiap domain mempunyai nama yang unik dan menunjukkan posisinya pada pohon DNS, pengurutan/penyebutan nama domain secara penuh dimulai dari domain paling bawah menuju ke root (.).
- Masing-masing nama yang membentuk suatu domain dipisahkan dengan titik/dot (.) dan diakhiri dengan titik yang merupakan nama absolut relatif terhadap root (.).





- Contoh: www.univrab.ac.id.
- "." merupakan root domain

- id merupakan Top Level Domain
- ac merupakan Second Level Domain
- its merupakan Third Level Domain
- www merupakan nama komputer/mesin yang bersangkutan
- Sistem penulisan nama secara absolut dan lengkap ini disebut FQDN (Fully Qualified Domain Name) - www.univrab.ac.id.

Hirarki

- Tiap organisasi yang telah mendaftar ke Network Information Center(NIC) akan mendapatkan nama domain sesuai dengan organisasi tersebut.
- Nama domain tersebut bisa dibagi menjadi subdomain sesuai kebutuhan organisasi.
- www.univrab.ac.id
- rabit.univrab.ac.id
- Dengan adanya sistem berbentuk hierarki/pohon ini maka tidak ada nama host yang sama pada domain/subdomain yang sama, karena masing-masing dari node/titik-cabang mempunyai nama unik dan tidak boleh ada yang menyamainya kecuali berbeda sub-tree/sub pohon.
- Tidak akan ada konflik antar organisasi karena masing-masing organisasi mempunyai domain yang berbeda-beda dan ini diatur oleh InterNIC untuk TLD.
- Kedalaman pohon dibatasi sampai level 127

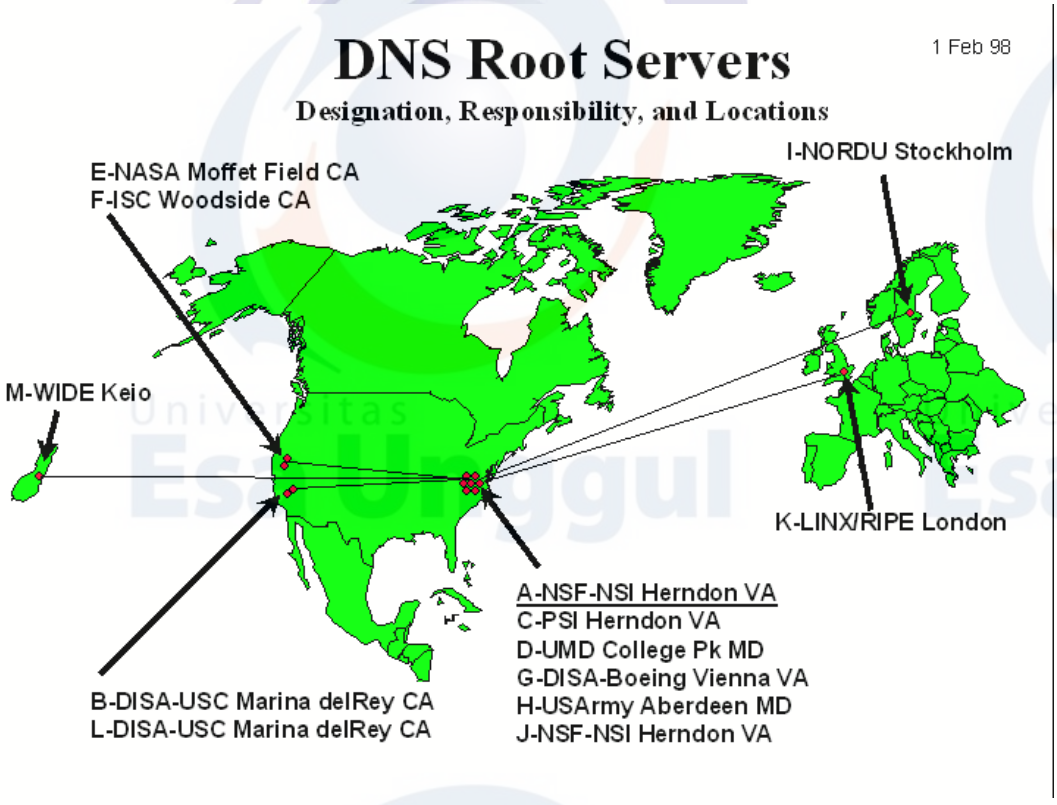
Top Level Domain (TLD)

- Domain Generik
  - com , net , gov , mil , org , edu , int
  - Selain 7 domain di atas ada lagi 7 domain baru dari ICANN (www.icann.org) yaitu: aero, biz , coop , info , museum , name , pro
- Domain Negara

- Contoh: id untuk Indonesia, au untuk Australia, uk untuk Inggris, dan lain-lain.
- Domain negara ini dapat dan umumnya diturunkan lagi ke level-level di bawahnya yang diatur oleh NIC dari masing-masing negara, untuk Indonesia yaitu IDNIC. Contoh level bawah dari id yaitu net.id, co.id, web.id.

Root name servers

- Server root digunakan untuk menemukan authoritative name servers untuk semua zona top-level.
- Ada 13 server root
- Digunakan untuk name resolution



Com - organisasi komersial

Edu - institusi pendidikan

Gov - institusi pemerintahan

Mil- organisasi militer

Net- Network support center

Org - Organisasi tertentu yang tidak disebutkan disini

Int - organisasi internasional

Us - United states

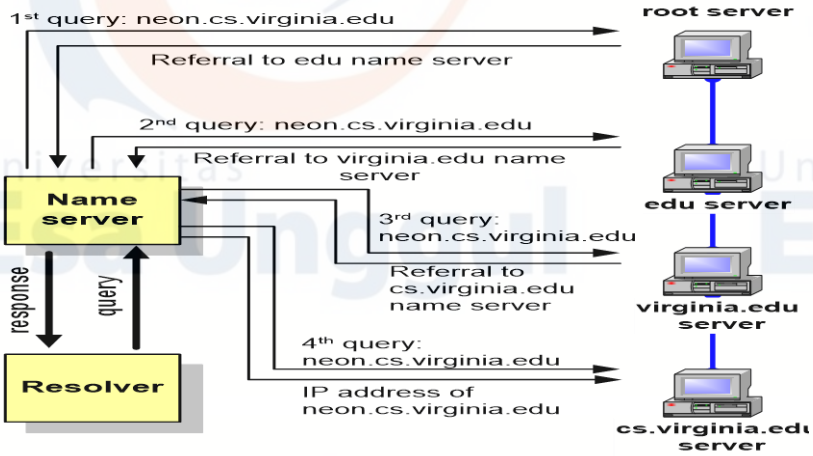
Uk - United kingdom

Id - Indonesian

Address root servers (2004)

A.ROOT-SERVERS.NET.	(VeriSign, Dulles, VA)	198.41.0.4
B.ROOT-SERVERS.NET.	(ISI, Marina Del Rey CA)	192.228.79.201
C.ROOT-SERVERS.NET.	(Cogent Communications)	192.33.4.12
D.ROOT-SERVERS.NET.	(University of Maryland)	128.8.10.90
E.ROOT-SERVERS.NET.	(Nasa Ames Research Center)	192.203.230.10
F.ROOT-SERVERS.NET.	(Internet Systems Consortium)	192.5.5.241
G.ROOT-SERVERS.NET.	(US Department of Defense)	192.112.36.4
H.ROOT-SERVERS.NET.	(US Army Research Lab)	128.63.2.53
I.ROOT-SERVERS.NET.	(Autonomica/NORDUnet)	192.36.148.17
J.ROOT-SERVERS.NET.	(Verisign, multiple cities)	192.58.128.30
K.ROOT-SERVERS.NET.	(RIPE,Europe multiple cities)	193.0.14.129
L.ROOT-SERVERS.NET.	(IANA, Los Angeles)	198.32.64.12
M.ROOT-SERVERS.NET.	(WIDE, Tokyo, Seoul, Paris)	202.12.27.33

Recursive queries



Caching

- Untuk mengurangi traffic, informasi mapping antara IP dan name servers disimpan di cache
- Ketika ada permintaan query server tidak perlu lagi menghubungi server lain

Resource Records

- Record database pada Database DNS terdistribusi disebut resource records (RR)
- Resource records disimpan pada file konfigurasi (zone files) pada name servers.

Berikut ini contoh sebuah zone Resource recordà

db.mylab.com

```
$TTL 86400
mylab.com. IN SOA PC4.mylab.com.
                  hostmaster.mylab.com. (
                  1 ; serial
                  28800 ; refresh
                  7200 ; retry
                  604800 ; expire
                  86400 ; ttl
                  )

;
mylab.com.   IN    NS    PC4.mylab.com.
;
localhost          A     127.0.0.1
PC4.mylab.com.     A     10.0.1.41
PC3.mylab.com.     A     10.0.1.31
PC2.mylab.com.     A     10.0.1.21
PC1.mvlab.com.     A     10.0.1.11
```

Resource Records

db.mylab.com

```
$TTL 86400
mylab.com. IN SOA PC4.mylab.com. hostmaster@mylab.com. (
                  1 ; serial
                  28800 ; refresh
                  7200 ; retry
                  604800 ; expire
                  86400 ; ttl
                  )
;
mylab.com.          IN        NS      PC4.mylab.com.
;
localhost                     A         127.0.0.1
PC4.mylab.com.      A         10.0.1.41
PC3.mylab.com.      A         10.0.1.31
PC2.mylab.com.      A         10.0.1.21
PC1.mylab.com.      A         10.0.1.11
```

Software

- Pada Redhat Linux yang sudah terinstall BIND (name server daemon) akan dijumpai beberapa file sebagai berikut :
- Di dalam /var/named akan ada 2 file yaitu :

- named.ca
- named.local

- Di dalam /etc akan terdapat file named.conf

File-File Konfigurasi

Standard

- named.conf di dalam /etc
- named.ca di dalam /var/named
- named.local di dalam /var/named

Jika ingin membuat master server maka harus ada:

- file zone -> mapping dari nama ke IP
- file reverse zone -> mapping dari IP ke nama

Named.conf

Blok dalam named.conf

options — List konfigurasi global dan default

include — berisi path file lain yang diperlukan

acl — IP address dalam access control list

server — properties khusus untuk remote servers

zone — informasi khusus untuk zona

1. Directory untuk menempatkan file zone

```
// generated by named-bootconf.pl

options {
directory "/var/named";
/*
* If there is a firewall between you and nameservers you want
* to talk to, you might need to uncomment the query-source
* directive below.  Previous versions of BIND always asked
* questions using port 53, but BIND 8.1 uses an unprivileged
* port by default.
*/
// query-source address * port 53;
};
```

2. Blok untuk mengatur akses

```
// a caching only nameserver config
//
controls {
inet 127.0.0.1 allow { localhost; };
};
```

3. Zone untuk root

```
zone "." IN {
type hint;
file "named.ca";
};
```

4. Zone untuk localhost

```
zone "localhost" IN {
type master;
file "localhost.zone";
allow-update { none; };
};
```

5. Zone untuk reverse address

```
zone "0.0.127.in-addr.arpa" IN {
        type master;
    file "named.local";
    allow-update { none; };
        };
```

Options

- **Biasanya ditaruh pada baris pertama named.conf**
- **Sintak :**

options {

value “property”;

}

options : allow-query

Menerima query hanya dari host dalam address yang sudah (default any host).

Penggunaan: allow-query {“address-list”};.

options : allow-transfer

Zone transfers menerima query hanya dari host dalam address yang sudah (default all host).

Penggunaan : allow-transfer {“address list”};.

options : directory

Tempat dimana file konfigurasi server berada.

Penggunaan: directory “path to directory”; (specify path).

options : forwarders

Menunjukkan IP addresses server untuk memforward query (default is none).

Penggunaan: forwarders “IP addresses of servers”; (specify IP addresses).

options : forward

Jika diset pertama kali, Server akan didaftar pada query forwarders pertama,

Penggunaan: forward “first or only”; (pilih salah satu).

options : listen-on

Port dimana server listen dari query yang ada (default is port 53).

Penggunaan : listen-on “port {address list}”;

options : recursion

Server secara recursive mencari jawaban query (default is yes).

Penggunaan: recursion “ yes or no”; (choose one).

Include

Acl

IP address dalam access control list. Hanya host yang terdaftar yang boleh akses ke server

```
acl "transferdns" {
        { 216.65.64.146/32; };
        { 209.25.238/24; };
        { 202.154.63.3/32; };
};
```

Named.ca

- Dikenal sebagai cache file untuk DNS
- Berisikan daftar world root servers

```
■;    This file holds the information on root name servers needed to
■;    initialize cache of Internet domain name servers
■;    (e.g. reference this file in the "cache  .  <file>"
■;    configuration file of BIND domain name servers).
■;
■;    This file is made available by InterNIC
■;    under anonymous FTP as
■;        file                /domain/named.cache
■;        on server           FTP.INTERNIC.NET
■;
■;    last update:    Nov 5, 2002
■;    related version of root zone:    2002110501
■;
■;
■; formerly NS.INTERNIC.NET
■;
■.                      3600000  IN  NS    A.ROOT-SERVERS.NET.
■A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
■;
■; formerly NS1.ISI.EDU
■;
■.                      3600000      NS    B.ROOT-SERVERS.NET.
■B.ROOT-SERVERS.NET.      3600000      A     128.9.0.107
■;
■; formerly C.PSI.NET
■;
■.                      3600000      NS    C.ROOT-SERVERS.NET.
■C.ROOT-SERVERS.NET.      3600000      A     192.33.4.12
■;
■; formerly TERP.UMD.EDU
■;
■.                      3600000      NS    D.ROOT-SERVERS.NET.
■D.ROOT-SERVERS.NET.      3600000      A     128.8.10.90
■;
■; formerly NS.NASA.GOV
■;
■.                      3600000      NS    E.ROOT-SERVERS.NET.
■E.ROOT-SERVERS.NET.      3600000      A     192.203.230.10
■;
■; formerly NS.ISC.ORG
■;
■.                      3600000      NS    F.ROOT-SERVERS.NET.
■F.ROOT-SERVERS.NET.      3600000      A     192.5.5.241
```

Named.local

- Berisikan informasi tentang localhost
- Berisikan info untuk me-resolv loopback address untuk localhost

```
@       IN    SOA    localhost. root.localhost.  (
                              1997022700 ; Serial
                              28800      ; Refresh
                              14400      ; Retry
                              3600000    ; Expire
                              86400 )    ; Minimum
              IN     NS     localhost.
1             IN     PTR    localhost.
```

Named.rev

- Menyediakan informasi untuk reserve lookups.
- Digunakan untuk mengetahui nama dari suatu host berdasarkan IP

```
63.154.202.in-addr.arpa. IN    SOA     ns1.pens-its.edu. admin.pens-its.edu.  (
                              2000081012 ; Serial
                              28800      ; Refresh
                              14400      ; Retry
                              3600000    ; Expire
                              86400 )    ; Minimum
              IN     NS     ns1.pens-its.edu.
              IN     NS     ns2.pens-its.edu.

4             IN     PTR    www.pens-its.edu.
5             IN     PTR    ies.pens-its.edu.
6             IN     PTR    elerning.pens-its.edu.
```

File ZONE

- File zone berisikan resource record (RR) tentang IP address
- File ZONE akan diawali oleh SOA yang merupakan penanda bahwa name server tersebut adalah merupakan sumber yang sah untuk domain tersebut
- SATU zone file HANYA akan punya SATU SOA

SOA

- Serial : Serial number dari file zone tersebut
- Refresh : waktu yang dibutuhkan untuk me-refresh data
- Retry : waktu yang dibutuhkan untuk menunggu sebelum berusaha mengontak server utama jika ada kegagalan
- Expire : jika secondary master gagal mengontak server utama dalam waktu ini maka database tentang domain tersebut akan dibuang
- TTL: Time to live untuk menentukan berapa lama data disimpan dalam cache

Resource Record

NS — NAME SERVERS

- Menunjukkan nama "name server".

A — THE IP ADDRESS FOR THE NAME

- Menunjukkan nomor IP "name server".

PTR — POINTER FOR ADDRESS NAME MAPPING

- Digunakan untuk menunjuk name server

CNAME — CANONICAL NAME

- Menunjukkan nama real host.

MX — MAIL EXCHANGE RECORD

- Menunjukkan sebagai mail server pada domain tersebut.

Dynamic DNS

- Suatu cara melakukan update DNS server tanpa harus melakukan restart terhadap konfigrasi DNS kita.
- Pada waktu konfigurasi DNS harus ada cara untuk mengupdate, Pada waktu suatu host hidup kita bisa menyediakan address via DHCP, kemudian DHCP meminta DNS untuk merubah record A dan PTR sesuai kebutuhan.
- Kolaborasi antara DNS dan DHCP
- Membutuhkan bind9 dan DHCP3
- Konfigurasi file utama : dhcpd.conf dan named.conf

Uraian sub topik ke-2

3. Sub sub topik ke-n

Uraian sub topik ke-n

C. Latihan

a. Sebutkan pengertian dan jenis jenis dari Name service
b. Apa yang dimaksud dengan DinamisDNS….?
c. Jelaskan apa yang dimaksud dengn Resources Record…?

D. Kunci Jawaban

a. Jawaban latihan soal ke-1

Pengertian Name Service

Name Service dalam Sistem Terdistribusi merupakan layanan penamaan yang berfungsi untuk menyimpan *naming context*, yakni kumpulan *binding* nama dengan objek, tugasnya untuk me-*resolve* nama.

b. Jawaban latihan soal ke-2

Dynamic DNS

- Suatu cara melakukan update DNS server tanpa harus melakukan restart terhadap konfigrasi DNS kita.
- Pada waktu konfigurasi DNS harus ada cara untuk mengupdate, Pada waktu suatu host hidup kita bisa menyediakan address via DHCP, kemudian DHCP meminta DNS untuk merubah record A dan PTR sesuai kebutuhan.
- Kolaborasi antara DNS dan DHCP
- Membutuhkan bind9 dan DHCP3
- Konfigurasi file utama : dhcpd.conf dan named.conf

c. Jawaban latihan soal ke-3

Catatan sumber daya, biasanya disebut sebagai RR, adalah unit entri informasi dalam file zona DNS; RR adalah blok bangunan dasar dari nama host dan informasi IP dan digunakan untuk menyelesaikan semua permintaan DNS. Catatan sumber daya ada karena banyak jenis untuk menyediakan layanan resolusi nama yang diperluas.

D. Daftar Pustaka

1. Couloris et. al. 2012. Distributed Systems Concepts and Design, Fifth Edition. Addison Wesley.
2. Van Steen and Tanenbaum, 2017. Distributed Systems: Prinsiples and Paradigms. 3e. Prentice-Hall

Link :

https://www.goodreads.com/book/show/405614.Distributed_Systems

https://www.goodreads.com/search?q=process+in+distributed+data+processing&qid=pNFFKZD0Uu

MODUL PEMROSESAN DATA TERSEBAR

(CPD 121)

MODUL SESI KE -7

SINKRONISASI

DALAM PEMROSESAN SATA TERSEBAR

DISUSUN OLEH

HERMANSYAH S.Kom., M.Kom.

UNIVERSITAS ESA UNGGUL

2020

PRNGERTIAN SINKRONISASI

A. Kemampuan Akhir Yang Diharapkan

Setelah mempelajari modul ini, diharapkan mahasiswa mampu :

1. Mahasiswa memahami perlunya sinkronisasi akibat perbedaan posisi letak bumi
2. Mahasiswa dapat memahami implementasi sinkronisasi dalam penerapannya ke GPS dan konsekuensi tidak selalu tersedianya bandwith untuk komunikasi

B. Uraian dan Contoh

1. **Pengertian Sinkronisasi**

SINKRONISASI

DALAM PEMROSESAN SATA TERSEBAR

Pengertian

Sinkronisasi adalah proses pengaturan jalannya beberapa proses pada saat yang bersamaan. Tujuan utama sinkronisasi adalah menghindari terjadinya inkonsitensi data karena pengaksesan oleh beberapa proses yang berbeda (mutual exclusion) serta untuk mengatur urutan jalannya proses-proses sehingga dapat berjalan dengan lancar dan terhindar dari deadlock dan starvation. Sinkronisasi umumnya dilakukan dengan bantuan perangkat sinkronisasi. Penyelesaian terhadap masalah ini sangat penting karena perkembangan teknologi sistem komputer menuju ke sistem multiprocessing, terdistribusi dan paralel yang mengharuskan adanya proses-proses kongkuren.

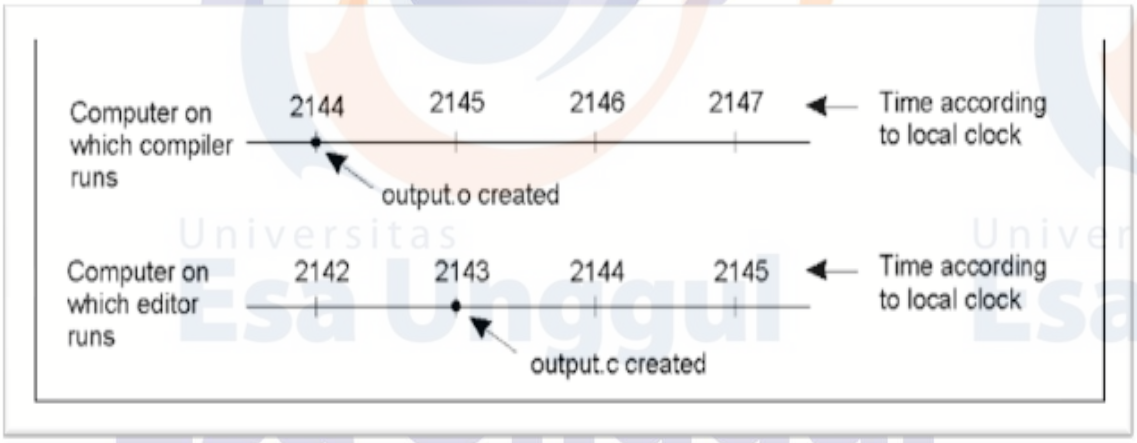
Sinkronisasi Clock

1. Algoritma untuk sinkronisasi dalam sistem terdistribusi memiliki beberapa sifat: Informasi yang relevan tersebar di beberapa computer
2. Keputusan pembuatan proses hanya berdasarkan informasi local.

3. Peristiwa kegagalan dengan penyebab tunggal di dalam sistem harus dihindarkan.
4. Tidak tersedianya clock atau sumber waktu global yang akurat.

Sikronisasi merupakan bagian penting untuk kerjasama dalam : Pemakaian sumberdaya berbagi (Sharing resources), pengurutan kejadian dan kesepakatan clock tersebar

Contoh Tidak Adanya Kesepakatan Clock Global



Gambar diatas menggambarkan bahwa bila waktu pada output o adalah 2144, Kemudian source codenya dimodifikasi di komputer lain yang clocknya lebih lambat, sehingga waktu source code adalah 2143. Karena source code memiliki waktu yang lebih lama daripada file objeknya, maka make tidak akan melakukan rekompilasi.

Sinkronisasi Straightforward

Cara yang paling mudah untuk menentukan waktu adalah dengan bertanya langsung ke server waktu (Universal Coordinated Time - UTC), hanya saja akan

banyak perbedaan dalam request . Karena waktu merupakan dasar dari cara orang berpikir, dan akibat tidak adanya sinkronisasi clock juga sangat dramatis, seperti yang dilihat pada contoh sebelumnya, sehingga wajar saja bila dalam pembahasan sikronisasi dimulai dengan pertanyaan sederhana :

Mungkinkah mensinkronkan semua clock yang ada dalam sistem tersebar ?

Clock logika

Boleh dikatakan semua komputer memiliki rangkaian pencatat waktu. Walaupun penggunakan kata Clock sudah meluas, kata yang lebih tepat adalah timer untuk merujuk komponen dari rangkaian tersebut. Timer ini menggunakan crystal quartz sebagai sumber frekuensinya. Walaupun frekuensi osilator pada osilator kristal biasanya stabil, tetap saja tidak mungkin menjamin bahwa semua kristal yang bekerja diberbagai komputer memiliki frekuensi yang persis sama.

Selalu ada sedikit perbedaan yang terjadi dan mengakibatkan perbedaan waktu pula yang disebut clock skew. Berbagai algoritma telah dikembangkan untuk menangani sinkronisasi clock dan beberapanya akan dibahas berikut ini.

Algoritma Lamport

• Menurut Lamport, sikronisasi clock tidak harus dilakukan dengan nilai mutlak clocknya, karena yang diperlukan dalam sikronisasi proses-proses adalah urutan proses tersebut.Jadi yang dipentingkan adalah konsistensi internal clock, bukan apakah clock tersebut harus sama persis dengan waktu real.

Clock jenis ini biasanya disebut clock logika.

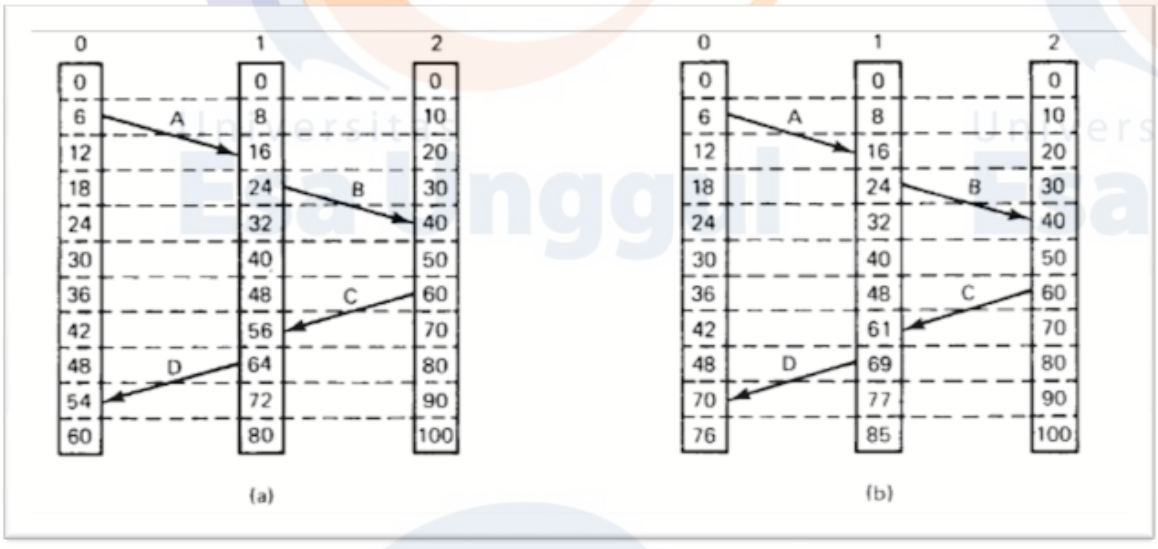
Pengurutan peristiwa

Sejumlah problem yang penting akan terpecahkan bila pegurutan peristiwa yang jelas dapat dibuat, bahkan bila waktu realnya tidak diketahui. Untuk mensinkronkan clock logika Lamport mendefinisikan relasi yang disebut happened-before.

Ekspresi a-> b dibaca “a terjadi sebelum b” dan artinya semua proses sepakat bahwa kejadian pertama adalah a, di ikuti sesudahnya kejadian b. Relasi happen-before dapat diamati langsung dalam dua situasi

1. Bila a dan b adalah kejadian (event) dalam proses yang sama, dan a terjadi sebelum b, maka a-> b adalah true.
2. Bila a adalah kejadian dari sebuah pesan yang dikirim oleh sebuah proses,dan b adalah kejadian dimana pesan tersebut diterima oleh proses lain,maka a-> b adalah true juga.

Gbr: Sinkronisasi Clock Logika dengan Lamport



- Bila a adalah kejadian dari sebuah pesan yang dikirim oleh sebuah proses,dan b adalah kejadian dimana pesan tersebut diterima oleh proses lain,maka a-> b adalah true juga.

- Pada gambar (a) tampak tiga buah sistem dengan clock Masing – masing yang bekerja dengan laju yang berbeda, dan gambar (b) clock sistem dikoreksi dengan algoritma Lamport.
- Cara untuk menetapkan waktu ke semua kejadian dalam sistem tersebar tergantung pada kondisi berikut:

- Bila a terjadi sebelum b di proses yang sama , C(a) < C(b).
- Bila a dan b mewakili kejadian pengiriman dan penerimaan pesan, maka C(a) < C(b)
- Untuk semua kejadian a dan b, C(a) <> C(b)

Clock fisik

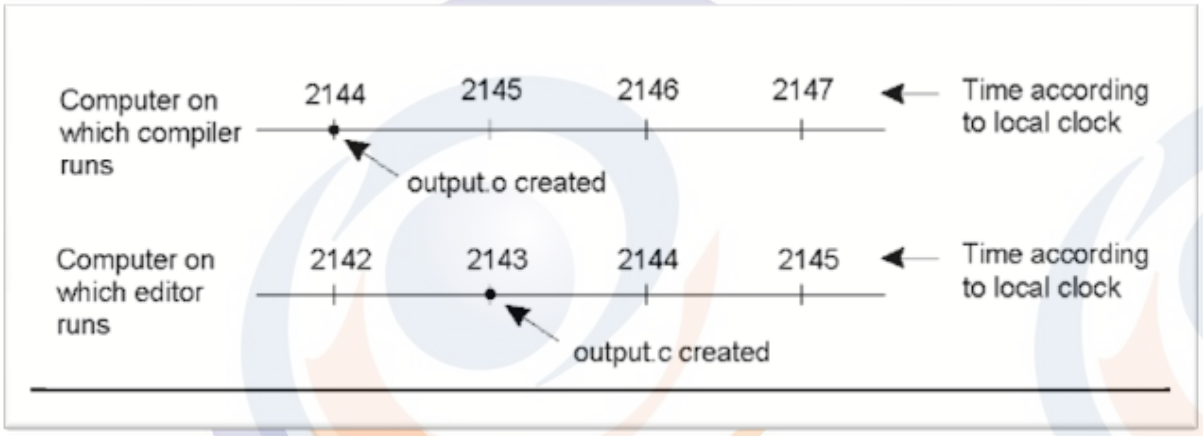
Pada beberapa sistem, waktu clock aktual menjadi penting, contohnya real – time sistem. Untuk sistem ini diperlukan clock fisik eksternal. Karena alasan efisiensi dan redundansi, clock fisik jamak biasanya digunakan, yang mengakibatkan ada dua masalah muncul:

Bagaimana mensinkronkan eksternal clock tersebut dengan clock sebenarnya - Bagaimana mensinkronkan antar clock yang ada. Sebelum membahas jawaban masalah di atas, terlebih dahulu dilihat bagaimana pengukuran waktu aktual dilakukan.

- Saat dimana matahari mencapai titik tertinggi di langit disebut transit of the sun, dan terjadi di siang hari. Interval antar dua transit berturutan disebut solar day. Sedangkan solar second didefinisikan tepat 1/86400 dari solar day.
- International Atomic Time (disingkat IAT) adalah rata-rata jumlah tick dari jam atom cesium 133 sejak tanggal 1 januari 1958 dibagi 9.192.631.770.

- Disebabkan waktu siang bertambah lama, TAI menjadi lebih lambat dibanding solar second. Untuk mengkoreksinya, digunakan leap second dengan cara meloncati waktu TAI sehingga sama dengan solar second (lihat gambar). Waktu yang telah dikoreksi ini disebut Universal Coordinated Time UTC).

NIST memiliki beberapa stasiun radio gelombang pendek yang memancarkan pulsa pada setiap awal detik UTC, yang dapat digunakan untuk sinkronisasi. Stasiun ini dikenal dengan nama WWV



Penggunaan Clock Sinkron

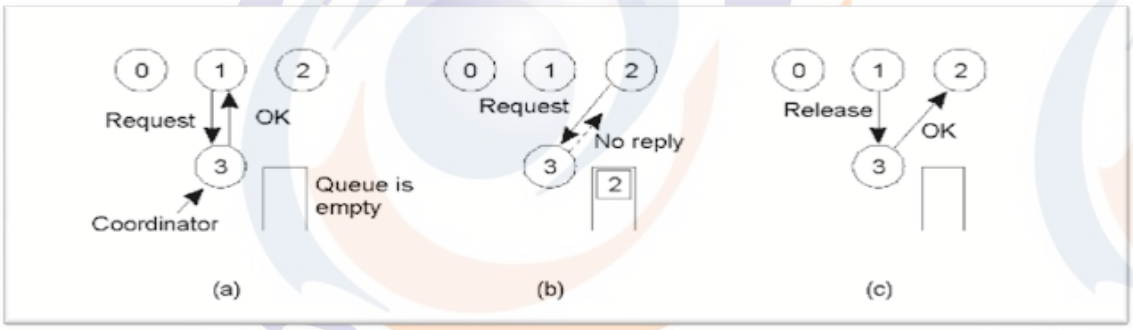
Pelaksanaan sinkronisasi clock dalam skala luas terjadi baru -baru ini saja, yang salah satu teknologi enabling - nya adalah internet. Adalah mungkin mensinkronkan jutaan clock dalam orde milidetik dengan UTC. Berbagai algoritma baru yang menggunakan clock sinkron mulai bermunculan, berikut ini contohnya.

1. A**t-Most-Once Message Delivery**

Setiap pesan membawa pengenal koneksi dan timestamp. Untuk setiap koneksi, server menyimpan timestamp terbaru ke dalam tabel. Bila ada pesan masuk dengan timestamp yang lebih lama daripada Timestamp yang disimpan, maka pesan tersebut akan ditolak dan dianggap sebagai duplikat.

2. **Konsistensi Cache Berbasis Clock**

Konsistensi cache dalam file System tersebar menjadi perhatian karena setiap client menginginkan cache file di lokal komputer. Bila dua komputer memodifikasi file secara bersamaan, berpotensi menyebabkan inkonsistensi. Pada algoritma terpusat, kondisi mutual exclusion (mutex) ditangani oleh sebuah proses yang dipilih sebagai koordinator untuk mengatur entry ke critical region. Setiap proses yang ingin meminta mutex mengirim pesan request ke koordinator. Bila proses tersebut menerima pesan reply dari koordinator maka proses tersebut diijinkan masuk ke daerah kritis. Sesudah keluar dari daerah kritis, proses mengirim pesan release ke koordinator dan melanjutkan eksekusinya.



- Proses 1 meminta ijin (request) ke koordinator untuk masuk ke critical region. Ijin diberikan (grant).
- Proses 2 meminta ijin ke koordinator untuk masuk ke critical region yang sama. Koordinator tidak menjawab.
- Bila proses 1 keluar dari critical region, proses tersebut memberitahu (release) koordinator yang kemudian mengijinkan proses

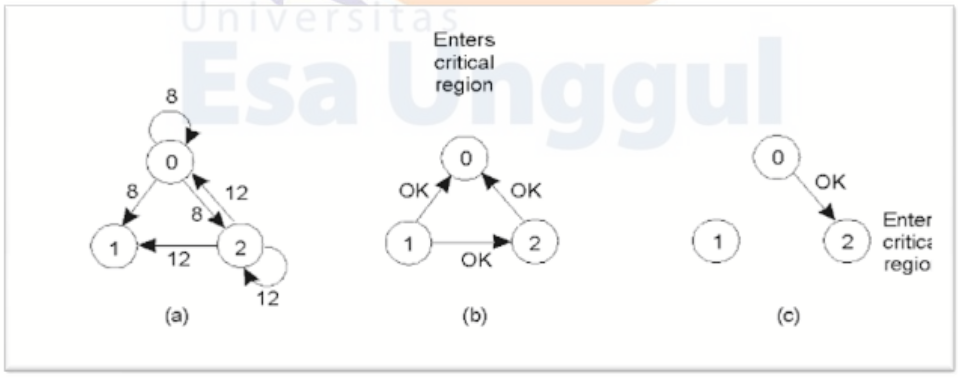
Algoritma Tersebar

Kejadian kegagalan karena penyebab tunggal tidak dapat ditoleransi dalam sistem tersebar, sehingga para peneliti mengembangkan berbagai algoritma mutual

exclusion tersebar. Algoritma ini bekerja dengan membuat sebuah proses yang ingin memasuki daerah kritis , terlebih dulu membuat pesan yang berisi nama daerah kritis yang ingin dimasuki, nomor proses dan waktu terkininya.

Pesan ini dikirim ke semua proses dengan asumsi komunikasi yang digunakan reliable. Bila sebuah proses menerima pesan request dari proses yang lain, respon yang diberikan tergantung dari state proses terhadap nama daerah kritis yang dalam pesan tersebut. Ada tiga kasus penerima yang mungkin yaitu:

1. Bila penerima tidak berada dalam daerah kritis dan tidak ingin masuk, maka pesan Ok dikirim balik.
2. Bila penerima sudah berada di dalam daerah kritis, maka tidak ada pesan yang dikirim.
3. Bila penerima ingin masuk ke daerah kritis tapi belum masuk, maka proses ini akan membandingkan catatan waktu dari pesan masuk dengan pesan yang dikirimkan. Bila pesan masuk memiliki catatan lebih lama, penerima akan membalas dengan pesan OK. Sebaliknya bila pesannya sendiri memiliki catatan waktu yang lebih lama maka penerima akan meletakkan pesan masuk ke antrian dan tidak membalas apapun.



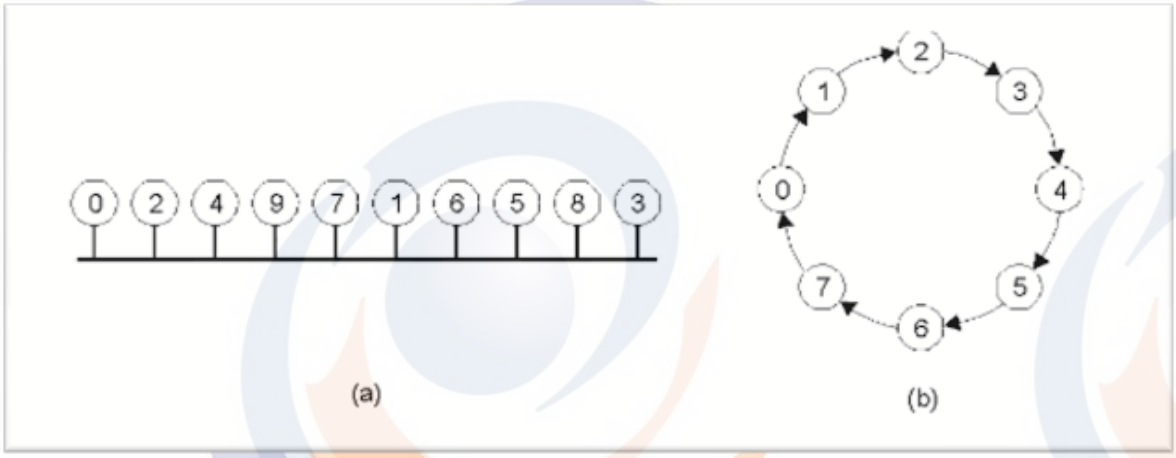
- Dua proses ingin masuk ke daerah kritis yang sama pada waktu yang bersamaan pula.
- Proses 0 memiliki timestamp yang lebih lama sehingga proses 0 menang.

• Bila proses 0 selesai, pesan OK dikirim sehingga proses 2 sekarang dapat masuk ke daerah kritis.

Algoritma Token Ring

Disini digunakan sebuah jaringan bus dengan proses - proses yang tidak berurutan. Melalui perangkat lunak, ring logika disusun dengan setiap proses ditetapkan posisinya di dalam ring seperti pada gambar b. Posisi ring dapat dialokasikan dengan menggunakan urutan nomor alamat jaringan atau dengan cara lain.

Hal yang terpenting adalah setiap proses harus tahu siapa proses sesudahnya



- Sebuah grup proses yang tidak berurut dalam jaringan.
- Ring logika yang disusun dalam software perbandingan Tiga Algoritma

Uraian sub topik ke-1

2. Perbandingan 3 Algoritma

Perbandingan Tiga Algoritma

Algoritma terpusat paling mudah dan efisien dibanding kedua algoritma lainnya. Hanya tiga proses yang dibutuhkan untuk masuk dan keluar dari daerah kritis: Request , grant dan release. Algoritma tersebar paling sensitif terhadap kejadian crash.

Algoritma	Pesan per entry/exit	Delay sebelum entry (in message times)	Problem
Terpusat	3	2	Koordinator *crash*
Tersebar	2 (n-1)	2 (n-1)	Proses *crash*
Token Ring	1 to infinity	0 to n-1	Token hilang,proses *crash*

Algoritma Pemilihan

Banyak algoritma tersebar membutuhkan sebuah proses yang berfungsi sebagai koordinator, inisiator, sekuenser, atau pelaksana fungsi khusus lain. Beberapa contoh seperti koordinator pada algoritma mutual exclusion terpusat. Bila koordinator tersebut mengalami kegagalan karena hostnya down, sistem harus dapat melanjutkan eksekusi hanya dengan memulai lagi sebuah copy proses koordinator baru di host yang lain. Algoritma yang menentukan dimana copy koordinator baru tersebut harus dimulai lagi disebut algoritma pemilihan.

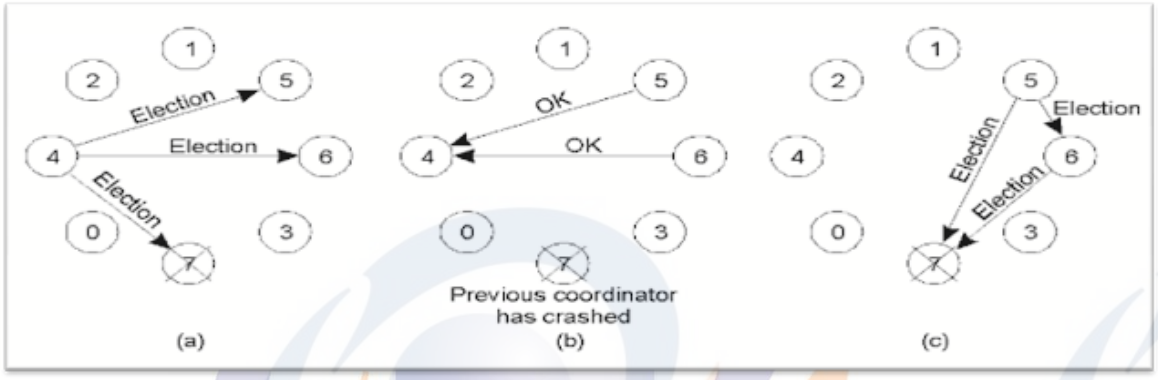
Ada dua algoritma pemilihan yang akan dibahas untuk dua jenis konfigurasi sistem tersebar.

1. Algoritma Bully

Bila sebuah proses mendapatkan koordinator tidak lagi menanggapi request yang dikirim, maka proses pemilihan akan diinisiasi. Proses P mengadakan pemilihan sebagai berikut:

- P mengirim pesan ELECTION ke semua proses dengan nomor proses yang lebih besar.
- Bila tidak ada tanggapan, proses P memenangkan pemilihan ini dan menjadi koordinator.

- Namun bila salah satu proses dengan nomor yang lebih tinggi menjawab, proses tersebutlah yang akan mengambil alih proses pemilihan. Pekerjaan proses P sendiri selesai disini.



• Dalam gambar proses pemilihan dengan algoritma bully dapat dilihat sebagai berikut - Proses 4 mengadakan pemilihan
(ELECTION)

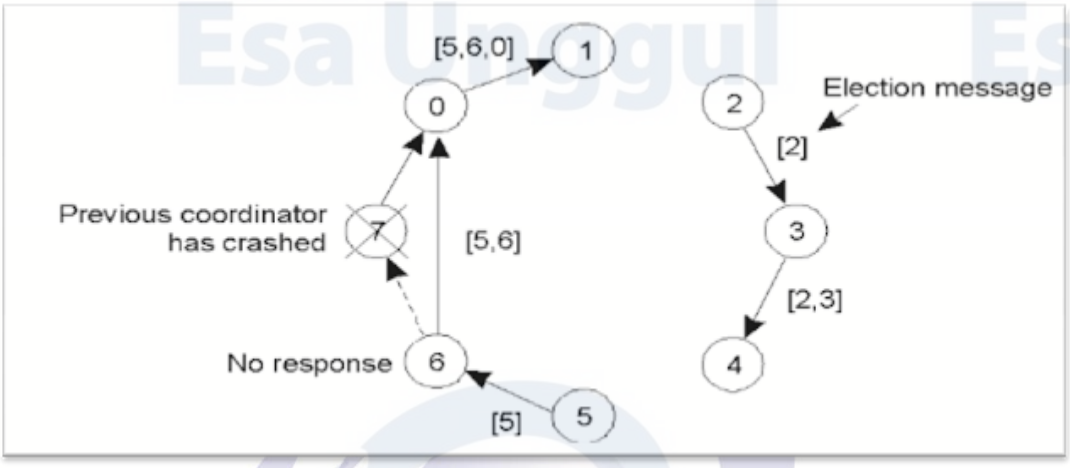
- Proses 5 dan 6 merespon, memberitahu 4 untuk berhenti
- Sekarang 5 dan 6 masing-masing akan mengadakan pemilihan

2 Algoritma Ring

• Algoritma ini berbasis ring tanpa token, dengan ersyaratan bahwa setiap proses harus sudah berurutan baik secara logika ataupun fisik. Bila sebuah proses mendapatkan koordinatornya tidak berfungsi, maka pesan ELECTION yang berisi nomor prosesnya dikirim ke proses berikut yang lebih tinggi nomornya.

Dalam gambar dibwah terlihat bahwa proses 2 dan 5 mendapatkan proses 7 yang berperan sebagai koordinator mengalamicrash. Kemudian proses 2 dan 5 membangun pesan ELECTION dan memulai sirkulasi pesan ini. Akhirnya pesan tersebut akan tersebar ke segala arah, kemudian kedua proses 2 dan 5 akan

mengubah pesan tersebut menjadi pesan COORDINATOR yang disirkulasikan lagi, dengan anggota dan urutan ring yang tepat sama seperti sebelumnya.



Deadlock adalah suatu kondisi dimana terdapat dua proses atau bahkan lebih dalam antrian proses yang lain untuk melepaskan resource yang sedang dipakai. dan berikut adalah gambarannya

 Starvation adalah kondisi yang biasanya terjadi setelah deadlock. Berikut gambaran dari starvation

Uraian sub topik ke-2

3. Sub sub topik ke-n

Uraian sub topik ke-n

C. Latihan

a. Jelaskan Pengertian dari Sinkronisasi dan fungsinya ….?

b. SebutkanJenis-jenis Sinkronisasi yang anda ketahui…?

c. Apa yang dimaksud dengan Algoritma Bully….?

D. Kunci Jawaban

a. Jawaban latihan soal ke-1

Sinkronisasi adalah proses pengaturan jalannya beberapa proses pada saat yang bersamaan. Tujuan utama sinkronisasi adalah menghindari terjadinya inkonsitensi data karena pengaksesan oleh beberapa proses yang berbeda (mutual exclusion) serta untuk mengatur urutan jalannya proses-proses sehingga dapat berjalan dengan lancar dan terhindar dari deadlock dan starvation

b. Jawaban latihan soal ke-2

- **Sinkronisasi Clock**
- **Sinkronisasi Straightforward**

c. Jawaban latihan soal ke-n

Bila sebuah proses mendapatkan koordinator tidak lagi menanggapi request yang dikirim, maka proses pemilihan akan diinisiasi. Proses P mengadakan pemilihan sebagai berikut:

- P mengirim pesan ELECTION ke semua proses dengan nomor proses yang lebih besar.
- Bila tidak ada tanggapan, proses P memenangkan pemilihan ini dan menjadi koordinator.
- Namun bila salah satu proses dengan nomor yang lebih tinggi menjawab, proses tersebutlah yang akan mengambil alih proses pemilihan. Pekerjaan proses P sendiri selesai disini.

E. Daftar Pustaka

1. Couloris et. al. 2012. Distributed Systems Concepts and Design, Fifth Edition. Addison Wesley.
2. Van Steen and Tanenbaum, 2017. Distributed Systems: Prinsiples and Paradigms. 3e. Prentice-Hall

Link :

https://cds.cern.ch/record/1056310/files/0132392275_TOC.pdf

MODUL PEMROSESAN DATA TERSEBAR

(PTI-611)

MODUL SESI - 8

REFLIKASI DALAM PEMROSESAN DATA TERSEBAR

DISUSUN OLEH

HERMANSYAH S.Kom., M.Kom.

UNIVERSITAS ESA UNGGUL

2020

PENGERTIAN, KONSEP DASAR REFLEKSI.

A. Kemampuan Akhir Yang Diharapkan

Setelah mempelajari modul ini, diharapkan mahasiswa mampu :

1. Mahasiswa memahami perlunya replikasi pada sistem DDP
2. Mahasiswa dapat memahami perlunya replikasi dan bagaimana penerapan replikasi ke dalam kasus

B. Uraian dan Contoh

1. Pengertian dan Konsep Dasar Refleksi.

Uraian sub topik ke-1

REFLEKSI DALAM DDP

Pengertan Replikasi

Replikasi adalah suatu teknik untuk melakukan copy / pendistribusian data dan objek-objek dalam melaksanakan sinkronisasi antara objek sehingga konsistensi data dapat terjamin.

Konsep dasar Replikasi :

- Dengan menggunakan teknik replikasi ini, data dapat didistribusikan ke lokasi yang berbeda melalui koneksi jaringan lokal maupun internet.
- Replikasi juga memungkinkan untuk mendukung kinerja aplikasi, penyebaran data fisik sesuai dengan penggunaannya, seperti pemrosesan transaksi online dan DSS(Desiscion Support System) atau pemrosesan database terdistribusi melalui beberapa server.

- Keuntungan replikasi tergantung dari jenis replikasi tetapi pada umumnya replikasi mendukung ketersediaan data setiap waktu dan dimanapun diperlukan.
- Secara garis besar ada dua yaitu reliability dan performance.

Reliability

Satu sistem, atau bahkan lebih dari satu, dapat terjadi tabrakan tanpa akses ke data yang mengalami interrupt. Memiliki salinan data dan mengijinkan data yang corrupt agar mudah dalam proses pendeteksian dan perbaikan

Performance

Adapun keuntungan lainnya adalah

- Memungkinkan beberapa lokasi menyimpan data yang sama. Hal ini sangatberguna pada saat lokasi-lokasi tersebut membutuhkan data yangsama atau memerlukan server yang terpisah dalam pembuatan aplikasi laporan.
- Aplikasi transaksi online terpisah dari aplikasi pembacaan seperti proses analisis database secara online, data smarts atau data warehouse.
- Memungkinkan otonomi yang besar. Pengguna dapat bekerja dengan meng-copy data pada saat tidak terkoneksi kemudian melakukan perubahan untuk dibuat database baru pada saat terkoneksi
- Data dapat ditampilkan seperti layaknya melihat data tersebut dengan menggunakan aplikasi berbasis Web
- Meningkatkan kinerja pembacaan

- Membawa data mendekati lokasi individu atau kelompok pengguna. Halini akan membantu mengurangi masalah karena modifikasi data danpemrosesan query yang dilakukan oleh banyak pengguna karena

data dapat didistribusikan melalui jaringan dan data dapat dibagi berdasarkan kebutuhan masing-masing unit atau pengguna.

- Penggunaan replikasi sebagai bagian dari strategi standby server.
- Replikasi dapat digunakan apabila sebuah organisasi atau perusahaan didukung oleh hardware dan aplikasi sofware dalam sebuah sistem yang tersebar.
- Aplikasi yang berbeda mempunyai kebutuhan yang berbeda untuk otonomi dan konsistensi data. Replikasi diperlukan dalam sistem tersebar apabila berikut ini:

1. Meng-copy dan mendistribusikan data dari satu atau lebih lokasi
2. Mendistribusikan hasil copy data berdasarkan jadwal
3. Mendistribusikan perubahan data ke server lain
4. Memungkinkan beberapa pengguna di beberapa lokasi untuk melakukan perubahan dan kemudian menggabungkan data yang telah dimodifikasi.
5. Membangun aplikasi data yang menggunakan perlengkapan online maupun offline.
6. Membangun aplikasi Web sehingga pengguna dapat melihat volume data yang besar. Merencanakan Replikasi.
7. Perencanaan yang baik sebelum replikasi dapat memaksimalkan konsistensi data, meminimalkan kebutuhan jaringan dan menghindari beberapa masalah.

Beberapa hal yang menjadi pertimbangan dalam perencanaan replikasi :

1. Kebutuhan data yang akan diubah dan siapa yang mengubah
2. Pendistribusian data memerlukan konsistensi, otonomi dan kesinambungan

3. Kelengkapan replikasi yang meliputi kebutuhan user, infra struktur teknik, jaringan dan keamanan serta karakteristik data
4. Jenis replikasi dan pilihannya
5. Topologi replikasi dan bagaimana mewujudkannya agar sesuai dengan jenis replikasi

2. Jenis-Jenis Refleksi

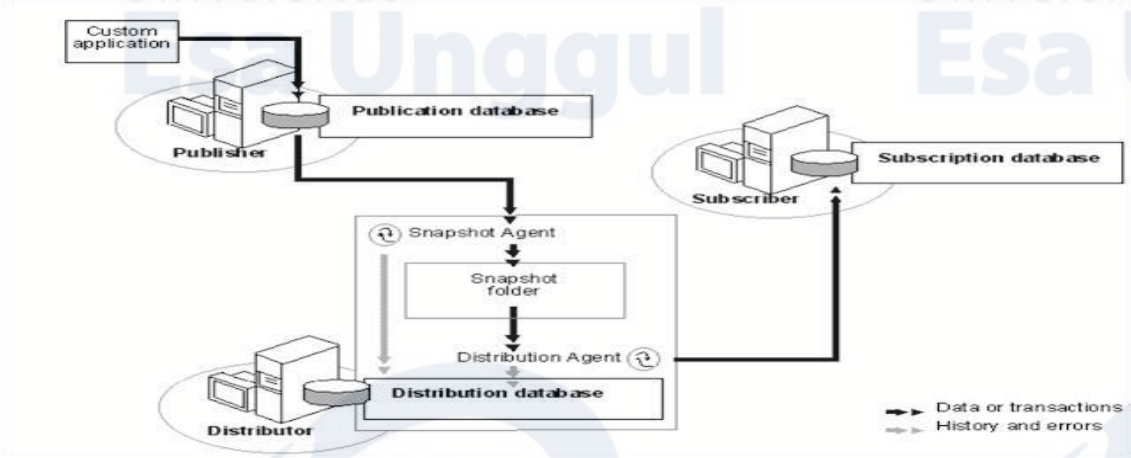
Uraian sub topik ke-2

Jenis–jenis Replikasi

- **Snapshot replication** : Mendistribusikan data yang dapat dilihat pada saat tertentu tanpa melakukan update. Biasanya digunakan pada saat memerlukan tampilan data seperti : daftar harga, katalog, data yang digunakan untuk pengambilan keputusan. Data-data ini sifatnya hanya 'Readonly'.

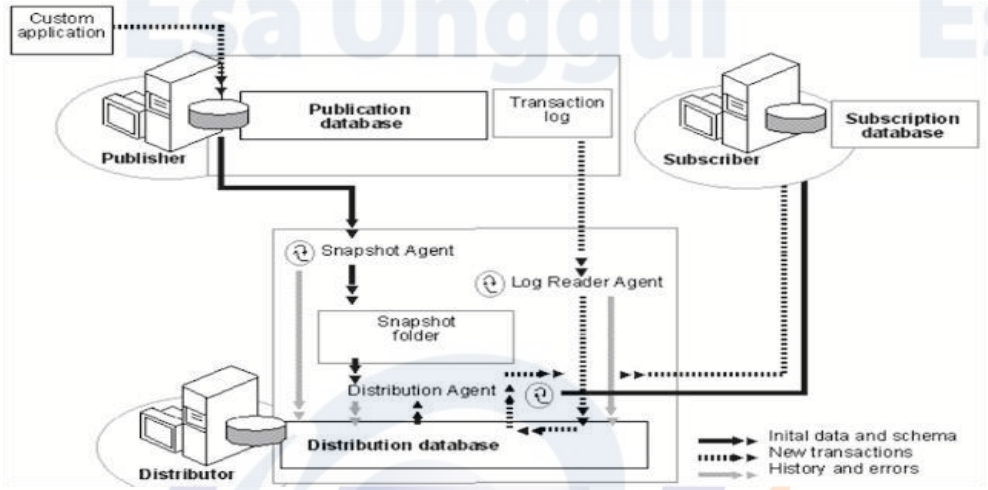
Replikasi ini membantu pada saat :

1. data sebagian besar statis dan tidak sering berubah
2. datanya sedikit
3. dapat menerima copy data yang telah melewati batas waktu yang ditentukan



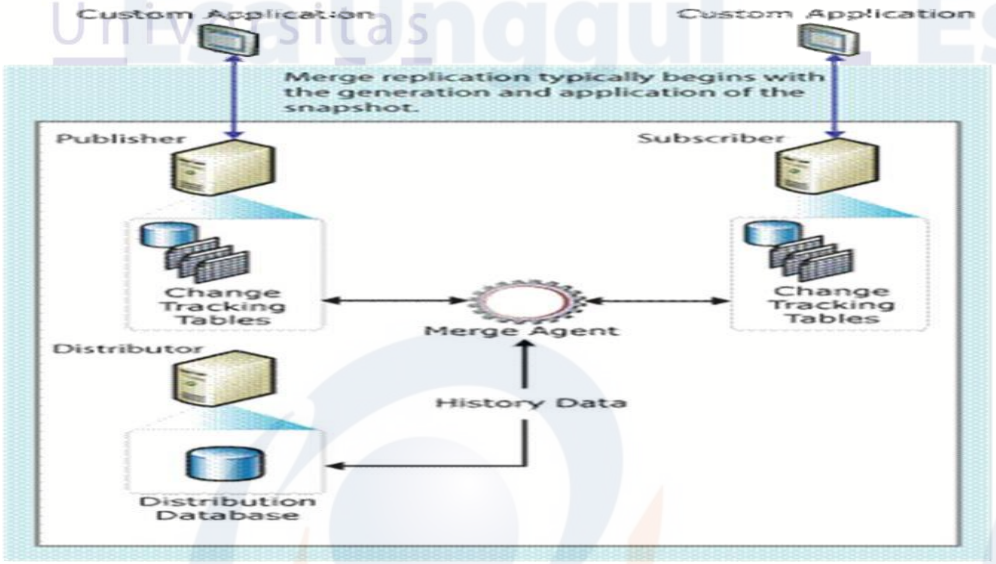
Gambar 8.1. Snapshot replication

- **Transactional replication : Memelihara kekonsistenan transaksi yang terjadi**



Gambar 8.2. Transactionl Replication

- **Merge Replication** : Merge replication memungkinkan pengguna bekerja dan merubah data sesuai dengan wewenangnya. Pada saat server tidak dikoneksikan ke seluruh lokasi dalam topologi, replikasi merubah ke nilai data yang sama.



Gambar 8.3. Merge Replication

Konsistensi dalam Sistem Terdistribusi

Konsistensi semantik merupakan kriteria penting dalam evaluasi sistem berkas yang menunjang berkas berbagi. Konsistensi semantik menunjukkan karakteristik sistem yang menspesifikasi semantik dari pengguna ganda yang mengakses berkas yang sama secara simultan. Konsistensi semantik berhubungan langsung dengan algoritma pada proses sinkronisasi.

Beberapa contoh penting konsistensi semantik sebagai berikut:

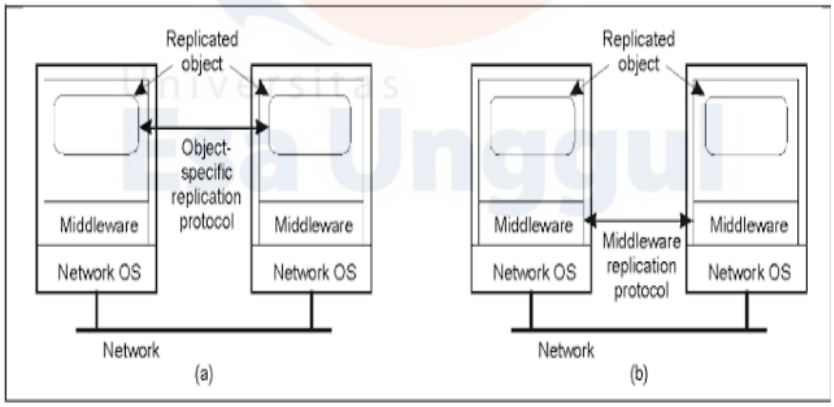
1. UNIX Semantics. Apa yang ditulis pengguna pada sebuah open berkas dapat dilihat pengguna lain yang juga sedang membuka berkas yang sama Sharing memungkinkan pengguna untuk berbagi pointer.
2. Session Semantics. Apa yang ditulis pengguna pada sebuah open berkas tidak dapat dilihat pengguna lain yang juga sedang membuka berkas yang sama. Setelah berkas itu di-close, perubahan yang terjadi karena ada pengguna yang menulis berkas dapat dilihat.
3. Immutable-Shared Files Semantics. Sebuah immutable berkas tidak dapat dimodifikasi. Walaupun beberapa pengguna mengakses immutable file, isi berkas tidak dapat diubah.

Model konsistensi pada data yang di share sulit diterapkan secara efisien, dalam beberapa kesempatan penggunaan model yang sederhana dapat juga dipakai, karena lebih mudah dalam implentasinya. Salah satunya adalah model client-centric consistency, dimana proses model ini menitikberatkan pada pendekatan single client.

Didalam sistem tersebar yang menjadi pemikiran pertama adalah bagaimana mengelola replika. Baru tahap berikutnya adalah menjaga agar server replika tetap konsisten.

Dua jenis model konsistensi adalah :

- Model konsistensi berpusat pada data (Data-Centric Concistency Models)
- Model konsistensi berpusat pada client

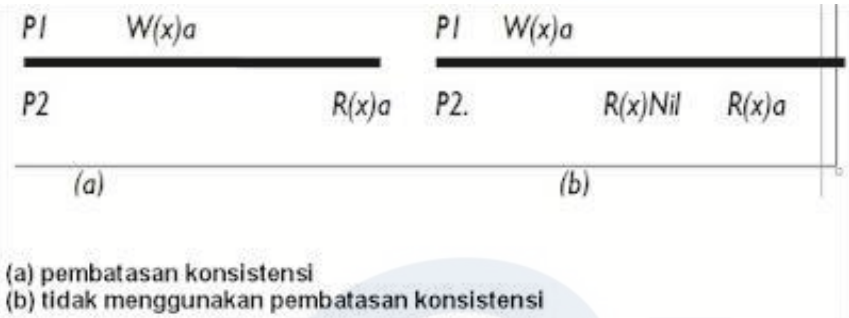


Gambar : 8.4 a) distributed System for replication -aware distributed objects
b) Distributed System responsible for replica management

Model konsistensi berpusat pada data (Data-Centric Concistency Models)

- Model Konsistensi ini menitik beratkan pada proses Read danWrite dalam kaitan dengan Read dan Write operasi pada data yang di -share.
- Hal ini disebut sebagai data store.contoh ; shared file System, memory space , database.
- Setiap proses dapat mengakses data dari media penyimpanan sesungguhnya memiliki salinan (copy) data dari media penyimpanan yang sesungguhnya secara lokal.
- Konsistensi model terjadi antara proses dan penyimpanan data, jika proses berjalan sebagaimana mestinya maka penyimpanan data berfungsi sebagaimana mestinya juga.
- Model konsistensi dapat membatasi nilai pada saat proses Read sehingga proses pengembalian data data dapat dilakukan. Beberapa diantaranya dibatasi, semakin terbatas pembatasan nilai yang ada semakin mudah diterapkan.
- Pembatasan konsistensi meliputi beberapa tahap. Apapun proses bacaan pada satu item data data x kembalikan satu nilai sesuai dengan hasil dari yang paling terbaru di tuliskan item data x.

- Pembatasan ini membutuhkan model konsistensi. Ini mengasumsikan keberadaan dari waktu global absolut, dan sangat mungkin di implementasikan
- Sebagai ilustrasi perilaku proses R(x) untuk proses Read pada data x yang memunculkan hasil k. Di mana W(x) merupakan proses Write.



(a) pembatasan konsistensi
(b) tidak menggunakan pembatasan konsistensi

Gambar 8.5. Ilustrasi perilaku proses.

Sequential Consistency and Linearizability

Sequential consistency : digunakan untuk shared memory pada sistem multiprosesor. Dalam data store dikatakan sequentialy consistent apabila memeenuhi kondisi berikut :

Hasil dari tiap eksekusi adalah sama jika operasi read dan write untuk seluruh proses di data store diekseskusi pada beberapa perintah yang terurut (sequential) dan operasi untuk setiap proses terlihat pada urutan yang diperintah secara spesifik oleh program.

Causal Consistency

Causal consistency lebih lemah dibandingkan sequential consistency. Causal consistency proses penulisan (write) harus terlihat pada perintah yang berbeda dan pada mesin yang berbeda.

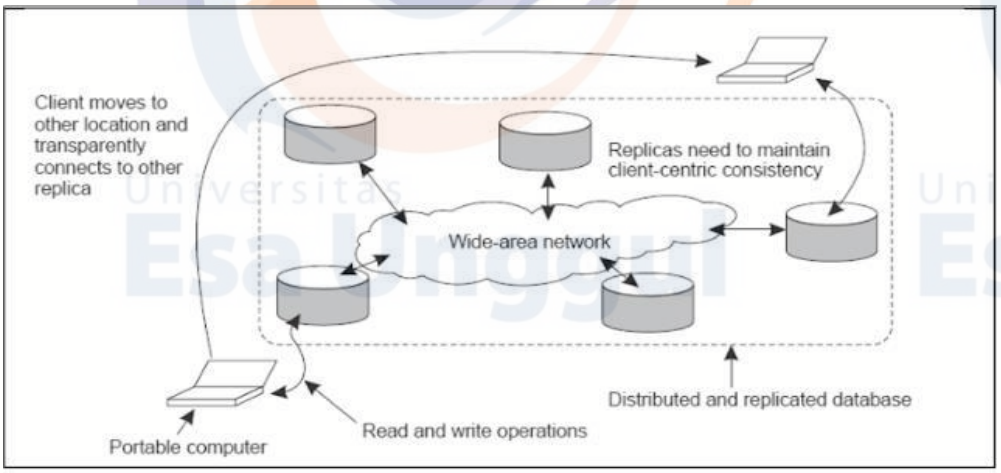
Jadi sistem menggunakan causal consistency jika Write berpotensi yang disebabkan saling terkait di lihat oleh node didalam sistem dengan perintah yang sama. Kebersamaan write akakn terlihat di dalam perintah yang berbeda pada node yang berbeda. Disinilah letak kelemahannya dibandingkan dengan sequential

consistency, yang membutuhkan node -node untuk melihat proses write pada pesanan yang sama.

Model konsistensi berpusat pada client (Client-centric consistency model). Kita berasumsi bahwa tidak ada proses update secara simultan terhdap penyimpanan data, atau ketika terjadi proses tersebut bisa dengan mudah diselesaikanbmereka terjadi mereka dapat dengan mudah dipecahkan, dan kebanyakan operasinya tersebut melibatkan pembacaan data. Kita perhatikan untuk Domain Name System atau World Wide Web.

Di dalam sistem ini, mayoritas operasi itu terbaca, dan sangat utama semua menulis dilaksanakan oleh penguasa pusat (pemilik –pemilik halaman web, hostmasters), jadi kita tidak pernah mempunyai write – write conflicts.

Jika tidak ada update berlangsung dalam jangka waktu lama, semua replika akan secara berangsur-angsur dijadikan konsisten (data lama akan di hapus dari cache). Proses ini disebut sebagai eventual consistency.



Gambar 8.6 : Hal dasar seorang pengguna mengakses replika yang berbeda dalam database terdistribusi

3. Protokol Protokol Untuk Konsistensi

Protokol-protokol untuk konsistensi

Protokol pada konsistensi digunakan untuk menguraikan lebih dalam mengenai model.

Pada Konsistensi. Ada tiga protokol yaitu :

- Primary-Based Protocols
    - Remote-Write Protocols & Local - Write Protocols
- Replicated-Write Protocols
    - Active Replication & Quorum-Based Protocols
- Cache-coherence Protocols

Replikasi adalah suatu teknik untuk melakukan copy dan pendistribusian data dan objek-objek dan melaksanakan sinkronisasi antara objek sehingga konsistensi data dapat terjamin.

Keuntungan replikasi tergantung dari jenis replikasi tetapi pada umumnya replikasi mendukung ketersediaan data setiap waktu dan dimanapun diperlu kan. Secara garis besar ada dua yaitu reliability dan performance.

Reliability maksudnya : Satu sistem, atau bahkan lebih dari satu, dapat terjadi tabrakan tanpa akses ke data yang mengalami interrupt. Memiliki salinan data dan mengijinkan data yang corrupt agar mudah dalah proses pendeteksian dan perbaikan. Performance maksudnya. beberapa salinan data dapat membantu dari sisi skala sehingga mampu menangani sistem yang lebih besar Menangani client.

Keuntungan replikasi lainnya adalah :

1. Memungkinkan beberapa lokasi menyimpan data yang sama. Hal ini sangatberguna pada saat lokasi-lokasi tersebut membutuhkan data yang sama atau memerlukan server yang terpisah dalam pembuatan aplikasi laporan.
2. Aplikasi transaksi online terpisah dari aplikasi pembacaan seperti proses analisis database secara online, data smarts atau data warehouse.
3. Memungkinkan otonomi yang besar. Pengguna dapat bekerja dengan meng-copy data pada saat tidak terkoneksi kemudian melakukan perubahan untuk dibuat database baru pada saat terkoneksi.

4. Data dapat ditampilkan seperti layaknya melihat data tersebut dengan menggunakan aplikasi berbasis Web.
5. Meningkatkan kinerja pembacaan.
6. Membawa data mendekati lokasi individu atau kelompok pengguna. Hal ini akan membantu mengurangi masalah karena modifikasi data dan pemrosesan query yang dilakukan oleh banyak pengguna karena data dapat didistri busikan melalui jaringan dan data dapat dibagi berdasarkan kebutuhan masing-masing unit atau pengguna.
7. Penggunaan replikasi sebagai bagian dari strategi standby server.

Replikasi dapat digunakan apabila sebuah organisasi atau perusahaan didukung oleh hardware dan aplikasi sofware dalam sebuah sistem yang tersebar. Aplikasi yang berbeda mempunyai kebutuhan yang berbeda untuk otonomi dan konsistensi data.

Replikasi diperlukan dalam sistem tersebar apabila berikut ini:

- Meng-copy dan mendistribusikan data dari satu atau lebih lokasi.
- Mendistribusikan hasil copy data berdasarkan jadwal.
- Mendistribusikan perubahan data ke server lain.
- Memungkinkan beberapa pengguna di beberapa lokasi untuk melakukan perubahan dan kemudian menggabungkan data yang telah dimodifikasi.
- Membangun aplikasi data yang menggunakan perlengkapan online maupun offline.
- Membangun aplikasi Web sehingga pengguna dapat melihat volume data yang besar.

Beberapa hal yang menjadi pertimbangan dalam perencanaan replikasi :

a. Kebutuhan data yang akan diubah dan siapa yang mengubah
b. Pendistribusian data memerlukan konsistensi, otonomi dan kesinambungan
c. Kelengkapan replikasi yang meliputi kebutuhan user, infrastruktur teknik, jaringan dan keamanan serta karakteristik data. 4. Jenis replikasi dan pilihannya

Topologi replikasi dan bagaimana mewujudkannya agar sesuai dengan jenis replikasi, Jenis-jenis replikasi :

- Snapshot replication
- Transactional replication
- Merge replication

Jenis-jenis replikasi : Konsistensi semantik merupakan kriteria penting dalam evaluasi sistem berkas yang menunjang berkas berbagi.
Beberapa contoh penting konsistensi semantik sebagai berikut:

- UNIX Semantics.
- Session Semantics.
- Immutable -Shared Files Semantics.

2 Jenis model konsistensi adalah :

- Konsistensi berpusat pada data (Data-CentricConcistency Models)
- Konsistensi berpusat pada client

Protokol pada konsistensi digunakan untuk menguraikan lebih dalam mengenai model konsistensi.
Ada tiga protokol yaitu :

- Primary-Based Protocols
  - Remote - Write Protocols & Local - Write Protocols
- Replicated - Write Protocols
  - ActiveReplication & Quorum-Based Protocols
- Cache-coherence Protocols

Uraian sub topik ke-n

C. Latihan

a. Sebutkan Pengertian dari refleksi dan keuntungannya.
b. Sebutkan beberapa protokol yang dipakai didalam refleksi…?
c. Sebutkan jenis jenis model konsistensi ...?

D. Kunci Jawaban

a. Jawaban latihan soal ke-1

- Replikasi adalah suatu teknik untuk melakukan copy / pendistribusian data dan objek-objek dalam melaksanakan sinkronisasi antara objek sehingga konsistensi data dapat terjamin.

Keuntungannya :

1. Memungkinkan beberapa lokasi menyimpan data yang sama. Hal ini sangatberguna pada saat lokasi-lokasi tersebut membutuhkan data yang sama atau memerlukan server yang terpisah dalam pembuatan aplikasi laporan.
2. Aplikasi transaksi online terpisah dari aplikasi pembacaan seperti proses analisis database secara online, data smarts atau data warehouse.
3. Memungkinkan otonomi yang besar. Pengguna dapat bekerja dengan meng-copy data pada saat tidak terkoneksi kemudian melakukan perubahan untuk dibuat database baru pada saat terkoneksi.
4. Data dapat ditampilkan seperti layaknya melihat data tersebut dengan menggunakan aplikasi berbasis Web.
5. Meningkatkan kinerja pembacaan.
6. Membawa data mendekati lokasi individu atau kelompok pengguna. Hal ini akan membantu mengurangi masalah karena modifikasi data

dan pemrosesan query yang dilakukan oleh banyak pengguna karena data dapat didistri busikan melalui jaringan dan data dapat dibagi berdasarkan kebutuhan masing-masing unit atau pengguna.

7. Penggunaan replikasi sebagai bagian dari strategi standby server.

b. Jawaban latihan soal ke-2

Ada tiga protokol yaitu :

- Primary-Based Protocols
  - Remote - Write Protocols & Local - Write Protocols
- Replicated - Write Protocols
  - ActiveReplication & Quorum-Based Protocols
- Cache-coherence Protocols

c. Jawaban latihan soal ke-n

Dua jenis model konsistensi adalah :

- Model konsistensi berpusat pada data (Data-Centric Concistency Models)
- Model konsistensi berpusat pada client

Daftar Pustaka

1. Couloris et. al. 2012. Distributed Systems Concepts and Design, Fifth Edition. Addison Wesley.
2. Van Steen and Tanenbaum, 2017. Distributed Systems: Prinsiples and Paradigms. 3e. Prentice-Hall

Link Journal :

https://komputasi.files.wordpress.com/2018/03/mvsteen-distributed-systems-3rd-preliminary-version-3-01pre-2017-170215.pdf

https://dinus.ac.id/repository/docs/ajar/Sister_7_Consistency_and_Replication.pdf

MODUL PEMROSESAN DAYA TERSEBAR

(PTI-611)

MODUL SESI 9

FOULT TOLERANCE

DISUSUN OLEH

HERMANSYAH, S.Kom., M.Kom.

UNIVERSITAS ESA UNGGUL

2020

Pengertian Foult Tolerance

A. Kemampuan Akhir Yang Diharapkan

Setelah mempelajari modul ini, diharapkan mahasiswa mampu :

1. Mahasiswa memahami konsekuensi dari DDP adalah sistem saling ketergantungan
2. Mahasiswa menyadari konsekuensi dari sistem saling ketergantungan akan berakibat kepada ketersediaan, keandalan, keamanan dan pemeliharaan sistem. Oleh karenanya perlu pengetahuan untuk antisipasi
3.

B. Uraian dan Contoh

1. Pengertian

FOULT TOLERANT

Apa yang dimaksud Fault Tolerant

Foult Tolerant adalah feature yang memungkinkan suatu sistem tetap berjalan normal miskipun ada komponen yang rusak pada salah satu komponennya. Foult tolerant juga dipakai dalam transmisi data sehingga miskipun ada beberapa data yang gagal diterima, namun pesan dapat diterima secara uth.

Dalam storage kita mengenal RAID di mana hardisk dikonfigurasi sedemikian rupa sehingga jika ada harddik yang rusak, maka data dapat foulttolerant disk yang masih berfungsi normal. Foult tolerant berhubungan dengan sistem yang mempunyai high availability yang tinggi. System yang foult tolerant mempunyai kaekteristiksebagai berikut :

1. Semua memiliki cadangan , jadi tidak ada komponen yang bergantung kepada satu alat saja.
2. Memiliki kemampuan memisahkan sistem yang gagal/rusak.
3. Bisa mencegah efek kerusakan supaya tidak menjalar ke komponen lain.

4. Kemampuan untuk berpindah ke komponen backup, dan kemudian kembali lagi ke koponen utama setelah sistem utama diperbaiki.

Transaksi Data

Transaksi pada basis data adalah satu atomic operasi berupa lojik pekerjaan maupun lojik recovery yang bisa terdiri dari beberapa intruksi. Tujuan dari transaksi adalah menjaga database dari kehilangan data dan kerusakan,seperti system crash dan pengaksesan data yang sama secara bersamaan oleh dua aplikasi yang berbeda yang menimbulkan gangguan. Ada empat elemen dalam transaksi yang biasa disingkat ACID, yaitu :

1. Atomicity, semua berhasil atau semua gagal
2. Consistency, transaksi mempertahankan konsistensi database
3. Isolation, transaksi terisolasi satu dengan yang lain
4. Durability, setelah commit update harus survive di database

Dan ada dua jenis transaksi yang paling penting dalam sistem basis data adalah :

1. Commit, memberi tanda bahwa transaksi telah selesai. Update dibuat permanen (bahkan jika setelah commit terjadi kegagalan system)
2. Rollback, memberi tanda bahwa transaksi gagal. Semua update harus di-undo

Untuk lojik recovery atau system recovery database dilakukan ketika terjadi kegagalan media, kegagalan system atau kesalahan pada transaksi. Sistem recovery menggunakan fungsi rollback dan checkpoint. Checkpoint adalah interval tertentu pada perjalanan transaksi basis data yang menyimpan keadaan basis data saat itu. Checkpoint dapat dilakukan untuk merecovery database secara backward (undo) maupun forward (redo).

Sedangkan concurrency adalah sebuah mekanisme pada system basis data yang mengijinkan banyak transaksi pada saat bersamaan untuk mengakses data yang

sama tanpa adanya gangguan. Pada umumnya terdapat 3 masalah utama pada concurrency :

1. Lost update problem, ketika dua user mengupdate dua buah data yang sama
2. Uncommited dependency problem, ketika user yang satu meretrieve data dan user yang lain merollback data tersebut
3. Inconsistent analysis problem, ketika user yang satu meretrieve data dan user yang lain mengupdate data tersebut .

Untuk menangani masalah tersebut, dilakukan proses locking, jika sebuah transaksi ingin record/resource tidak berubah dalam waktu tertentu maka dia meminta lock. Ada dua jenis lock yaitu

1. Exclusive Lock (Xlock) à write lock
2. Shared Lock (Slock) à read lock

Jadi cara kerjanya :

1. Jika transaksi A memegang Xlock pada sebuah record, maka permintaan lock (X,S) pada record yang sama harus diabaikan.
2. Jika transaksi A memegang Slock pada record R maka :

Permintaan Xlock transaksi lain pada R ditolak o Permintaan Slock transaksi lain pada R diterima Tapi, ada satu masalah yang dapat terjadi ketika melakukan proses locking ini, yaitu deadlock. Yaitu, situasi dimana dua atau lebih transaksi dalam kondisi wait-state, satu sama lain menunggu lock dilepaskan sebelum dapat memulai. Cara penanganannya adalah :

1. Deteksi dan pecahkan deadlock
2. Deteksi deadlock à wait-for-graph
3. Pecahkan deadlock à salah satu dirollback paksa
4. Ostrich Algorithm à diabaikan

Replikasi

Replikasi adalah suatu teknik untuk melakukan copy dan pendistribusian data dan objek-objek database dari satu database ke database lain dan melaksanakan sinkronisasi antara database sehingga konsistensi data dapat terjamin. Dengan menggunakan teknik replikasi ini, data dapat didistribusikan ke lokasi yang berbeda melalui koneksi jaringan lokal maupun internet. Replikasi juga memungkinkan untuk mendukung kinerja aplikasi, penyebaran data fisik sesuai dengan penggunaannya, seperti pemrosesan transaksi online dan DSS (Desiscion Support System) atau pemrosessan database terdistribusi melalui beberapa server.
Keuntungan replikasi tergantung dari jenis replikasi tetapi pada umumnya replikasi mendukung ketersediaan data setiap waktu dan dimanapun diperlukan. Adapun keuntungan lainnya adalah

1. Memungkinkan beberapa lokasi menyimpan data yang sama. Hal ini sangat berguna pada saat lokasi-lokasi tersebut membutuhkan data yang sama atau memerlukan server yang terpisah dalam pembuatan aplikasi laporan.
2. Aplikasi transaksi online terpisah dari aplikasi pembacaan seperti proses analisis database secara online, data smarts atau data warehouse.
3. Memungkinkan otonomi yang besar. Pengguna dapat bekerja dengan meng-copy data pada saat tidak terkoneksi kemudian melakukan perubahan untuk dibuat database baru pada saat terkoneksi
4. Data dapat ditampilkan seperti layaknya melihat data tersebut dengan menggunakan aplikasi berbasis Web
5. Meningkatkan kinerja pembacaan
6. Membawa data mendekati lokasi individu atau kelompok pengguna. Hal ini akan membantu mengurangi masalah karena modifikasi data dan pemrosesan query yang dilakukan oleh banyak pengguna karena data dapat didistribusikan melalui jaringan dan data dapat dibagi berdasarkan kebutuhan masing-masing unit atau pengguna.
7. Penggunaan replikasi sebagai bagian dari strategi standby server.

Replikasi dapat digunakan apabila sebuah organisasi atau perusahaan didukung oleh hardware dan aplikasi sofware dalam sebuah sistem yang terdistribusi.

Aplikasi yang berbeda mempunyai kebutuhan yang berbeda untuk otonomi dan konsistensi data. Replikasi diperlukan dalam sistem terdistibusi apabila berikut ini:

1. Mengcopy dan mendistribusikan data dari satu atau lebih lokasi
2. Mendistribusikan hasil copy data berdasarkan jadwal
3. Mendistribusikan perubahan data ke server lain
4. Memungkinkan beberapa pengguna di beberapa lokasi untuk melakukan perubahan dan kemudian menggabungkan data yang telah dimodifikasi
5. Membangun aplikasi data yang menggunakan perlengkapan online maupun offline
6. Membangun aplikasi Web sehingga pengguna dapat melihat volume data yang besar.

Untuk memahami peran dari toleransi kesalahan di dalam sistem tersebar, kita kebutuhan pertama untuk melihat lebih dekat pada apa yang itu benar-benar berarti karena suatu sistem tersebar untuk toleransi terhadap kesalahan-kesalahan. Toleran kesalahan adalah betul-betul dihubungkan dengan apakah menyebut sistem yang ketergantungan.

2. Komponen Toleransi Kesalahan

Komponen Toleransi Kesalahan

Sistem dikatakan gagal (fail) apabila tidak mampu memenuhi spesifikasi tekniknya.

Sistem Komputer dapat gagal karena kesalahan beberapa komponen seperti: Processor, memory, I/O device, cable atau software

Kesalahan dapat diklasifikasikan sebagai:

- Transient
- Intermittent
- Permanent

Kesalahan

Transient terjadi sekali dan kemudian menghilang. Jika operasi diulangi, kesalahan tidak muncul.

Intermittent terjadi kemudian menghilang, lalu muncul lagi, lalu menghilang lagi, dan seterusnya. Contohnya seperti hubungan konektor yang longgar.

Permanent terjadi seterusnya sampai komponen yang fault diperbaiki. Contoh chips terbakar, software bugs, disk head crash.

Tujuan perancangan dan pembuatan toleransi kesalahan adalah menjamin bahwa System secara keseluruhan mampu terus berfungsi secara benar meskipun fault terjadi.

Jadi disini tidak mensyaratkan individual komponen yang sangat reliable (andal)

Systems Failures

Keandalan sistem (System reliability) sangat penting di dalam sebuah sistem terdistribusi karena di dalam System tersebut terkandung sejumlah besar komponen dan kemungkinan terjadinya kegagalan sangat besar.Fault atau kesalahan suatu sistem dapat dibedakan menjadi:

Fail-silent faults atau fail stop faults : sistem berhenti dan tidak memberikan respon terhadap masukan yang ada.

Bizantine Faults : sistem terus bekerja meskipun fault dan memberikan hasil yang salah.

Sistem yang mempunyai sifat dalam kondisi normal bekerja akan memberikan respon terhadapat input dalam waktu terbatas yang telah diketahui disebut sistem Synchronous. Sistem yang tak punya sifat seperti itu disebut sistem aSynchronous. Sistem aSynchronous sangat sulit dikelola dibandingkan dengan Synchronous

Penggunaan Redudancy

Pendekatan umum fault tolerance (toleransi terhadap kegagalan) adalah menggunakan redundancy. 3 jenis redundancy:

- Information redundancy

- Time redundancy
- Physical redundancy

Information redundancy

Metoda ini menambahkan extra bit untuk membuat sedemikian hingga dapat me recovery informasi yang telah rusak. Contoh Hamming code ditambahkan pada transmitted data.

Time redundancy

Sebuah operasi dilakukan dan kemudian jika diperlukan diulangi lagi. Contoh, penggunaan atomic transaction. Jika transaction dibatalkan, proses tersebut dapat diulangi lagi tanpa menimbulkan masalah. Metoda ini sangat bermanfaat jika fault - nya adalah transient atau intermittent.

Physical redundancy

Pendekatan ini menggunakan penambahan perangkat ekstra. Sebagai contoh ekstra processor dapat ditambahkan ke System sehingga jika beberapa processor rusak maka System secara keseluruhan masih dapat berfungsi dengan benar. Ada dua cara untuk mengelola ekstra processor tersebut: active replication dan primary backup.

Toleransi Kesalahan dengan menggunakan Active Replication

Pada teknik ini semua processor / device digunakan sepanjang waktu dan setiap device memiliki replikasinya masing - masing sehingga dapat menyembunyikan fault dengan penuh.

Gambar diatas menunjukkan sinyal melalui device A,B,C secara berurutan. Setiap device memiliki 3 replikasi. Dan setiap replikasi diikuti sebuah voter. Setiap voter memiliki 3 input dan satu output. Jika dua atau tiga input sama, maka output sama dengan input. Jika 3 input berbeda hasil output tak terdefinisi. Misalkan element A2 gagal. Setiap voter V1, V2 dan V3 m end apatkan 2 masukan identik yang benar dan sebauh salah, tetapi Voter tetap menghasilkan

output yang benar untuk masukan tahap berikutnya. Sehingga pada dasarnya efek A2 tidak berpengaruh secara keseluruhan System

Toleransi Kesalahan dengan menggunakan Primary Backup

Availability

Availability menjamin bahwa informasi dan layanan dapat diakses dan berfungsi dengan benar (accessible and functional) pada saat dibutuhkan.

Untuk menyediakan jaringan dengan availability yang tinggi, maka harus dijamin bahwa Security proses adalah handal (reliable) dan responsif.

Sistem dan software termasuk System Security yang modular perlu saling Interoperable.

Sistem yang mempunyai availability yang tinggi mempunyai karakteristik antara lain mempunyai MTBF (Mean Time Between Failur) yang panjang dengan dukungan redundant power suplay dan hot - swappable module.

Integrity

Integrity (keutuhan) menjamin bahwa informasi atau software adalah lengkap, akurat dan otentik. Dengan integrity orang atau proses yang tak berhak tak bisa membuat perubahan pada sistem. Untuk network entegrity kita perlu menjamin bahwa message yang diterima adalah sama dengan message yang dikirim. Isi dari messa ge harus lengkap dan tak dimodifikasi, dan link antara sumber dan tujuan node valid. Connection integrity dapat disediakan oleh cryptography dan routing control.

Confidentiality

Confidentiality (kerahasiaan) melindungi informasi sensitif dari penyingkapan /pengaksesan yang tak berhak. Cryptography dan access control digunakan untuk melindungi kerahasiaan. Usaha penerapan perlindungan kerahasiaan tergantung pada sensitivitas dari informasi dan kemungkinan sifat pengamat atau penyusup.

Access Control

Access Control adalah proses pembatasan hak untuk penggunaan sumber - sumber sistem. Ada tiga jenis control untuk pembatasan akses: Administration control berdasarkan kebijakan organisasi.

- Physical Control misalkan pembatasan akses ke node jaringan, perlindungan pengkabelan jaringan, dan sebagainya.
- Logical control berdasarkan access control list, communication control and cryptography.
- Access control berdasarkan pengujian identitas (Authentication) dan kemudian penjaminan hak akses berdasarkan identitas (Authorization).

= Akses dapat dijaminkan kepada orang, mesin, layanan atau program.

Authentication

Authentication adalah pengujian identitas yang diklaim oleh pemakai, proses atau device. Authentication menjamin hak akses berdasarkan identitas. Confidentiality dan integrity tak akan berlangsung bila identitas pemakai data tersebut tidak lolos uji. Tingkatan Authentication yang diperlukan untuk sebuah System ditentukan oleh kebutuhan keamanan (Security) yang diperlukan oleh organisasi. Sebagai contoh transaksi keuangan sangat membutuhkan Authentication .

Contoh Hardware atau software token seperti smart card bentuk Authentication adalah penggunaan IP address untuk menentukan identitas.

Faktor Authentication adalah sebagai berikut: What a person knows. Contohnya adalah passwords dan Personal Identificatio n Numbers (PIN).

Authorization

Authorization adalah hak yang dijamin oleh suatu utilitas agar mampu mengakses layanan atau informasi untuk identitas khusus atau sekelompok identitas. Untuk System yang sangat tinggi tingkat keamanannya, default otorisasinya adalah tidak dapat akses. Sedangkan untuk System publik, otorisasinya adalah sebagai tamu (guest) atau pemakai anonym. Authentication adalah kunci untuk menjamin bahwa hanya pemakai yang telah mempunyai hak (authorized user) yang dapat mengakses informasi.

Accounting

Accounting adalah rekaman dari aktivitas jaringan dan akses sumber informasi. Dari perspektif keamanan, accounting dapat digunakan untuk pendeteksian dan analisa kejadian yang terkait dengan keamanan jaringan.

C. Latihan

a. Jelaskan Pengertian dari Foult Tolerance…?

b. Jelaskan Komponen Kesalahan yang sering terjadi pada system komputer…?

C, Toleransi Kesalahan dengan menggunakan Primary Backup

D. Kunci Jawaban

a. Jawaban latihan soal ke-1

Foult Tolerant adalah feature yang memungkinkan suatu sistem tetap berjalan normal miskipun ada komponen yang rusak pada salah satu komponennya. Foult tolerant juga dipakai dalam transmisi data sehingga miskipun ada beberapa data yang gagal diterima, namun pesan dapat diterima secara uth

b. Jawaban latihan soal ke-2

Sistem Komputer dapat gagal karena kesalahan beberapa komponen seperti: Processor, memory, I/O device, cable atau software

Kesalahan dapat diklasifikasikan sebagai:

- Transient
- Intermittent
- Permanent

c. Jawaban latihan soal ke-n

Kesalahan dengan menggunakan Primary Backup

- **Availability**
- Integrity

- Confidentiality
- Authentication
- Access Control
- Dan lain lain

B. Kemampuan Akhir Yang Diharapkan

Setelah mempelajari modul ini, diharapkan mahasiswa mampu :

1. Memahami dan Mengerti Foult Tolerant Pada Jaringan
2. Memahami Jaringan TCP/IP dan penanganan kesalahannya.

C. Uraian dan Contoh

1. Keamanan Jaringan TCP/IP

Keamanan pada jaringan TCP/IP

Jaringan Internet tidak menjamin adanya privasi atau integritas data. Sehingga data perlu dienkripsi sebelum ditransmisikan dan di – dekripsi saat diterima di penerima (Cryptography)

Cryptography adalah teknik penulisan dan pembacaan kode atau sandi rahasia (cipher). Cryptography digunakan untuk pengamanan informasi agar informasi tetap privasi dan untuk meng-authenticate identitas pengirim atau penerima informasi. Cryptography dapat juga menyediakan keutuhan (integrity) informasi, sebab ia hanya mengijinkan orang atau prose s yang berhak yang bisa mengakses informasi, dan dapat mendeteksi kerusakan atau perubahan informasi asli.

Ada tiga kategori fungsi Cryptography yaitu:

- Symatric key-
- Aymatic key
- Hash function

Symmetric Cryptography

Symmetric Cryptography menggunakan kunci yang sama untuk proses enkripsi dan dekripsi informasi. Setiap pasang pemakai menggunakan bersama - sama

sebuah key untuk pertukaran pesan/ message. Dan mereka harus tetap menjaga kerahasiaan key yang digunakan. Contoh DES, 3DES, IDEA, RC4

Asymmetric Cryptography

Asymmetric Cryptography dikenal juga sebagai public key Cryptography . Algoritma ini menggunakan sepasang key yang secara matematik saling terkait, tetapi diberikan hanya satu key. Satu key digunakan untuk enkripsi dan key yang lain untuk dekripsi. Salah satu kunci tetap dijaga rahasia dan key yang lain di distri busikan secara umum. Contoh : Diffie–Hellman, DSA, ECC

Hash Function

Hash Function digunakan untuk memadatkan message yang mempunyai panjang variable ke dalam sebuah kode yang panjangnya tetap (disebut sebagai hash atau message digest) . Algoritma yang berbeda akan menghasilkan panjang hash yang berbeda pula. Contoh Hash Function : Message Digest 5 (MD5), Secure Hash Algorithm (SHA) ,Haval

Application Layer Security

Application Layer Security menyediakan keamanan end - to - end dari aplikasi pada satu host ke aplikasi pada host lainnya. Layer ini menyediakan secara lengkap persyaratan keamanan, kelengkapan, kerahasiaan. Beberapa contoh Application Layer Security seperti : Pretty Good Privacy (PGP) dan Secure Hypertext Transfer Protocol (S - H TTP).

Pretty Good Privacy (PGP) digunakan untuk privasi dan tanda tangan digital dari message email. PGP menyediakan end to-end Security dari pengirim ke penerima. Secure Hypertext Transfer Protocol (S-HTTP) S-HTTP dirancang untuk menyediakan keamanan aplikasi Web. S-HTTP merupakan protocol keamanan berdasarkan message artinya message dapat diamankan secara individual. S-HTTP menggunakan symmetric key dan menggunakan out-of-hand communication.

Transport Layer Security

Skema ini menyediakan keamanan process-to-process antara host. Hampir kebanyakan skema ini dirancang untuk TCP. Security Sockets Layer (SSL) dan Transport Layer Security (TLS). SSL sangat luas dipakai di Internet untuk transaksi berdasarkan Web seperti pengiriman data credit card SSL dapat juga digunakan untuk protocol lainnya seperti Telnet, FTP, LDAP, IMAP dan SMTP tetapi ini tak umum dipakai.

TLS adalah terbuka berdasarkan standard IETF pada SSL 3.0. TLS didefinisikan di RFC 2246, RFC 2712, RFC 2817, RFC 2818. SSL dan TLS tidak saling interoperability. SSL dan TLS menyediakan keamanan untuk TCP session tunggal. Server dan browser harus mampu mendukung salah satu SSL atau TLS untuk membuat komunikasi Web yang aman.

Secure Shell (SSH) menyediakan remote login yang aman yaitu untuk keamananTelnet session dan file transfer. Protokol SSH menyediakan channel yang aman untuk shell session interaktif dan tunnelling pada aplikasi TCP yang lain. Filtering Packet filter dapat diimplementasikan pada router dan device Layer 3 untuk mengontrol paket apakah akan diblok atau diteruskan pada setiap interface-nya.

Network Layer Security

Skema ini dapat diterapkan untuk keamanan trafik untuk semua aplikasi atau protocol transport pada Layer di atasnya. IP Security Protocol (IPSec) Protokol ini dapat menyediakan access control, Authentication, data integrity dan Confidentiality untuk setiap paket IP antara dua network node yang saling berkomunikasi. IPSec Architecture menyediakan tiga fungsi utama:

Authentication, disediakan melalui protokol Authentication Header (AH). AH didefinisikan di RFC 2402.

Authentication dan confidential (enkripsi), disediakan melalui protocol Encapsulation Security Payload (ESP). ESP didefinisikan di RFC 2406.

Pertukaran Key, disediakan secara otomatius melalui protokol internet key exchange (IKE) atau manual. IKE didefinisikan di RFC 2409.

Security Association (SA) mendefinisikan bagaimana dua atau lebih pengguna IPSec akan menggunakan layanan keamanan dari protocol keamanan (AH atau ESP) untuk berkomunikasi yang direpresentasikan pada aliran data tertentu (particular flow). SA berisi key rahasia yang digunakan untuk melindungi data dalam sebuah aliran dan waktu hidupnya (life time). SA bersifat uni-directional (satu arah) dan unik per Security protocol (AH atau ESP). SA diidentifikasi oleh tiga parameter: Security parameter index (SPI), IP destination addess dan Security protocol identifier.

Filtering (Access Control List) Paket filter dapat diimplementasikan pada router dan device Layer 3 untuk mengontrol sumber dan tujuan IP address yang diperbolehkan untuk melewati gateway. Standart access list dapat mem-filter pada sources address. Sedangkan extended access list dapat mem-filter protocol ICMP, IGMP atau IP pada network Layer

Skema ini bekerja berdasarkan point-to-point seperti melalui sebuah leased line atau frame relay permane nt virtual circuit Perangkat hardware khusus ditambahkan pada setiap ujung link untuk melakukan enkripsi dan dekripsi. Kalangan militer, pemerintah dan perbankan sangat umum menggunakan pendekatan ini. Skema ini tidak sesuai untuk jaringan yang besar. Keuntungan metoda ini yaitu penyusup tidak bisa menentukan alamat pengirim atau penerima.

Firewall

Firewall umumnya ditempatkan pada batas network untuk membangun batas pinggir keamanan (Security). Firewall digunakan untuk melindungi internal network dari akses eksternal yang tak diinginkan. Firewall juga dapat digunakan secara internal untuk mengontrol akses jaringan pada spesifik bagian atau resources. Ada tiga jenis Firewall yang tersedia saat ini, yaitu :

Packet Filter. Jenis ini melihat protokol, alamat atau informasi port dalam setiap paket dan membuat keputusan apakah paket diteruskan atau tidak berdasarkan aturan tertentu. Contoh jenis ini adalah Access Control List (ACL) pada router.

Proxy Servers. Jenis ini menggunakan aplikasi khusus untuk setiap layanan yang akan diteruskan melalui firewall . Proxy menawarkan keamanan yang terbaik, tetapi pemakai harus mempunyai sebuah aplikasi untuk setiap layanan/service yang akan diproses oleh firewall. Jenis ini memiliki performansi terlambat dibandingkan jenis lainnya.

Stateful Inspection. Jenis ini menganalisa semua Layer komunikasi, meng-ekstrak komunikasi yang relevan dan informasi application state dan secara dinamik mempertahankan state dari komunikasi dalam sebuah table.

Access Control List

Fungsi sebuah access control list akan tergantung pada konteks dimana ia digunakan. Sebagai contoh, access list dapat :

Mengontrol akses jaringan yang dihubungkan ke sebuah router atau mendifinisikan jenis trafik tertentu yang diijinkan melewati ked dan dari jaringan.

Membatasi isi updating routing yang di" iklankan" oleh berbagai macam protocol routing.

Melindungi router itu sendiri dengan pembatasan akses kelayanan/service seperti SNMP dan Telnet.

Mendifinisikan trafik yang menarik untuk routing Dail-on-Demand.

Mendifinisikan fitur buffer dengan menentukan tingkat prioritas paket yang satu terhadap yang lain.

Network Address Translation (NAT)

NAT adalah mekanisme yang dapat digunakan untuk mentranslasikan / merubah IP address di dalam paket IP. Mekanisme tersebut dapat membuat suatu tempat (VLWH) yang menggunakan IP address khusus (privat) dapat berkomunikasi dengan jaringan global Internet. Jaringan yang menggunakan IP address

khusus/privat tidak akan bisa berhubungan dengan jaringan global Internet bila tanpa menggunakan translasi IP address.

NAT beroperasi pada sebuah devais yang menghubungkan dua jaringan bersama-sama. Umumnya satu network menggunakan IP address berdasarkan RFC 1918 (Private address) sedangkan lainnya menggunakan IP address yang berlaku global. Mekanisme NAT sebenarnya diran cang bukan untuk maksud Security, tetapi dengan NAT akan membuat lebih sulit para hacker atau penyusup untuk mendapatkan sumber paket atau mendapatkan sources atau address destination aslinya. NAT diuraikan secara lengkap pada dokumen RFC 2663.

D. Latihan

1. Jelaskan Fungsi Keamanan Data pada system computer …?
2. Sebutkan Jenis jenis keamanan yang bisaditerapka pada jaringan TCP/IP
3. Latih, an soal ke-n

E. Kunci Jawaban

1. Jawaban latihan soal ke-1

   Jaringan Internet tidak menjamin adanya privasi atau integritas data. Sehingga data perlu dienkripsi sebelum ditransmisikan dan di – dekripsi saat diterima di penerima (Cryptography),sebut. untuk itu diperukan keamanan terhadap jaringan e
2. Jawaban latihan soal ke-2

   Ada tiga kategori fungsi Cryptography yaitu:

   - Symatric key-
   - Aymatic key
   - Hash function

F. Daftar Pustaka

1. Couloris et. al. 2012. Distributed Systems Concepts and Design, Fifth Edition. Addison Wesley.
2. Van Steen and Tanenbaum, 2017. Distributed Systems: Prinsiples and Paradigms. 3e. Prentice-Hall

Link :

https://link.springer.com/chapter/10.1007/978-3-7091-8990-0_3

https://www.journals.elsevier.com/journal-of-parallel-and-distributed-computing/

FOULT TOLERANT

Apa yang dimaksud Fault Tolerant

Foult Tolerant adalah feature yang memungkinkan suatu sistem tetap berjalan normal miskipun ada komponen yang rusak pada salah satu komponennya. Foult tolerant juga dipakai dalam transmisi data sehingga miskipun ada beberapa data yang gagal diterima, namun pesan dapat diterima secara uth.

Dalam storage kita mengenal RAID di mana hardisk dikonfigurasi sedemikian rupa sehingga jika ada harddik yang rusak, maka data dapat foulttolerant disk yang masih berfungsi normal. Foult tolerant berhubungan dengan sistem yang mempunyai high availability yang tinggi. System yang foult tolerant mempunyai kaekteristiksebagai berikut :

1. Semua memiliki cadangan , jadi tidak ada komponen yang bergantung kepada satu alat saja.
2. Memiliki kemampuan memisahkan sistem yang gagal/rusak.
3. Bisa mencegah efek kerusakan supaya tidak menjalar ke komponen lain.
4. Kemampuan untuk berpindah ke komponen backup, dan kemudian kembali lagi ke koponen utama setelah sistem utama diperbaiki.

Transaksi Data

Transaksi pada basis data adalah satu atomic operasi berupa lojik pekerjaan maupun lojik recovery yang bisa terdiri dari beberapa intruksi. Tujuan dari transaksi adalah menjaga database dari kehilangan data dan kerusakan,seperti system crash dan pengaksesan data yang sama secara bersamaan oleh dua aplikasi yang berbeda yang menimbulkan gangguan. Ada empat elemen dalam transaksi yang biasa disingkat ACID, yaitu :

5. Atomicity, semua berhasil atau semua gagal
6. Consistency, transaksi mempertahankan konsistensi database
7. Isolation, transaksi terisolasi satu dengan yang lain
8. Durability, setelah commit update harus survive di database

Dan ada dua jenis transaksi yang paling penting dalam sistem basis data adalah :

3. Commit, memberi tanda bahwa transaksi telah selesai. Update dibuat permanen (bahkan jika setelah commit terjadi kegagalan system)
4. Rollback, memberi tanda bahwa transaksi gagal. Semua update harus di-undo

Untuk lojik recovery atau system recovery database dilakukan ketika terjadi kegagalan media, kegagalan system atau kesalahan pada transaksi. Sistem recovery menggunakan fungsi rollback dan checkpoint. Checkpoint adalah interval tertentu pada perjalanan transaksi basis data yang menyimpan keadaan basis data saat itu. Checkpoint dapat dilakukan untuk merecovery database secara backward (undo) maupun forward (redo).

Sedangkan concurrency adalah sebuah mekanisme pada system basis data yang mengijinkan banyak transaksi pada saat bersamaan untuk mengakses data yang sama tanpa adanya gangguan. Pada umumnya terdapat 3 masalah utama pada concurrency :

4. Lost update problem, ketika dua user mengupdate dua buah data yang sama
5. Uncommited dependency problem, ketika user yang satu meretrieve data dan user yang lain merollback data tersebut
6. Inconsistent analysis problem, ketika user yang satu meretrieve data dan user yang lain mengupdate data tersebut .

Untuk menangani masalah tersebut, dilakukan proses locking, jika sebuah transaksi ingin record/resource tidak berubah dalam waktu tertentu maka dia meminta lock. Ada dua jenis lock yaitu

1. Exclusive Lock (Xlock) à write lock
2. Shared Lock (Slock) à read lock

Jadi cara kerjanya :

2. Jika transaksi A memegang Xlock pada sebuah record, maka permintaan lock (X,S) pada record yang sama harus diabaikan.

2. Jika transaksi A memegang Slock pada record R maka :

Permintaan Xlock transaksi lain pada R ditolak o Permintaan Slock transaksi lain pada R diterima Tapi, ada satu masalah yang dapat terjadi ketika melakukan proses locking ini, yaitu deadlock. Yaitu, situasi dimana dua atau lebih transaksi dalam kondisi wait-state, satu sama lain menunggu lock dilepaskan sebelum dapat memulai. Cara penanganannya adalah :

5. Deteksi dan pecahkan deadlock
6. Deteksi deadlock à wait-for-graph
7. Pecahkan deadlock à salah satu dirollback paksa
8. Ostrich Algorithm à diabaikan

Replikasi

Replikasi adalah suatu teknik untuk melakukan copy dan pendistribusian data dan objek-objek database dari satu database ke database lain dan melaksanakan sinkronisasi antara database sehingga konsistensi data dapat terjamin. Dengan menggunakan teknik replikasi ini, data dapat didistribusikan ke lokasi yang berbeda melalui koneksi jaringan lokal maupun internet. Replikasi juga memungkinkan untuk mendukung kinerja aplikasi, penyebaran data fisik sesuai dengan penggunaannya, seperti pemrosesan transaksi online dan DSS (Desiscion Support System) atau pemrosessan database terdistribusi melalui beberapa server. Keuntungan replikasi tergantung dari jenis replikasi tetapi pada umumnya replikasi mendukung ketersediaan data setiap waktu dan dimanapun diperlukan. Adapun keuntungan lainnya adalah

8. Memungkinkan beberapa lokasi menyimpan data yang sama. Hal ini sangat berguna pada saat lokasi-lokasi tersebut membutuhkan data yang sama atau memerlukan server yang terpisah dalam pembuatan aplikasi laporan.
9. Aplikasi transaksi online terpisah dari aplikasi pembacaan seperti proses analisis database secara online, data smarts atau data warehouse.

10. Memungkinkan otonomi yang besar. Pengguna dapat bekerja dengan meng-copy data pada saat tidak terkoneksi kemudian melakukan perubahan untuk dibuat database baru pada saat terkoneksi
11. Data dapat ditampilkan seperti layaknya melihat data tersebut dengan menggunakan aplikasi berbasis Web
12. Meningkatkan kinerja pembacaan
13. Membawa data mendekati lokasi individu atau kelompok pengguna. Hal ini akan membantu mengurangi masalah karena modifikasi data dan pemrosesan query yang dilakukan oleh banyak pengguna karena data dapat didistribusikan melalui jaringan dan data dapat dibagi berdasarkan kebutuhan masing-masing unit atau pengguna.
14. Penggunaan replikasi sebagai bagian dari strategi standby server.

Replikasi dapat digunakan apabila sebuah organisasi atau perusahaan didukung oleh hardware dan aplikasi sofware dalam sebuah sistem yang terdistribusi. Aplikasi yang berbeda mempunyai kebutuhan yang berbeda untuk otonomi dan konsistensi data. Replikasi diperlukan dalam sistem terdistibusi apabila berikut ini:

1. Mengcopy dan mendistribusikan data dari satu atau lebih lokasi
2. Mendistribusikan hasil copy data berdasarkan jadwal
3. Mendistribusikan perubahan data ke server lain
4. Memungkinkan beberapa pengguna di beberapa lokasi untuk melakukan perubahan dan kemudian menggabungkan data yang telah dimodifikasi
5. Membangun aplikasi data yang menggunakan perlengkapan online maupun offline
6. Membangun aplikasi Web sehingga pengguna dapat melihat volume data yang besar.

Untuk memahami peran dari toleransi kesalahan di dalam sistem tersebar, kita kebutuhan pertama untuk melihat lebih dekat pada apa yang itu benar-benar berarti karena suatu sistem tersebar untuk toleransi terhadap kesalahan-kesalahan.

Toleran kesalahan adalah betul-betul dihubungkan dengan apakah menyebut sistem yang ketergantungan.

Komponen Toleransi Kesalahan

Sistem dikatakan gagal (fail) apabila tidak mampu memenuhi spesifikasi tekniknya.

Sistem Komputer dapat gagal karena kesalahan beberapa komponen seperti: Processor, memory, I/O device, cable atau software

Kesalahan dapat diklasifikasikan sebagai:

- Transient
- Intermittent
- Permanent

Kesalahan

Transient terjadi sekali dan kemudian menghilang. Jika operasi diulangi, kesalahan tidak muncul.

Intermittent terjadi kemudian menghilang, lalu muncul lagi, lalu menghilang lagi, dan seterusnya. Contohnya seperti hubungan konektor yang longgar.

Permanent terjadi seterusnya sampai komponen yang fault diperbaiki. Contoh chips terbakar, software bugs, disk head crash.

Tujuan perancangan dan pembuatan toleransi kesalahan adalah menjamin bahwa System secara keseluruhan mampu terus berfungsi secara benar meskipun fault terjadi.

Jadi disini tidak mensyaratkan individual komponen yang sangat reliable (andal)

Systems Failures

Keandalan sistem (System reliability) sangat penting di dalam sebuah sistem terdistribusi karena di dalam System tersebut terkandung sejumlah besar komponen dan kemungkinan terjadinya kegagalan sangat besar.Fault atau kesalahan suatu sistem dapat dibedakan menjadi:

Fail-silent faults atau fail stop faults : sistem berhenti dan tidak memberikan respon terhadap masukan yang ada.

Bizantine Faults : sistem terus bekerja meskipun fault dan memberikan hasil yang salah.

Sistem yang mempunyai sifat dalam kondisi normal bekerja akan memberikan respon terhadapat input dalam waktu terbatas yang telah diketahui disebut sistem Synchronous. Sistem yang tak punya sifat seperti itu disebut sistem aSynchronous. Sistem aSynchronous sangat sulit dikelola dibandingkan dengan Synchronous

Penggunaan Redudancy

Pendekatan umum fault tolerance (toleransi terhadap kegagalan) adalah menggunakan redundancy. 3 jenis redundancy:

- Information redundancy
- Time redundancy
- Physical redundancy

Information redundancy

Metoda ini menambahkan extra bit untuk membuat sedemikian hingga dapat me recovery informasi yang telah rusak. Contoh Hamming code ditambahkan pada transmitted data.

Time redundancy

Sebuah operasi dilakukan dan kemudian jika diperlukan diulangi lagi. Contoh, penggunaan atomic transaction. Jika transaction dibatalkan, proses tersebut dapat diulangi lagi tanpa menimbulkan masalah. Metoda ini sangat bermanfaat jika fault - nya adalah transient atau intermittent.

Physical redundancy

Pendekatan ini menggunakan penambahan perangkat ekstra. Sebagai contoh ekstra processor dapat ditambahkan ke System sehingga jika beberapa processor rusak maka System secara keseluruhan masih dapat berfungsi dengan benar. Ada

dua cara untuk mengelola ekstra processor tersebut: active replication dan primary backup.

Toleransi Kesalahan dengan menggunakan Active Replication

Pada teknik ini semua processor / device digunakan sepanjang waktu dan setiap device memiliki replikasinya masing - masing sehingga dapat menyembunyikan fault dengan penuh.

Gambar diatas menunjukkan sinyal melalui device A,B,C secara berurutan. Setiap device memiliki 3 replikasi. Dan setiap replikasi diikuti sebuah voter. Setiap voter memiliki 3 input dan satu output. Jika dua atau tiga input sama, maka output sama dengan input. Jika 3 input berbeda hasil output tak terdefinisi. Misalkan element A2 gagal. Setiap voter V1, V2 dan V3 m end apatkan 2 masukan identik yang benar dan sebauh salah, tetapi Voter tetap menghasilkan output yang benar untuk masukan tahap berikutnya. Sehingga pada dasarnya efek A2 tidak berpengaruh secara keseluruhan System

Toleransi Kesalahan dengan menggunakan Primary Backup

Availability

Availability menjamin bahwa informasi dan layanan dapat diakses dan berfungsi dengan benar (accessible and functional) pada saat dibutuhkan.

Untuk menyediakan jaringan dengan availability yang tinggi, maka harus dijamin bahwa Security proses adalah handal (reliable) dan responsif.

Sistem dan software termasuk System Security yang modular perlu saling Interoperable.

Sistem yang mempunyai availability yang tinggi mempunyai karakteristik antara lain mempunyai MTBF (Mean Time Between Failur) yang panjang dengan dukungan redundant power suplay dan hot - swappable module.

Integrity

Integrity (keutuhan) menjamin bahwa informasi atau software adalah lengkap, akurat dan otentik. Dengan integrity orang atau proses yang tak berhak tak bisa membuat perubahan pada sistem. Untuk network entegrity kita perlu menjamin

bahwa message yang diterima adalah sama dengan message yang dikirim. Isi dari messa ge harus lengkap dan tak dimodifikasi, dan link antara sumber dan tujuan node valid. Connection integrity dapat disediakan oleh cryptography dan routing control.

Confidentiality

Confidentiality (kerahasiaan) melindungi informasi sensitif dari penyingkapan /pengaksesan yang tak berhak. Cryptography dan access control digunakan untuk melindungi kerahasiaan. Usaha penerapan perlindungan kerahasiaan tergantung pada sensitivitas dari informasi dan kemungkinan sifat pengamat atau penyusup.

Access Control

Access Control adalah proses pembatasan hak untuk penggunaan sumber - sumber sistem. Ada tiga jenis control untuk pembatasan akses: Administration control berdasarkan kebijakan organisasi.

- Physical Control misalkan pembatasan akses ke node jaringan, perlindungan pengkabelan jaringan, dan sebagainya.
- Logical control berdasarkan access control list, communication control and cryptography.
- Access control berdasarkan pengujian identitas (Authentication) dan kemudian penjaminan hak akses berdasarkan identitas (Authorization).

= Akses dapat dijaminkan kepada orang, mesin, layanan atau program.

Authentication

Authentication adalah pengujian identitas yang diklaim oleh pemakai, proses atau device. Authentication menjamin hak akses berdasarkan identitas. Confidentiality dan integrity tak akan berlangsung bila identitas pemakai data tersebut tidak lolos uji. Tingkatan Authentication yang diperlukan untuk sebuah System ditentukan oleh kebutuhan keamanan (Security) yang diperlukan oleh organisasi. Sebagai contoh transaksi keuangan sangat membutuhkan Authentication .

Contoh Hardware atau software token seperti smart card bentuk Authentication adalah penggunaan IP address untuk menentukan identitas.

Faktor Authentication adalah sebagai berikut: What a person knows. Contohnya adalah passwords dan Personal Identificatio n Numbers (PIN).

Authorization

Authorization adalah hak yang dijamin oleh suatu utilitas agar mampu mengakses layanan atau informasi untuk identitas khusus atau sekelompok identitas. Untuk System yang sangat tinggi tingkat keamanannya, default otorisasinya adalah tidak dapat akses. Sedangkan untuk System publik, otorisasinya adalah sebagai tamu (guest) atau pemakai anonym. Authentication adalah kunci untuk menjamin bahwa hanya pemakai yang telah mempunyai hak (authorized user) yang dapat mengakses informasi.

Accounting

Accounting adalah rekaman dari aktivitas jaringan dan akses sumber informasi. Dari perspektif keamanan, accounting dapat digunakan untuk pendeteksian dan analisa kejadian yang terkait dengan keamanan jaringan.

Keamanan pada jaringan TCP/IP

Jaringan Internet tidak menjamin adanya privasi atau integritas data. Sehingga data perlu dienkripsi sebelum ditransmisikan dan di – dekripsi saat diterima di penerima (Cryptography)

Cryptography adalah teknik penulisan dan pembacaan kode atau sandi rahasia (cipher). Cryptography digunakan untuk pengamanan informasi agar informasi tetap privasi dan untuk meng-authenticate identitas pengirim atau penerima informasi. Cryptography dapat juga menyediakan keutuhan (integrity) informasi, sebab ia hanya mengijinkan orang atau prose s yang berhak yang bisa mengakses informasi, dan dapat mendeteksi kerusakan atau perubahan informasi asli.

Ada tiga kategori fungsi Cryptography yaitu:

- Symatric key-

- Aymatic key
- Hash function

Symmetric Cryptography

Symmetric Cryptography menggunakan kunci yang sama untuk proses enkripsi dan dekripsi informasi. Setiap pasang pemakai menggunakan bersama - sama sebuah key untuk pertukaran pesan/ message. Dan mereka harus tetap menjaga kerahasiaan key yang digunakan. Contoh DES, 3DES, IDEA, RC4

Asymmetric Cryptography

Asymmetric Cryptography dikenal juga sebagai public key Cryptography . Algoritma ini menggunakan sepasang key yang secara matematik saling terkait, tetapi diberikan hanya satu key. Satu key digunakan untuk enkripsi dan key yang lain untuk dekripsi. Salah satu kunci tetap dijaga rahasia dan key yang lain di distri busikan secara umum. Contoh : Diffie–Hellman, DSA, ECC

Hash Function

Hash Function digunakan untuk memadatkan message yang mempunyai panjang variable ke dalam sebuah kode yang panjangnya tetap (disebut sebagai hash atau message digest) . Algoritma yang berbeda akan menghasilkan panjang hash yang berbeda pula. Contoh Hash Function : Message Digest 5 (MD5), Secure Hash Algorithm (SHA) ,Haval

Application Layer Security

Application Layer Security menyediakan keamanan end - to - end dari aplikasi pada satu host ke aplikasi pada host lainnya. Layer ini menyediakan secara lengkap persyaratan keamanan, kelengkapan, kerahasiaan. Beberapa contoh Application Layer Security seperti : Pretty Good Privacy (PGP) dan Secure Hypertext Transfer Protocol (S - H TTP).

Pretty Good Privacy (PGP) digunakan untuk privasi dan tanda tangan digital dari message email. PGP menyediakan end to-end Security dari pengirim ke penerima.

Secure Hypertext Transfer Protocol (S-HTTP) S-HTTP dirancang untuk menyediakan keamanan aplikasi Web. S-HTTP merupakan protocol keamanan berdasarkan message artinya message dapat diamankan secara individual. S-HTTP menggunakan symmetric key dan menggunakan out-of-hand communication.

Transport Layer Security

Skema ini menyediakan keamanan process-to-process antara host. Hampir kebanyakan skema ini dirancang untuk TCP. Security Sockets Layer (SSL) dan Transport Layer Security (TLS). SSL sangat luas dipakai di Internet untuk transaksi berdasarkan Web seperti pengiriman data credit card SSL dapat juga digunakan untuk protocol lainnya seperti Telnet, FTP, LDAP, IMAP dan SMTP tetapi ini tak umum dipakai.

TLS adalah terbuka berdasarkan standard IETF pada SSL 3.0. TLS didefinisikan di RFC 2246, RFC 2712, RFC 2817, RFC 2818. SSL dan TLS tidak saling interoperability. SSL dan TLS menyediakan keamanan untuk TCP session tunggal. Server dan browser harus mampu mendukung salah satu SSL atau TLS untuk membuat komunikasi Web yang aman.

Secure Shell (SSH) menyediakan remote login yang aman yaitu untuk keamananTelnet session dan file transfer. Protokol SSH menyediakan channel yang aman untuk shell session interaktif dan tunnelling pada aplikasi TCP yang lain. Filtering Packet filter dapat diimplementasikan pada router dan device Layer 3 untuk mengontrol paket apakah akan diblok atau diteruskan pada setiap interface-nya.

Network Layer Security

Skema ini dapat diterapkan untuk keamanan trafik untuk semua aplikasi atau protocol transport pada Layer di atasnya. IP Security Protocol (IPSec) Protokol ini dapat menyediakan access control, Authentication, data integrity dan

Confidentiality untuk setiap paket IP antara dua network node yang saling berkomunikasi. IPSec Architecture menyediakan tiga fungsi utama:

Authentication, disediakan melalui protokol Authentication Header (AH). AH didefinisikan di RFC 2402.
Authentication dan confidential (enkripsi), disediakan melalui protocol Encapsulation Security Payload (ESP). ESP didefinisikan di RFC 2406.
Pertukaran Key, disediakan secara otomatius melalui protokol internet key exchange (IKE) atau manual. IKE didefinisikan di RFC 2409.
Security Association (SA) mendefinisikan bagaimana dua atau lebih pengguna IPSec akan menggunakan layanan keamanan dari protocol keamanan (AH atau ESP) untuk berkomunikasi yang direpresentasikan pada aliran data tertentu (particular flow). SA berisi key rahasia yang digunakan untuk melindungi data dalam sebuah aliran dan waktu hidupnya (life time). SA bersifat uni-directional (satu arah) dan unik per Security protocol (AH atau ESP). SA diidentifikasi oleh tiga parameter: Security parameter index (SPI), IP destination addess dan Security protocol identifier.

Filtering (Access Control List) Paket filter dapat diimplementasikan pada router dan device Layer 3 untuk mengontrol sumber dan tujuan IP address yang diperbolehkan untuk melewati gateway. Standart access list dapat mem-filter pada sources address. Sedangkan extended access list dapat mem-filter protocol ICMP, IGMP atau IP pada network Layer
Skema ini bekerja berdasarkan point-to-point seperti melalui sebuah leased line atau frame relay permane nt virtual circuit Perangkat hardware khusus ditambahkan pada setiap ujung link untuk melakukan enkripsi dan dekripsi. Kalangan militer, pemerintah dan perbankan sangat umum menggunakan pendekatan ini. Skema ini tidak sesuai untuk jaringan yang besar. Keuntungan metoda ini yaitu penyusup tidak bisa menentukan alamat pengirim atau penerima.

Firewall

Firewall umumnya ditempatkan pada batas network untuk membangun batas pinggir keamanan (Security). Firewall digunakan untuk melindungi internal network dari akses eksternal yang tak diinginkan. Firewall juga dapat digunakan secara internal untuk mengontrol akses jaringan pada spesifik bagian atau resources. Ada tiga jenis Firewall yang tersedia saat ini, yaitu :

Packet Filter. Jenis ini melihat protokol, alamat atau informasi port dalam setiap paket dan membuat keputusan apakah paket diteruskan atau tidak berdasarkan aturan tertentu. Contoh jenis ini adalah Access Control List (ACL) pada router.

Proxy Servers. Jenis ini menggunakan aplikasi khusus untuk setiap layanan yang akan diteruskan melalui firewall . Proxy menawarkan keamanan yang terbaik, tetapi pemakai harus mempunyai sebuah aplikasi untuk setiap layanan/service yang akan diproses oleh firewall. Jenis ini memiliki performansi terlambat dibandingkan jenis lainnya.

Stateful Inspection. Jenis ini menganalisa semua Layer komunikasi, meng-ekstrak komunikasi yang relevan dan informasi application state dan secara dinamik mempertahankan state dari komunikasi dalam sebuah table.

Access Control List

Fungsi sebuah access control list akan tergantung pada konteks dimana ia digunakan. Sebagai contoh, access list dapat :

Mengontrol akses jaringan yang dihubungkan ke sebuah router atau mendifinisikan jenis trafik tertentu yang diijinkan melewati ked dan dari jaringan.

Membatasi isi updating routing yang di" iklankan" oleh berbagai macam protocol routing.

Melindungi router itu sendiri dengan pembatasan akses kelayanan/service seperti SNMP dan Telnet.

Mendifinisikan trafik yang menarik untuk routing Dail-on-Demand.

Mendifinisikan fitur buffer dengan menentukan tingkat prioritas paket yang satu terhadap yang lain.

Network Address Translation (NAT)

NAT adalah mekanisme yang dapat digunakan untuk mentranslasikan / merubah IP address di dalam paket IP. Mekanisme tersebut dapat membuat suatu tempat (VLWH) yang menggunakan IP address khusus (privat) dapat berkomunikasi dengan jaringan global Internet. Jaringan yang menggunakan IP address khusus/privat tidak akan bisa berhubungan dengan jaringan global Internet bila tanpa menggunakan translasi IP address.

NAT beroperasi pada sebuah devais yang menghubungkan dua jaringan bersama-sama. Umumnya satu network menggunakan IP address berdasarkan RFC 1918 (Private address) sedangkan lainnya menggunakan IP address yang berlaku global. Mekanisme NAT sebenarnya diran cang bukan untuk maksud Security, tetapi dengan NAT akan membuat lebih sulit para hacker atau penyusup untuk mendapatkan sumber paket atau mendapatkan sources atau address destination aslinya. NAT diuraikan secara lengkap pada dokumen RFC 2663.

MODUL PEMROSESAN DATA TERSEBAR

(PTI-611)

MODUL SESI 10

SECURITY

DISUSUN OLEH

HERMANSYAH S.Kom., M.Kom.

UNIVERSITAS ESA UNGGUL

2020

KEAMANAN DALAM PEMROSESAN DATA TERDISTRIBUSI

A. Kemampuan Akhir Yang Diharapkan

Setelah mempelajari modul ini, diharapkan mahasiswa mampu :

1. Mahasiswa dapat memahami ancaman dan mekanisme pencegahan di sistem DDP
2. Mahasiswa memahami berbagai macam ancaman di sistem DDP dan memahami penggunaan beberapa tool keamanan untuk pencegahan
3. S

B. Uraian dan Contoh

1. Pendahuluan dan Konsep Keamanan

KEAMANAN DALAM

PEMROSESAN DATA TERSEBAR

Pendahuluan dan Konsep Keamanan

Keamanan sering dipandang hanyalah merupakan masalah teknis yang melibatkan dapat atau tidaknya tertembusnya suatu sistem. Keamanan ini sendiri memiliki suatu konsep yang lebih luas yang berkaitan dengan ketergantungan suatu institusi terhadap institusi lainnya. Di dalam aplikasi, suatu pembentukan sistem yang aman akan mencoba melndungi adanya beberapa kemungkinan serangan yang dapat dilakukan pihak lain diantaranya adalah :

1. **Intrusion** : penyerangan jenis ini seseorang penyerang akan dapat menggunakan sistem komputer yang kita miliki.
2. **Denail of services** : penyerangan ini mengakibatkan pengguna yang sah tidak dapat mengakses sistem.
3. **Joyrider** : penyerangan jenis ini disebabkan oleh orang yang merasa iseng dan ingin memperoleh kesenangan dengan cara menyerang suatu sistem.

4. **Vandal** : jenis serangan ini bertujuan untuk merusak sistem yang sering dituju untuk site-site besar.
5. **Scorekeeper**: jenis serangan ini hanyalah bertujuan untuk mendapatkan reputasi dengan cara mengacak-acak system sebanyak mungkin.
6. **Mata-mata** : jenis serangan ini bertujuan untuk memperoleh data atau informsi rahasia dari pihak pesaing. Tujuan utama adanya sistem keamanan adalah untuk membatasi akses informasi dan resources hanya untuk pemakai yang memiliki hak.

Beberapa ancaman keamanan yang dapat mengancam suatu sistem adalah :

1. Leakgace : pengambilan informasi oleh penerima yang tidak berhak.
2. Tampering : pengubahan informasi yang tidak legal.
3. Vandalism : gangguan operasi sistem tertentu, dimana pelaku tidak mengharapkan kuntungan apapun.

Adapun bentuk perancangan sistem yang aman adalah :

Rancangan harus mengikuti standard yang ada Mendemokan validasi melawan ancaman yang diketahui Melakukan audit terhadap kegagalan yang terdeteksi Adanya keseimbangan antara biaya terhadap serangan yang ada.

Layanan Keamanan menurut definisi OSI yaitu :

- Access control : perlindungan terhadap pemakaian tak legal Authentication : menyediakan jaminan identitas seseorang Confidentiality : perlindungan terhadap pengungkapan identitas tak legal Integrity : melindungi dari pengubahan data yang tak legal Non-repudiation : melindungi terhadap penolakan komunikasi yang sudah pernah dilakukan. Tiga dasar mekanisme keamanan yang dibangun :
- Enkripsi : digunakan untuk menyediakan kerahasiaan, dapat menyediakan authentication dan perlindungan integritas
- Digital signature : digunakan untuk menyediakan authentication, perlindungan integritas Algoritma checksum/hash : digunakan untuk

menyediakan perlindungan integritas dan dapat menyediakan authentication.

- Teknik keamanan adalah hal penting dalam menjaga kerahasiaan data. Proses enkripsi di dalam teknik keamanan merupakan proses pengkodean pesan untuk menyembunyikan isi file. Sedangkan algoritma enkripsi modern menggunakan kunci kriptografi dimana hasil enkripsi tidak dapat di dekripsi tanpa kunci yang sesuai.

Kriptografi adalah suatu ilmu yang mempelajari bagaimana membuat suatu pesan menjadi aman selama pengiriman dari pengirim sampai ke penerima. Pesan yang akan di enkripsi disebut plaintext sedngkan pesan yang telah di enkripsi disebut chipertext.

Serangan pada sistem terdistribusi tergantung pada pengaksesan saluran komunikasi yang ada atau membuat saluran baru yang menyamarkan sebagai koneksi legal. Penyerangan yang ada yaitu penyerangan pasif dan aktif.

Selain itu juga terdapat pula metode-metode penyerangan terhadap suatu sistem. Klasifikasi metode penyerangan tersebut adalah :

1. ***Eavesdropping*** : mendapatkan duplikasi pesan tanpa ijin
2. ***Masquerading*** : mengirim atau menerima pesan menggunakan identitas lain tanpa ijin mereka
3. ***Message tampering*** : mencegat atau menangkap pesan dan mengubah isinya sebelum dilanjutkan ke penerima sebenarnya.
4. ***Replaying*** : menyimpan pesan yang ditangkap untuk pemakaian berikutnya dan mengubah isinya sebelum dilanjutkan kepenerima sebenarnya
5. ***Denail of services*** : membanjiri saluran atau resources dengan pesan yang bertujuan untuk menggagalkan pengaksesan pemakaian lain.

Mengapa sistem informasi rentan terhadap gangguan keamanan

1. Sistem yg dirancang untuk bersifat “terbuka” (mis: Internet)

- Tidak ada batas fisik dan kontrol terpusat
- Perkembangan jaringan (internetworking) yang amat cepat

2. Sikap dan pandangan pemakai
   - Aspek keamanan belum banyak dimengerti
   - Menempatkan keamanan sistem pada prioritas rendah
3. Tidak ada solusi yang komprehensif
   - Solusi terhadap masalah keamanan sistem informasi
   - Pusat-pusat informasi tentang keamanan
     - CERT
     - Milis-milis tentang keamanan sistem
     - Institusi lainnya: SecurityFocus, Symantec

Penggunaan mekanisme deteksi global

- Pembentukan jaringan tim penanggap insiden di seluruh dunia
- Peningkatan kesadaran terhadap masalah keamanan
- Pendidikan bagi pengguna umum
- Pelatihan bagi personil teknis (administrator sistem dan jaringan, CIO, CTO)

Konsep-konsep keamanan

Keamanan sebagai bagian dari sistem QoS

- Ketersediaan, kehandalan, kepastian operasional, dan keamanan
- Keamanan: perlindungan thdp obyek-obyek dlm kaitannya dengan kerahasiaan dan integritas

Keamanan sebagai. fungsi waktu: Sec(t)

- Memungkinkan kuantifikasi tingkat-tingkat keamanan, mirip dengan konsep MTTF (mean time to failure) pada kehandalan

- Biaya pengamanan sistem
- Pengertian “aman”: penyusup hrs mengeluarkan usaha, biaya, dan waktu yg besar utk dpt menembus sistem
- Biaya pengamanan
- kombinasi banyak faktor yg saling berpengaruh
- Perlu dicari optimisasi: biaya pengamanan vs potensi kerusakan.

Kebijakan keamanan harus berfungsi dengan baik sekaligus mudah dipakai

- Dapat mencegah penyusup pada umumnya
- Mampu menarik pemakai untuk menggunakanya

Aspek-aspek dalam Masalah Keamanan

- Kerahasiaan
- Melindungi obyek informasi dari pelepasan (release) yg tidak sah
- Melindungi obyek resource dari akses yg tidak sah
- Integritas
- Menjaga obyek agar tetap dapat dipercaya (trustworthy)
- Melindungi obyek dari modifikasi yang tidak sah
- Keamanan Informasi sebagai Aset Informasi adalah salah satu aset bagi sebuah organisasi yang bagaimana aset lainnya yang memiliki nilai tertentu bagi organisasi tersebut sehingga harus dilindungi untuk menjamin kelangsungan organisasi, meminimilisasi kerusakan karena kebocoran sistem keamanan informasi, mempercepat kembalinnya investasi dan memperluas peluang usaha. Beragam bentuk informasi yang mungkin dimiliki oleh sebuah organisasi meliputi diantarannya:

- Informasi yang tersimpan dalam komputer (desktop komputer maupun mobile komputer), informasi ditransmisikan melalui network, informasi yang dicetak, kirim melalui fax, email, Compact Disk atau media penyimpanan lainnya. Informasi yang dilakukan dalam pembicaraan dikirim melalui telex, email, dan informasi yang tersimpan dalam database direpsentasikan dengan media OHP, proyektor atau media presentasi lainnya, dan metode-m,etode lain yang dapat digunakan untuk menyimpan informasi dan ide-ide baru organisasi atau perusahaan.
- Informasi yang merupakan harus dilindungi keamanannya. Keamanan secara umum diartikan sebagai “Quality or state of being secure to be free from danger”. Untuk menjadi aman adalah dengan dilindungi dari musuh dan bahaya. Keamanan bisa dicapai dengan beberapa strategi yang biasa dilakukan secara simultan atau digunakan dalam kombinasi satu dengan lainya. Strategi keamanan informasi masing-masing memilki focus dan dibagun pada masing-masing kekhususannya.

Berikut contoh dari tinjauan keamanan informasi adalah :

- Physical security yang memfokuskan pada startegi untuk mengamankan pekerja, anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.• Pesonal Security Personal Security yang overlap dengan physical security dalam melindungi orang-orang dalam organisasi.
- Operation Security Operation security yang memfokuskan strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk berkerja tanpa gangguan.• Communication Security Communication security yang bertujuan mengamankan kemampuan media komunikasi, teknologi komunikasi dan isinya serta kemampuan untuk memanfaatkan alat ini untuk mencapai tujuan organisasi

Uraian sub topik ke-1

2. Keamanan Jaringan

Network Security

- Network security yang memfokuskan pada pengamanan peralatan jaringan data organisasi, jaringan data isinya serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.
- Masing – masing kemampuan diatasber kontribusi dalam program keamanan informasi secara keseluruhan. Keamanan informasi adalah perlindungan informasi termasuk sistem dan perangkat yang digunakan menyimpan, dan mengirimkannya.Keamanan informasi melindungi informasi dari berbagai ancaman untuk menjamin kelangsungan usaha, meminimalisasi kerusakan akibat terjadinya ancaman, mempercepat kembalinya investasi dan peluang usaha.

  .

Tujuan Keamanan Informasi

Keamanan informasi ditujukan untuk mencapai tiga tujuan utama: Kerahasiaan, ketersediaan, dan integritas.

Kerahasiaan

Perusahaan berusaha untuk melindungidata dan informasinya dari pengungkapan kepada orang-orang yang tidak berwewenang. Sistem informasi eksekutif, sistem informasi sumber daya manusia, dan sistem pemrosesan transakasi seperti penggajian, piutang dagang, pembeliuan, dan utang dagang amat penting dalam hal ini.

Aspek-spek Keamanan

Privacy / Confidentiality:

Inti utama aspek pivacy atau confidentiality adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Privacy lebih ke arah data-data yang sifatnya privat, sedangkan confidentiality biasanya berhubungan dengan data yang

diberikan ke pihak lain untuk keperluan tertentu (misalnya sebagai bagian dari pedaftaran sebuah sevice) dan hanya diperbolehkan untuk keperluan tertentu tersebut.

Integrity:

Aspek ini menentukan bahwa informasi tidak boleh diubah tanpa seizin pemilik informasi. Informasi yang diterima harus sesuai dan sama persis seperti saat infomasi dikirimkan. Jika terdapat perbedaan antara infomasi atau data yang dikirimkan dengan yang diterima maka aspek integrity tidak tercapai. Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa izin merupakan masalah yang harus dihadapi.

Berhubungan dengan akses untuk mengubah data dan informasi, data dan informasi yang berbeda dalam suatu sistem komputer hanya dapat diubah oleh orang berhak. Aspek ini menekankan bahwa informasi tidak boleh diubah tapa seizin pemilik infomasi. Adanya cirus, trojan horse, atau pemakai lain yang mengubah informasi tanpa izin merupakan contoh masalah yang harus dihadapi.

Authentication:

Aspek ini berhubungan dengan metode atau cara untuk menyatakan bahwa informasi betul-betul asli, orang yang mengases atau memberikan informasi adalah betul-betul orang yang dimaksud, atau sever yang kita hubungi adalah betul-betul server yang asli. Biasanya metode yang sangat kita kenal untuk terkoneksi dengan server dan mendapatkan layanan adalah dengan metode password dimana terdapat suatu karakter yang diberikan oleh pengguna ke server dan server mengenalinya sesuai dengan policy yang ada. Saat ini dengan perkembangan TI terdapat beberapa metode authentication yang lebih canggih dan aman seperti menggunakan retina mata, pengenalan suara, dan telapak tangan pengguna.

Availability:

Aspek ini berhubungan dengan ketersediaan data dan informasi Data dan informasi yang berada dalam suatu sistem komputer tersedia dan dapat dimanfaatkan oleh orang yang berhak. Aspek availability atau keterseidaan berhubungan dengan

ketersediaan informasi ketika dibutuhkan. Coba bayangkan jika kita sebagai user yang absah ingin mengakses mail atau layanan lainnya namun pada saat kita membutuhkannya layanan tersebut tidak dapat memenuhinya karena beberapa alasan, misalnya server yang down oleh serangan DoS, terkena Hack, atau terjadi Web Deface.

Keamanan Jaringan.

Keamanan jaringan adalah aktivitas mencegah dan melindungi data dan informasi di dalam sistem jaringan. yang biasanya ada dalam sebuah korporasi, dari gangguan yang tidak sah atau bukan bagian dari pengakses info atau data yang sah. Mencakup teknologi, piranti, dan proses untuk mengamankan semua yang ada di dalam sistem jaringan.

Dalam penggunaan internet dan cloud berbasis jaringan, data yang aman dan informasi merupakan hal yang sangat utama. Cloud atau jaringan yang digunakan kencang dan mudah diakses akan tetap sia-sia jika di dalamnya tidak aman.

Alasan Pentingnya Keamanan Jaringan

Menciptakan ini melibatkan lima alasan yaitu confidentiality (kerahasiaan), integrity (integritas), availability (ketersediaan), authentication (autetintikasi data), nonrepudiation (minim penyangkalan), dan access control (kontrol akses). Confidentiality mengharuskan informasi atau data di dalam sistem hanya bisa diakses oleh beberapa pihak yang mempunyai wewenang. Integrity mengharuskan informasi hanya dapat diubah oleh pihak yang memiliki wewenang.

Selain itu, availability mengharuskan informasi hanya tersedia untuk pihak berwenang saat dibutuhkan. Authentication mengharuskan pengirim informasi dapat teridentifikasi dengan tepat dan bukan pengguna palsu. Nonrepudiation mengharuskan pengirim dan penerima informasi tidak dapat menyangkal atau menolak pengiriman atau penerimaan informasi. Access control merupakan upaya pengaturan akses dengan menggunakan kombinasi user ID dan password atau mekanisme lainnya yang rumit agar tidak mudah diretas.

Jenis Serangan terhadap Keamanan Jaringan

Sebagai sesuatu yang berhubungan dengan keamanan, terdapat beberapa jenis serangan atau gangguan yang mampu menyerang yaitu interruption (gangguan), interception (penangkapan), modification (perubahan), dan fabrication (pemalsuan). Serangan atau gangguan ini dapat membahayakan data atau informasi yang ada di dalam sistem.

Interruption

merupakan penyerangan sehingga sistem yang aman tidak tersedia lagi atau digunakan oleh pengguna asli atau yang berwenang. Interception merupakan penyadapan data dalam jaringan yang diretas oleh pihak berupa program, sistem, hingga perseorangan.

Modification :

Adalah perubahan nilai data atau informasi sehingga tidak berisi hal yang semestinya. Sedangkan fabrication adalah pengiriman pesan atau data palsu ke orang lain untuk tujuan menipu.

Elemen Penting Pada Keamanan Jaringan

Dalam praktiknya, elemen terbentuknya network security terdapat dalam dua elemen utama. Tembok pengaman dalam bentuk fisik atau maya berfungsi sebagai protector atau pelindung. Sedangkan rencana pengamanan merupakan implementasi untuk melindungi dari berbagai risiko peretasan.

Syarat Keamanan Jaringan

Untuk keamanan jaringan yang baik, terdapat tiga syarat dapat dinyatakan aman terlindungi.

- Terdapat prevention (pencegahan),
- observation (observasi), dan
- response (respon)

Ketiga syarat ini sangat diperlukan dalam sebuah agar sistem jaringan tetap aman dari gangguan.

Prevention :

Adalah upaya untuk menghentikan akses yang tidak diinginkan dalam sistem jaringan. Hal ini dapat dilakukan dengan memilih layanan konfigurasi dengan hati-hati. Observation merupakan proses perawatan yang berupa melihat isi log apakah ada aktivitas tidak normal atau tidak. Hal ini bisa dilakukan lewat sistem IDS sebagai bagian dari proses observasi. Sedangkan response adalah tindakan yang diambil ketika adanya peretasan atau penyusupan pada sistem jaringan.

Hal Dasar yang Harus Ada di Keamanan Jaringan

Keamanan jaringan haruslah terdiri dari hal-hal mendasar untuk yang aman dan baik. Kemanan jaringan haruslah memiliki protection (proteksi), detection (deteksi), dan reaction (reaksi). Protection merupakan konfigurasi sitem jaringan yang harus akurat. Detection adalah pengidentifikasian kapan perubahan konfigurasi harus dilakukan dan pemantauan lalu lintas jaringan yang menunjukkan atau tidak ada masalah. Sedangkan reaction adalah pengidentifikasian masalah dengan cepat tanggap dan mengembalikannya dalam kondisi aman seperti semula.

Dalam memperkuat keamanan jaringan, terdapat beberapa jenis teknik dan tipe yang harus Anda kenali dan ketahui. Dengan mengetahui jenis dan tipe ini, Anda bisa memilih dan mengusai yang paling tepat dan aman bagi sistem jaringan yang Anda lindungi.

Terdapat access control (kontrol akses), anti-malware, application security (keamanan aplikasi), behavioral analytics (analisis perilaku), data loss prevention (pencegahan kehilangan data), email security (keamanan email), Firewall, intrusion detection and prevention (deteksi dan pencegahan intrusi), mobile device and wireless security (perangkat seluler dan keamanan nirkabel), network segmentation (segmentasi jaringan), security information and event management (informasi keamanan dan manajemen kejadian – SIEM), VPN, dan web security (keamanan web).

Segala hal dan detail tentang metode keamanan jaringan haruslah dipelajari dengan baik karena metode ini memiliki peran penting. Salah satu profesi yang wajib mempelajari metode ini adalah administrator. Tugas dan peran administrator keamanan jaringan bisa Anda simak dalam detail berikut ini.

Tugas Penting Administrator Keamanan Jaringan dalam Keamanan Jaringan

Dalam menjaga keamanan jaringan, terdapat satu peran penting yang wajib ada dalam pengamanan sistem jaringan ini yaitu administrator keamanan jaringan. Administrator jaringan adalah individu atau kelompok yang mengelola dan menjaga seluruh elemen yang ada pada dan di dalam sistem jaringan agar lebih efektif dan efisien bekerja. Pastinya, tugas administrator jaringan juga memegang peran penting dalam kuatnya keamanan jaringan.

Network Security administrator atau administrator kemanan jaringan haruslah memiliki skill dan kemampuan umum yaitu pengetahuan dasar dan teknikal mengenai teori dan praktik komputer, pengetahuan akan berbagai perangkat keras jaringan komputer termasuk cara kerja, memasang, dan konfigurasi alat, dan memiliki pemahaman tentang routing atau konfigurasi sistem yang termasuk tentang sistem keamanan komputer beserta jaringannya. Semua skill tadi juga haruslah dikemas dengan etika profesional yang baik.

Tugas penting administrator kemanan jaringan adalah berkutat dengan network, hardware, dan application. Secara spesifik, tugas administrator keamanan jaringan adalah berurusan dengan security management yang berurusan dengan keamanan jaringan. Untuk bisa mencapai security management yang baik, seorang administrator keamanan jaringan harus menguasai firewall (sistem pengizin lalu linta jaringan), user access (informasi log in beserta password control), dan resource access (pembatasan penggunaan sistem jaringan dengan memberikan hak akses ke beberapa orang saja).

Penggunaan keamanan jaringan membutuhkan pengaturan dalam tingkat fisik maupun non fisik. Pengaturan ini melibatkan proses pengontrolan. Proses

pengontrolan keamanan jaringan yang harus dipahami oleh administrator jaringan adalah melibatkan controlling corporate strategic (pengendalian strategis perusahaan yang berupa asset), controlling complexity (pengendalian kemajemukan sistem), improving service (peningkatkan layanan penggunaan), balancing various needs (penyeimbangan berbagai kebutuhan), reducing downtime (pengurangan terjadinya penghentian), dan controlling costs (pengendalian biaya yang dikeluarkan).

Itulah semua detail mengenai keamanan jaringan yang wajib Anda ketahui. Dengan mengetahui segala detail tentang keamanan jaringan, Anda bisa melindungi sistem jaringan atau cloud yang Anda gunakan dengan lebih aman dan lebih baik. Semoga membantu!

Uraian sub topik ke-2

3. Keamanan Sistem Informasi

Keamanan dalam Sistem Informasi :

Keamanan informasi merupakan perlindungan informasi dari berbagai ancaman agar menjamin kelanjutan proses bisnis, mengurangi risiko bisnis, dan meningkatkan *return of investment* (ROI) serta peluang bisnis (Chaeikar, etc., 2012). Dalam merancang sistem keamanan sistem informasi terdapat aspek-aspek keamanan informasi yang perlu di perhatikan. Aspek-aspek tersebut antara lain:

1. *Confidentiality*

Aspek yang menjamin kerahasiaan informasi atau data dan memastikan informasi hanya dapat diakses oleh pihak yang berwenang.

2. *Integrity*

Aspek yang menjamin data tidak dapat dirubah tanpa ada ijin pihak yang berwenang, menjaga kelengkapan informasi dan menjaga dari kerusakan

atau ancaman lain yang bisa menyebabkan perubahan pada informasi atau data asli.

3. *Availability*

Aspek yang menjamin bahwa data akan tersedia pada saat dibutuhkan dan menjamin *user* dapat mengakses informasi tanpa adanya gangguan.

Menurut (Whitman & Mattord, 2011) informasi merupakan salah satu aset yang penting untuk dilindungi keamanannya. Perusahaan perlu memperhatikan keamanan aset informasinya, kebocoran informasi dan kegagalan pada sistem dapat mengakibatkan kerugian baik pada sisi finansial maupunn produktifitas perusahaan. Keamanan secara umum dapat diartikan sebagai *'quality or state of being secure-to be free from danger'*. Contoh tinjauan keamanan informasi sebagai berikut:

- *Physical Security*, strategi yang memfokuskan untuk mengamankan anggota organisasi, aset fisik, akses tanpa otorisasi dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran
- *Personal Security*, strategi yang lebih memfokuskan untuk melindungi orang-orang dalam organisasi
- *Operation Security*, strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan ancaman.
- *Communications Security*, strategi yang bertujuan untuk mengamankan media informasi dan teknologi informasi.
- *Network Security*, strategi yang memfokuskan pengamanan peralatan jaringan pada data organisasi.

Uraian sub topik ke-n

C. Latihan

a. Sebutkan pengertian dari Keamanan
b. Sebutkan jenis-jenis serangan terhadap sistem computer
c. Sebutkan beberapa teknik pencegahannya…?

D. Kunci Jawaban

a. Jawaban latihan soal ke-1

Keamanan berkaitan dengan ketergantungan suatu institusi terhadap institusi lainnya. Di dalam aplikasi, suatu pembentukan sistem yang aman akan mencoba melndungi adanya beberapa kemungkinan serangan yang dapat dilakukan pihak lain.

b. Jawaban latihan soal ke-2

Jnis serangan antara lain :

1. **Intrusion** : penyerangan jenis ini seseorang penyerang akan dapat menggunakan sistem komputer yang kita miliki.
2. **Denail of services** : penyerangan ini mengakibatkan pengguna yang sah tidak dapat mengakses sistem.
3. **Joyrider** : penyerangan jenis ini disebabkan oleh orang yang merasa iseng dan ingin memperoleh kesenangan dengan cara menyerang suatu sistem.
4. **Vandal** : jenis serangan ini bertujuan untuk merusak sistem yang sering dituju untuk site-site besar.
5. **Scorekeeper**: jenis serangan ini hanyalah bertujuan untuk mendapatkan reputasi dengan cara mengacak-acak system sebanyak mungkin.
6. **Mata-mata** : jenis serangan ini bertujuan untuk memperoleh data atau informsi rahasia dari pihak pesaing. Tujuan utama adanya sistem keamanan adalah untuk membatasi akses informasi dan resources hanya untuk pemakai yang memiliki hak.

c. Jawaban latihan soal ke-n

Layanan Keamanan :

- Access control : perlindungan terhadap pemakaian tak legal Authentication : menyediakan jaminan identitas seseorang Confidentiality : perlindungan terhadap pengungkapan identitas tak legal Integrity : melindungi dari pengubahan data yang tak legal Non-

repudiation : melindungi terhadap penolakan komunikasi yang sudah pernah dilakukan. Tiga dasar mekanisme keamanan yang dibangun :

- Enkripsi : digunakan untuk menyediakan kerahasiaan, dapat menyediakan authentication dan perlindungan integritas
- Digital signature : digunakan untuk menyediakan authentication, perlindungan integritas Algoritma checksum/hash : digunakan untuk menyediakan perlindungan integritas dan dapat menyediakan authentication.

Teknik keamanan adalah hal penting dalam menjaga kerahasiaan data. Proses enkripsi di dalam teknik keamanan merupakan proses pengkodean pesan untuk menyembunyikan isi file. Sedangkan algoritma enkripsi modern menggunakan kunci kriptografi dimana hasil enkripsi tidak dapat di dekripsi tanpa kunci yang sesuai

D. **Daftar Pustaka**

1. Couloris et. al. 2012. Distributed Systems Concepts and Design, Fifth Edition. Addison Wesley
2. Van Steen and Tanenbaum, 2017. Distributed Systems: Prinsiples and Paradigms. 3e. Prentice-Hall

Link Jurnal :

https://cds.cern.ch/record/1056310/files/0132392275_TOC.pdf

https://cds.cern.ch/record/1056310/files/0132392275_security

KEAMANAN DALAM
PEMROSESAN DATA TERSEBAR

Pendahuluan.

Keamanan sering dipandang hanyalah merupakan masalah teknis yang melibatkan dapat atau tidaknya tertembusnya suatu sistem. Keamanan ini sendiri memiliki suatu konsep yang lebih luas yang berkaitan dengan ketergantungan suatu institusi terhadap institusi lainnya. Di dalam aplikasi, suatu pembentukan sistem yang aman akan mencoba melndungi adanya beberapa kemungkinan serangan yang dapat dilakukan pihak lain diantaranya adalah :

7. **Intrusion** : penyerangan jenis ini seseorang penyerang akan dapat menggunakan sistem komputer yang kita miliki.
8. **Denail of services** : penyerangan ini mengakibatkan pengguna yang sah tidak dapat mengakses sistem.
9. **Joyrider** : penyerangan jenis ini disebabkan oleh orang yang merasa iseng dan ingin memperoleh kesenangan dengan cara menyerang suatu sistem.
10. **Vandal** : jenis serangan ini bertujuan untuk merusak sistem yang sering dituju untuk site-site besar.
11. **Scorekeeper**: jenis serangan ini hanyalah bertujuan untuk mendapatkan reputasi dengan cara mengacak-acak system sebanyak mungkin.
12. **Mata-mata** : jenis serangan ini bertujuan untuk memperoleh data atau informsi rahasia dari pihak pesaing. Tujuan utama adanya sistem keamanan adalah untuk membatasi akses informasi dan resources hanya untuk pemakai yang memiliki hak.

Beberapa ancaman keamanan yang dapat mengancam suatu sistem adalah :

1. Leakgace : pengambilan informasi oleh penerima yang tidak berhak.
2. Tampering : pengubahan informasi yang tidak legal.

3. Vandalism : gangguan operasi sistem tertentu, dimana pelaku tidak mengharapkan kuntungan apapun.

Adapun bentuk perancangan sistem yang aman adalah :

Rancangan harus mengikuti standard yang ada Mendemokan validasi melawan ancaman yang diketahui Melakukan audit terhadap kegagalan yang terdeteksi Adanya keseimbangan antara biaya terhadap serangan yang ada.

Layanan Keamanan menurut definisi OSI yaitu :

- Access control : perlindungan terhadap pemakaian tak legal Authentication : menyediakan jaminan identitas seseorang Confidentiality : perlindungan terhadap pengungkapan identitas tak legal Integrity : melindungi dari pengubahan data yang tak legal Non-repudiation : melindungi terhadap penolakan komunikasi yang sudah pernah dilakukan. Tiga dasar mekanisme keamanan yang dibangun :
- Enkripsi : digunakan untuk menyediakan kerahasiaan, dapat menyediakan authentication dan perlindungan integritas
- Digital signature : digunakan untuk menyediakan authentication, perlindungan integritas Algoritma checksum/hash : digunakan untuk menyediakan perlindungan integritas dan dapat menyediakan authentication.
- Teknik keamanan adalah hal penting dalam menjaga kerahasiaan data. Proses enkripsi di dalam teknik keamanan merupakan proses pengkodean pesan untuk menyembunyikan isi file. Sedangkan algoritma enkripsi modern menggunakan kunci kriptografi dimana hasil enkripsi tidak dapat di dekripsi tanpa kunci yang sesuai.

Kriptografi adalah suatu ilmu yang mempelajari bagaimana membuat suatu pesan menjadi aman selama pengiriman dari pengirim sampai ke penerima. Pesan yang akan di enkripsi disebut plaintext sedngkan pesan yang telah di enkripsi disebut chipertext.

Serangan pada sistem terdistribusi tergantung pada pengaksesan saluran komunikasi yang ada atau membuat saluran baru yang menyamarkan sebagai koneksi legal. Penyerangan yang ada yaitu penyerangan pasif dan aktif.

Selain itu juga terdapat pula metode-metode penyerangan terhadap suatu sistem. Klasifikasi metode penyerangan tersebut adalah :

6. ***Eavesdropping*** : mendapatkan duplikasi pesan tanpa ijin
7. ***Masquerading*** : mengirim atau menerima pesan menggunakan identitas lain tanpa ijin mereka
8. ***Message tampering*** : mencegat atau menangkap pesan dan mengubah isinya sebelum dilanjutkan ke penerima sebenarnya.
9. ***Replaying*** : menyimpan pesan yang ditangkap untuk pemakaian berikutnya dan mengubah isinya sebelum dilanjutkan kepenerima sebenarnya
10. ***Denail of services*** : membanjiri saluran atau resources dengan pesan yang bertujuan untuk menggagalkan pengaksesan pemakaian lain.

Mengapa sistem informasi rentan terhadap gangguan keamanan

1. Sistem yg dirancang untuk bersifat “terbuka” (mis: Internet)
    - Tidak ada batas fisik dan kontrol terpusat
    - Perkembangan jaringan (internetworking) yang amat cepat
2. Sikap dan pandangan pemakai
    - Aspek keamanan belum banyak dimengerti
    - Menempatkan keamanan sistem pada prioritas rendah
3. Tidak ada solusi yang komprehensif
    - Solusi terhadap masalah keamanan sistem informasi
    - Pusat-pusat informasi tentang keamanan
        - CERT
        - Milis-milis tentang keamanan sistem
        - Institusi lainnya: SecurityFocus, Symantec

Penggunaan mekanisme deteksi global

- Pembentukan jaringan tim penanggap insiden di seluruh dunia
- Peningkatan kesadaran terhadap masalah keamanan
- Pendidikan bagi pengguna umum
- Pelatihan bagi personil teknis (administrator sistem dan jaringan, CIO, CTO)

Konsep-konsep keamanan

Keamanan sebagai bagian dari sistem QoS

- Ketersediaan, kehandalan, kepastian operasional, dan keamanan
- Keamanan: perlindungan thdp obyek-obyek dlm kaitannya dengan kerahasiaan dan integritas

Keamanan sebagai. fungsi waktu: Sec(t)

- Memungkinkan kuantifikasi tingkat-tingkat keamanan, mirip dengan konsep MTTF (mean time to failure) pada kehandalan
- Biaya pengamanan sistem
- Pengertian “aman”: penyusup hrs mengeluarkan usaha, biaya, dan waktu yg besar utk dpt menembus sistem
- Biaya pengamanan
- kombinasi banyak faktor yg saling berpengaruh
- Perlu dicari optimisasi: biaya pengamanan vs potensi kerusakan.

Kebijakan keamanan harus <u>berfungsi dengan baik</u> sekaligus <u>mudah dipakai</u>

- Dapat mencegah penyusup pada umumnya
- Mampu menarik pemakai untuk menggunakanya

Aspek-aspek dalam Masalah Keamanan

- Kerahasiaan
- Melindungi obyek informasi dari pelepasan (release) yg tidak sah
- Melindungi obyek resource dari akses yg tidak sah
- Integritas
- Menjaga obyek agar tetap dapat dipercaya (trustworthy)
- Melindungi obyek dari modifikasi yang tidak sah
- Keamanan Informasi sebagai Aset Informasi adalah salah satu aset bagi sebuah organisasi yang bagaimana aset lainnya yang memiliki nilai tertentu bagi organisasi tersebut sehingga harus dilindungi untuk menjamin kelangsungan organisasi, meminimilisasi kerusakan karena kebocoran sistem keamanan informasi, mempercepat kembalinnya investasi dan memperluas peluang usaha. Beragam bentuk informasi yang mungkin dimiliki oleh sebuah organisasi meliputi diantarannya:
- Informasi yang tersimpan dalam komputer (desktop komputer maupun mobile komputer), informasi ditransmisikan melalui network, informasi yang dicetak, kirim melalui fax, email, Compact Disk atau media penyimpanan lainnya. Informasi yang dilakukan dalam pembicaraan dikirim melalui telex, email, dan informasi yang tersimpan dalam database direpsentasikan dengan media OHP, proyektor atau media presentasi lainnya, dan metode-m,etode lain yang dapat digunakan untuk menyimpan informasi dan ide-ide baru organisasi atau perusahaan.
- Informasi yang merupakan harus dilindungi keamanannya. Keamanan secara umum diartikan sebagai “Quality or state of being secure to be free from danger”. Untuk menjadi aman adalah dengan dilindungi dari musuh dan bahaya. Keamanan bisa dicapai dengan beberapa strategi yang biasa dilakukan secara simultan atau digunakan dalam kombinasi

satu dengan lainya. Strategi keamanan informasi masing-masing memilki focus dan dibagun pada masing-masing kekhususannya.

Berikut contoh dari tinjauan keamanan informasi adalah :

- Physical security yang memfokuskan pada startegi untuk mengamankan pekerja, anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.• Pesonal Security Personal Security yang overlap dengan physical security dalam melindungi orang-orang dalam organisasi.
- Operation Security Operation security yang memfokuskan strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk berkerja tanpa gangguan.• Communication Security Communication security yang bertujuan mengamankan kemampuan media komunikasi, teknologi komunikasi dan isinya serta kemampuan untuk memanfaatkan alat ini untuk mencapai tujuan organisasi

Network Security

- Network security yang memfokuskan pada pengamanan peralatan jaringan data organisasi, jaringan data isinya serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.
- Masing – masing kemampuan diatasber kontribusi dalam program keamanan informasi secara keseluruhan. Keamanan informasi adalah perlindungan informasi termasuk sistem dan perangkat yang digunakan menyimpan, dan mengirimkannya.Keamanan informasi melindungi informasi dari berbagai ancaman untuk menjamin kelangsungan usaha, meminimalisasi kerusakan akibat terjadinya ancaman, mempercepat kembalinya investasi dan peluang usaha.

.

Tujuan Keamanan Informasi

Keamanan informasi ditujukan untuk mencapai tiga tujuan utama: Kerahasiaan, ketersediaan, dan integritas.

Kerahasiaan

Perusahaan berusaha untuk melindungidata dan informasinya dari pengungkapan kepada orang-orang yang tidak berwewenang. Sistem informasi eksekutif, sistem informasi sumber daya manusia, dan sistem pemrosesan transakasi seperti penggajian, piutang dagang, pembeliuan, dan utang dagang amat penting dalam hal ini.

Aspek-spek Keamanan

Privacy / Confidentiality:

Inti utama aspek pivacy atau confidentiality adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Privacy lebih ke arah data-data yang sifatnya privat, sedangkan confidentiality biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu (misalnya sebagai bagian dari pedaftaran sebuah sevice) dan hanya diperbolehkan untuk keperluan tertentu tersebut.

Integrity:

Aspek ini menentukan bahwa informasi tidak boleh diubah tanpa seizin pemilik informasi. Informasi yang diterima harus sesuai dan sama persis seperti saat infomasi dikirimkan. Jika terdapat perbedaan antara infomasi atau data yang dikirimkan dengan yang diterima maka aspek integrity tidak tercapai. Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa izin merupakan masalah yang harus dihadapi.

Berhubungan dengan akses untuk mengubah data dan informasi, data dan informasi yang berbeda dalam suatu sistem komputer hanya dapat diubah oleh orang berhak. Aspek ini menekankan bahwa informasi tidak boleh diubah tapa seizin pemilik infomasi. Adanya cirus, trojan horse, atau pemakai lain yang mengubah informasi tanpa izin merupakan contoh masalah yang harus dihadapi.

Authentication:

Aspek ini berhubungan dengan metode atau cara untuk menyatakan bahwa informasi betul-betul asli, orang yang mengases atau memberikan informasi adalah betul-betul orang yang dimaksud, atau sever yang kita hubungi adalah betul-betul server yang asli. Biasanya metode yang sangat kita kenal untuk terkoneksi dengan server dan mendapatkan layanan adalah dengan metode password dimana terdapat suatu karakter yang diberikan oleh pengguna ke server dan server mengenalinya sesuai dengan policy yang ada. Saat ini dengan perkembangan TI terdapat beberapa metode authentication yang lebih canggih dan aman seperti menggunakan retina mata, pengenalan suara, dan telapak tangan pengguna.

Availability:

Aspek ini berhubungan dengan ketersediaan data dan informasi Data dan informasi yang berada dalam suatu sistem komputer tersedia dan dapat dimanfaatkan oleh orang yang berhak. Aspek availability atau keterseidaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Coba bayangkan jika kita sebagai user yang absah ingin mengakses mail atau layanan lainnya namun pada saat kita membutuhkannya layanan tersebut tidak dapat memenuhinya karena beberapa alasan, misalnya server yang down oleh serangan DoS, terkena Hack, atau terjadi Web Deface.

Keamanan Jaringan.

Keamanan jaringan adalah aktivitas mencegah dan melindungi data dan informasi di dalam sistem jaringan. yang biasanya ada dalam sebuah korporasi, dari gangguan yang tidak sah atau bukan bagian dari pengakses info atau data yang sah. Mencakup teknologi, piranti, dan proses untuk mengamankan semua yang ada di dalam sistem jaringan.

Dalam penggunaan internet dan cloud berbasis jaringan, data yang aman dan informasi merupakan hal yang sangat utama. Cloud atau jaringan yang digunakan kencang dan mudah diakses akan tetap sia-sia jika di dalamnya tidak aman.

Alasan Pentingnya Keamanan Jaringan

Menciptakan ini melibatkan lima alasan yaitu confidentiality (kerahasiaan), integrity (integritas), availability (ketersediaan), authentication (autetintikasi data), nonrepudiation (minim penyangkalan), dan access control (kontrol akses). Confidentiality mengharuskan informasi atau data di dalam sistem hanya bisa diakses oleh beberapa pihak yang mempunyai wewenang. Integrity mengharuskan informasi hanya dapat diubah oleh pihak yang memiliki wewenang.

Selain itu, availability mengharuskan informasi hanya tersedia untuk pihak berwenang saat dibutuhkan. Authentication mengharuskan pengirim informasi dapat teridentifikasi dengan tepat dan bukan pengguna palsu. Nonrepudiation mengharuskan pengirim dan penerima informasi tidak dapat menyangkal atau menolak pengiriman atau penerimaan informasi. Access control merupakan upaya pengaturan akses dengan menggunakan kombinasi user ID dan password atau mekanisme lainnya yang rumit agar tidak mudah diretas.

Jenis Serangan terhadap Keamanan Jaringan

Sebagai sesuatu yang berhubungan dengan keamanan, terdapat beberapa jenis serangan atau gangguan yang mampu menyerang yaitu interruption (gangguan), interception (penangkapan), modification (perubahan), dan fabrication (pemalsuan). Serangan atau gangguan ini dapat membahayakan data atau informasi yang ada di dalam sistem.

Interruption

merupakan penyerangan sehingga sistem yang aman tidak tersedia lagi atau digunakan oleh pengguna asli atau yang berwenang. Interception merupakan penyadapan data dalam jaringan yang diretas oleh pihak berupa program, sistem, hingga perseorangan.

Modification :

Adalah perubahan nilai data atau informasi sehingga tidak berisi hal yang semestinya. Sedangkan fabrication adalah pengiriman pesan atau data palsu ke orang lain untuk tujuan menipu.

Elemen Penting Pada Keamanan Jaringan

Dalam praktiknya, elemen terbentuknya network security terdapat dalam dua elemen utama. Tembok pengaman dalam bentuk fisik atau maya berfungsi sebagai protector atau pelindung. Sedangkan rencana pengamanan merupakan implementasi untuk melindungi dari berbagai risiko peretasan.

Syarat Keamanan Jaringan

Untuk keamanan jaringan yang baik, terdapat tiga syarat dapat dinyatakan aman terlindungi.

- Terdapat prevention (pencegahan),
- observation (observasi), dan
- response (respon)

Ketiga syarat ini sangat diperlukan dalam sebuah agar sistem jaringan tetap aman dari gangguan.

Prevention :

Adalah upaya untuk menghentikan akses yang tidak diinginkan dalam sistem jaringan. Hal ini dapat dilakukan dengan memilih layanan konfigurasi dengan hati-hati. Observation merupakan proses perawatan yang berupa melihat isi log apakah ada aktivitas tidak normal atau tidak. Hal ini bisa dilakukan lewat sistem IDS sebagai bagian dari proses observasi. Sedangkan response adalah tindakan yang diambil ketika adanya peretasan atau penyusupan pada sistem jaringan.

Hal Dasar yang Harus Ada di Keamanan Jaringan

Keamanan jaringan haruslah terdiri dari hal-hal mendasar untuk yang aman dan baik. Kemanan jaringan haruslah memiliki protection (proteksi), detection (deteksi), dan reaction (reaksi). Protection merupakan konfigurasi sitem jaringan yang harus akurat. Detection adalah pengidentifikasian kapan perubahan konfigurasi harus dilakukan dan pemantauan lalu lintas jaringan yang menunjukkan atau tidak ada masalah. Sedangkan reaction adalah pengidentifikasian masalah dengan cepat tanggap dan mengembalikannya dalam kondisi aman seperti semula.

Dalam memperkuat keamanan jaringan, terdapat beberapa jenis teknik dan tipe yang harus Anda kenali dan ketahui. Dengan mengetahui jenis dan tipe ini, Anda bisa memilih dan mengusai yang paling tepat dan aman bagi sistem jaringan yang Anda lindungi.

Terdapat access control (kontrol akses), anti-malware, application security (keamanan aplikasi), behavioral analytics (analisis perilaku), data loss prevention (pencegahan kehilangan data), email security (keamanan email), Firewall, intrusion detection and prevention (deteksi dan pencegahan intrusi), mobile device and wireless security (perangkat seluler dan keamanan nirkabel), network segmentation (segmentasi jaringan), security information and event management (informasi keamanan dan manajemen kejadian – SIEM), VPN, dan web security (keamanan web).

Segala hal dan detail tentang metode keamanan jaringan haruslah dipelajari dengan baik karena metode ini memiliki peran penting. Salah satu profesi yang wajib mempelajari metode ini adalah administrator. Tugas dan peran administrator keamanan jaringan bisa Anda simak dalam detail berikut ini.

Tugas Penting Administrator Keamanan Jaringan dalam Keamanan Jaringan

Dalam menjaga keamanan jaringan, terdapat satu peran penting yang wajib ada dalam pengamanan sistem jaringan ini yaitu administrator keamanan jaringan. Administrator jaringan adalah individu atau kelompok yang mengelola dan menjaga seluruh elemen yang ada pada dan di dalam sistem jaringan agar lebih efektif dan efisien bekerja. Pastinya, tugas administrator jaringan juga memegang peran penting dalam kuatnya keamanan jaringan.

Network Security administrator atau administrator kemanan jaringan haruslah memiliki skill dan kemampuan umum yaitu pengetahuan dasar dan teknikal mengenai teori dan praktik komputer, pengetahuan akan berbagai perangkat keras jaringan komputer termasuk cara kerja, memasang, dan konfigurasi alat, dan

memiliki pemahaman tentang routing atau konfigurasi sistem yang termasuk tentang sistem keamanan komputer beserta jaringannya. Semua skill tadi juga haruslah dikemas dengan etika profesional yang baik.

Tugas penting administrator kemanan jaringan adalah berkutat dengan network, hardware, dan application. Secara spesifik, tugas administrator keamanan jaringan adalah berurusan dengan security management yang berurusan dengan keamanan jaringan. Untuk bisa mencapai security management yang baik, seorang administrator keamanan jaringan harus menguasai firewall (sistem pengizin lalu linta jaringan), user access (informasi log in beserta password control), dan resource access (pembatasan penggunaan sistem jaringan dengan memberikan hak akses ke beberapa orang saja).

Penggunaan keamanan jaringan membutuhkan pengaturan dalam tingkat fisik maupun non fisik. Pengaturan ini melibatkan proses pengontrolan. Proses pengontrolan keamanan jaringan yang harus dipahami oleh administrator jaringan adalah melibatkan controlling corporate strategic (pengendalian strategis perusahaan yang berupa asset), controlling complexity (pengendalian kemajemukan sistem), improving service (peningkatkan layanan penggunaan), balancing various needs (penyeimbangan berbagai kebutuhan), reducing downtime (pengurangan terjadinya penghentian), dan controlling costs (pengendalian biaya yang dikeluarkan).

Itulah semua detail mengenai keamanan jaringan yang wajib Anda ketahui. Dengan mengetahui segala detail tentang keamanan jaringan, Anda bisa melindungi sistem jaringan atau cloud yang Anda gunakan dengan lebih aman dan lebih baik. Semoga membantu!

Keamanan dalam Sistem Informasi :

Keamanan informasi merupakan perlindungan informasi dari berbagai ancaman agar menjamin kelanjutan proses bisnis, mengurangi risiko bisnis, dan meningkatkan *return of investment* (ROI) serta peluang bisnis (Chaeikar, etc., 2012).

Dalam merancang sistem keamanan sistem informasi terdapat aspek-aspek keamanan informasi yang perlu di perhatikan. Aspek-aspek tersebut antara lain:

4. *Confidentiality*

Aspek yang menjamin kerahasiaan informasi atau data dan memastikan informasi hanya dapat diakses oleh pihak yang berwenang.

5. *Integrity*

Aspek yang menjamin data tidak dapat dirubah tanpa ada ijin pihak yang berwenang, menjaga kelengkapan informasi dan menjaga dari kerusakan atau ancaman lain yang bisa menyebabkan perubahan pada informasi atau data asli.

6. *Availability*

Aspek yang menjamin bahwa data akan tersedia pada saat dibutuhkan dan menjamin *user* dapat mengakses informasi tanpa adanya gangguan.

Menurut (Whitman & Mattord, 2011) informasi merupakan salah satu aset yang penting untuk dilindungi keamanannya. Perusahaan perlu memperhatikan keamanan aset informasinya, kebocoran informasi dan kegagalan pada sistem dapat mengakibatkan kerugian baik pada sisi finansial maupunn produktifitas perusahaan. Keamanan secara umum dapat diartikan sebagai *'quality or state of being secure-to be free from danger'*. Contoh tinjauan keamanan informasi sebagai berikut:

- *Physical Security*, strategi yang memfokuskan untuk mengamankan anggota organisasi, aset fisik, akses tanpa otorisasi dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran
- *Personal Security*, strategi yang lebih memfokuskan untuk melindungi orang-orang dalam organisasi
- *Operation Security*, strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan ancaman.
- *Communications Security*, strategi yang bertujuan untuk mengamankan media informasi dan teknologi informasi.
- *Network Security*, strategi yang memfokuskan pengamanan peralatan jaringan pada data organisasi.

MODUL PEMROSESAN DATA TERSEBAR

(PTI-611)

MODUL SESI 11

DISTRIBUTED OBJECT SYSTEM

DISUSUN OLEH

HERMANSYAH S.Kom., M.Kom.

UNIVERSITAS ESA UNGGUL

2020

CORBA - COMMON OJECT REQUEST BROKER ARCHITECTURE

A. Kemampuan Akhir Yang Diharapkan

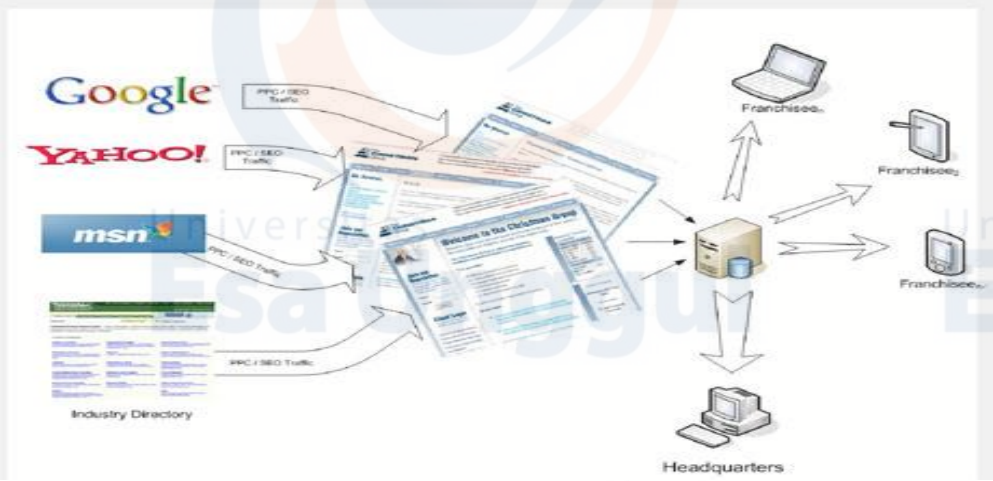
Setelah mempelajari modul ini, diharapkan mahasiswa mampu :

1. Mengerti dan memahami konsep obyek sistem terdistribusi dan mekanisme komunikasi diantara mereka
2. Mahasiswa mengerti konsep obyek terdistribusi dan mekanisme replikasi dan komunikasi diantara mereka

B. Uraian dan Contoh

1. CORBA dan Sejarah

CORBA - COMMON OJECT REQUEST BROKER ARCHITECTURE



CORBA dan Sejarahnya

Dalam dunia yang terus berkembang ini, kebutuhan komputer yang mengaplikasikan sistem terdistribusi menjadi sangat tinggi. Sistem komputer yang terdistribusi adalah sebuah sistem yang memungkinkan aplikasi komputer beroperasi secara terintegrasi pada lebih dari satu lingkungan yang terpisah secara fisik dan memiliki karakteristik concurrency, synchronization, dan failures. Adalah tidak mungkin untuk mengembangkan sistem terdistribusi yang homogen,

karena secara alamiah sistem komputer terdistribusi tumbuh dari lingkungan yang heterogen baik dalam hal perangkat keras, sistem operasi, maupun bahasa pemrogaman. Dari sini lah muncul istilah interoperabilitas yang artinya adalah kemampuan kerjasama antar sistem komputer.

Interoperabilitas sudah banyak dikenal orang. Salah satunya adalah protokol komunikasi data yang kita kenal dengan istilah TCP/IP. Namun ada satu hal yang belum banyak dikenal, yaitu interoperabilitas pada level perangkat lunak aplikasi. Dalam konteks sistem komputer terdistribusi, walaupun komponen aplikasi dibuat dengan bahasa pemrogaman yang berbeda, menggunakan development tools yang berbeda, dan beroperasi di lingkungan yang beragam pula, mereka harus tetap dapat saling bekerjasama.

Dari kebutuhan tersebut lah maka berdasarkan "kesepakatan" antara sejumlah vendor dan pengembanga perangkat lunak terkenal semacam IBM, Hewlett-Packard, dan DEC, yang tergabung dalam sebuah konsorsium bernama Object Management Group (OMG) lahirlah CORBA.

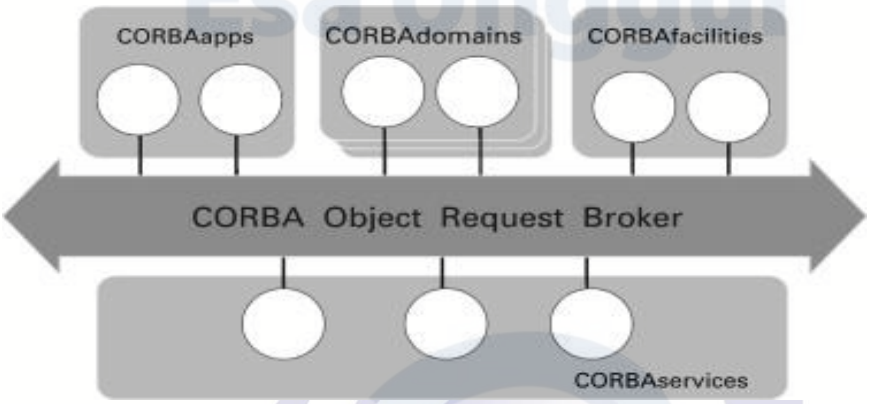
1. CORBA

CORBA adalah sebuah arsitektur software yang berbasis Object Oriented dengan paradigma client-server. Dalam terminologi tersebut, sebuah objek berkomunikasi dengan objek lain dengan cara pengiriman pesan (message passing). Diterjemahkan dalam modelclient-server, satu objek berperan sebagai si pengirim pesan (client) dan yang lain bertindak sebagai penerima dan pemroses pesan (server).

Keunikan dari CORBA adalah arsitektur ini memiliki Object Request Broker (ORB) yang memungkinkan untuk client dan server diimplementasikan dalam hardware, sistem operasi, bahasa pemrogaman, dan dilokasi yang berbeda, tapi tetap bisa saling berkomunikasi. Secara gampangnya ORB ini akan menjadi "broker/pialang" yang akan menjebatatani heterogenitas antara kedua objek. ORB akan menangani perbedaan platform, pelacakan lokasi objek, dan proses transfer pesan sedemikian rupa sehingga transparan terhadap kedua objek. Dengan

demikian pemrogaman client dan implementasi objek bisa berkonsentrasi sepenuhnya pada aspek fungsionalitas keduanya.

2. Structur CORBA ORBA



Komponen CORBA yang terletak di sisi Server

1. Server Side ORB Interface
2. Static IDL Skeleton
3. Dynamic Skeleton Interface
4. Object Adapter
5. Server Side Implementation

Komponen CORBA pada sisi Client:

1. Client Application
2. Client IDL Stubs
3. Dynamic Invocation Interface
4. Interface Repository
5. Client Side ORB Interface

3. Model Arsitekur OMG

Arsitektur CORBA (Common Object Request Broker Architecture) yang pertama kali dikembangkan oleh OMG (Object Management Group), bertujuan untuk pengembangan pemrograman berorientasi pada obyek yang terdistribusi. CORBA itu sendiri bukanlah merupakan suatu bahasa pemrograman, tetapi merupakan

suatu spesifikasi standard arsitektur untuk mengembangkan obyek-obyek terdistribusi. Beberapa software yang mengimplementasikan CORBA misalnya ORBIX (oleh Technologies), VisiBroker (oleh msprise), dan Java IDL (oleh JavaSoft). CORBA memiliki arsitektur yang berbasiskan model obyek. Model ini diturunkan strak Core Object Model yang didefiniskan OMG di dalam OMA (Object agement Architecture). Model mi merupakan gambaran abstrak yang tidak dapat diimplementasikan tanpa menggunakan teknologi tertentu. Dengan model tersebut, suatu aplikasi dapat dibangun dengan standard yang telah ditentukan.

Model Arsitektur OMG

Sistem CORBA terdiri dari obyek-obyek yang mengisolasi suatu client dari suatu server dengan menggunakan interface enkapsulasi yang didefinisikan secara ketat. Obyek CORBA dapat berjalan di atas berbagai platform, dapat terletak dimana saja dalam suatu network, dan dapat dikodekan dengan bahasa pemrograman apapun asal memiliki mapping.

Aplikasi enterprise tradisional kebanyakan adalah monolitik artinya data store, business logic, dan user interface. Perubahan yang sedikit saja mengakibatkan seluruh system perlu dikompilasi ulang. Dengan demikian reusability dari modul-modul adalah rendah sedang aplikasi terdistribusi yang dikembangkan dengan CORBA, komponen-komponennya dapat dipisahkan. Contoh dalam suatu aplikasi modular 3-tier, setiap komponen menjadi bagian yang terpisah. Semua komponen yang berupa obyek dapat dipakai oleh obyek-obyek lain dimana obyek-obyek itu tidak perlu ditulis dalam bahasa yang sama, tidak perlu berada pada platform yang sama atau pada mesin yang sama. Sekali obyek dibuat maka obyek itu dapat digunakan dari klien mana saja. User interface tier yang menampilkan informasi kepada pemakai akan menjadi tipis. Hal ini disebabkan karena obyek telah dipindahkan ke service tier yang bertindak sebagai middle war. Pada lapisan obyek logic ini terdapat CORBA object. Obyek-obyek inilah yang kemudian akan mengakses database yang berada pada data store tier..

Dengan CORBA beban dari suatu layanan bisa disebar ke beberapa server lain. CORBA dapat juga membuat bahasa pemrograman, misalnya Java, dan dapat berkomunikasi dengan obyek yang dibuat dengan bahasa yang lain dimanapun. Berkat kemampuan dinamic invocatioan interface dan dynamic skeleton interface CORBA, sebuah obyek (obyek Java) misalnya yang menjadi pelayan dapat memberi informasi mengenai jati dirinya kepada obyek lain agar obyek lain tersebut dapat meminta suatu layanan yang tersedia. Sebagai balasannya, ketidaktergantungan platform dari Java (write once – run anywhere) tentu memudahkan administrator dalam memutuskan di mesin mana obyek CORBA yang dibuat akan diletakkan asalkan ada Java Virtual Machine pasti akan jalan.

4. Object Management Architecture (OMA)

Object Management Architecture (OMA) mendefinisikan berbagai fasilitas high-level yang diperlukan untuk komputasi berorientasi obyek. Bagian utama dari OMA adalah Object Request Broker (ORB). ORB merupakan suatu mekanisme yang memberikan transparansi lokasi, komunikasi, dan aktivasi. Suatu obyek. ORB adalah semacam software bus untuk obyek-obyek dalam CORBA. Berdasarkan OMA, spesifikasi CORRBA harus dipatuhi oleh ORB.

CORBA disusun oleh komponen-komponen utama :

1. ORB (Object Request Broker)
2. IDL (Interface Definition Language)
3. DII (Dynamic Invocation Interface)
4. IR (Interface Repositories)
5. OA (Object Adapter)

5. Komponen Object Request Broker (ORB)

Inti dari CORBA adalah ORB, dimana ORB bertanggungjawab untuk menjalankan semua mekanisme yang dibutuhkan, antara lain yaitu:

1. menemukan implementasi obyek untuk memenuhi suatu request,
2. menyiapkan implementasi obyek untuk menerima suatu request,
3. melakukan komunkasi data untuk memenuhi suatu request.

Sebuah permintaan (request) yang dikirimkan suatu client ke suatu object implementation akan melewati ORB. Dengan ORB, yang terdiri dari interface, suatu entitas dapat berkomunikasi dengan object implementation tanpa adanya batasan platform, topologi jaringan, bahasa pemrograman, dan letak obyek.

Dengan menggunakan ORB, obyek client dapat meminta sebuah method pada sebuah object server yang bisa saja terdapat dalam satu mesin maupun jaringan yang berbeda. ORB menerima panggilan dan menemukan obyek yang bisa mengimplementasikan permintaan, mengirim parameter, invoke method, dan mengembalikan hasil yang diperoleh.Berikut adalah gambar yang menunjukkan komponen utama dari arsitektur CORBA ORB (Object Request Broker).

6. CORBA ORB Architecture

1. Object Implementation (OI)

Suatu Object Implementation (OI) menyediakan semantik dari obyek, yang umumnya dilakukan dengan mendefiniskan data untuk object instance dan kode untuk method-method obyek tersebut. Seringkali kita menggunakan obyek lain atau menggunakan software tambahan untuk mengimplementasikan sifat suatu obyek.

Berbagai Object Implementation (O1) dapat didukung oleh server yang terpisah, librarys, sebuah program setiap method, aplikasi ter-enkapuslasi, object-oriented database, dan lain-lain. Dengan menggunakan object adapters (OA) tambahan, dimungkinkan untuk mendukung suatu Object Implementation (OI) secara virtual.

Secara umum, Object Implementation (OI) tidak tergantung pada ORB atau bagaimana suatu client memanggil suatu obyek. Object Implementation (OI)

dapat memilih interface-nya ke ORB-dependent service yang dipilih dengan memilih Object dapter (OA).

Object Implementation (OI) menerima suatu request melalui

1. IDL Skeleton
2. Dynamic Skeleton Interface(DSl)

Object Implementation (0I) dapat memanggil Object Adapter (OA) dan ORB pada saat memproses sebuah request.

2. CORBA ORB ARCHITECTURE

6. CORBA ORB Architecture

1. Object Implementation (OI)

Suatu Object Implementation (OI) menyediakan semantik dari obyek, yang umumnya dilakukan dengan mendefiniskan data untuk object instance dan kode untuk method-method obyek tersebut. Seringkali kita menggunakan obyek lain atau menggunakan software tambahan untuk mengimplementasikan sifat suatu obyek.

Berbagai Object Implementation (O1) dapat didukung oleh server yang terpisah, librarys, sebuah program setiap method, aplikasi ter-enkapuslasi, object-oriented database, dan lain-lain. Dengan menggunakan object adapters (OA) tambahan, dimungkinkan untuk mendukung suatu Object Implementation (OI) secara virtual.

Secara umum, Object Implementation (OI) tidak tergantung pada ORB atau bagaimana suatu client memanggil suatu obyek. Object Implementation (OI) dapat memilih interface-nya ke ORB-dependent service yang dipilih dengan memilih Object dapter (OA).

Object Implementation (OI) menerima suatu request melalui

1. IDL Skeleton
2. Dynamic Skeleton Interface(DSl)

Object Implementation (0I) dapat memanggil Object Adapter (OA) dan ORB pada saat memproses sebuah request.

7. ORB Interface

ORB Interface Merupakan interface yang berhubungan langsung dengan ORB yang sama untuk semua ORB dan tidak tergantung pada interface suatu obyek atau Obyek Adapter (OA). Karena banyak fungsionalitas ORB yang disediakan melalui OA, stub, skeleton , maupun dynamic invocation; maka ada sedikit operasi yang umum bagi semua obyek.

Inteface suatu obyek dapat didefinisikan dengan cara statis, yaitu menggunakan IDL (Interface Definition Languange). IDL mendefiniskan tipe suatu obyek berdasarkan operasi-operasi (yang mungkin dijalankan pada obyek tersebut) dan parameter operasi tersebut. Interface dapat pula ditambahkan ke dalam suatu IRS (Interface Repository Service) yang menggambarkan komponen-komponen dari interface suatu obyek. Client dapat mengakses komponen-komponen ini saat runtime.

Client meminta suatu request dengan melakukan akses ke OR (Object Reference) suatu obyek yang dituju dan mengetahui tipe dari obyek dan operasi-operasi yang dapat dilakukan pada obyek tersebut. Client menginisialisasi request dengan memanggil rutin-rutin suatu stub yang sesuai dengan obyek atau membangun request secara dinamik. Interface dinamik dan interface stub harus memiliki semantic request yang masih dalam pemanggilan suatu request.

ORB mencari implementation code yang dituju, mengirimkan parameter-parameter dan mentransfer kontrol pada Object Implementation memalui IDL Sekeleton atau Dynamic Skeleton. Secara spesifik, skeleton berupa interface dan OA (Object Adapter).

Dalam mengolah suatu request, Object Implementation memberikan service pada ORB melalui OA (Object Adapter). Saat suatu request selesai dijalankan, kontrol dan nilai keluaran dikembalikan ke client. 0I dapat memilih OA yang akan digunakan. Keputusan pemilihan OA ditentukan oleh jenis service yang dibutuhkan oleh 0I tersebut. Infomasi tentang 0I diberikan pada saat instalasi dan disimpan dalam IR (Implementation Repository) yang digunakan selama pengiriman hasil request.

Dalam arsitekturnya, ORB tidak perlu dimplementasikan dalam sebuah komponen tunggal; namun, ORB didefinisikan menggunakan interface-interface yang dimilikinya. Interface-interface tersebut dikelompokan menjadi:

1. operasi yang sama untuk semua implementasi ORB,
2. operasi khusus untuk tipe obyek tertentu,
3. operasi khusus untuk style OI tertentu.

8. Object Reference (OR)

Object Reference (OR) merupakan informasi yang dibutuhkan untuk menentukan sebuah obyek dalam ORB. Client dan Object Implementation (OI) memiliki bagian yang tertutup dari OR dengan language mapping, yang kemudian disekat dari representasi aktualnya. Dua implementasi ORB dapat memiliki representasi OR yang berbeda. Representasi OR pada sisi client hanya valid selama masa hidup client tersebut.

Semua ORB harus menyediakan language mapping yang sama untuk sebuah OR (umumnya disebut obyek) untuk sebuah bahasa pemrograman tertentu. Hal ini memungkinkan sebuah program ditulis dalam bahasa apapun untuk mengakses OR secara independen terhadap ORB tertentu.

9. Komponen Interface Definition Language (IDL)

Obyek-obyek CORBA dispesifikasikan menggunakan interface, yang merupakan menghubung antara client dan server. Interface Definition Language (IDL) digunakan untuk mendefinisikan interface-interface tersebut.

IDL menentukan tipe-tipe suatu obyek dengan mendefinisikan interface-interface obyek tersebut. Sebuah interface terdiri dari kumpulan operasi dan parameter operasi. IDL hanya mendeskripsikan interface dan tidak mengimplementasikannya. Meskipun sintaks yang dimiliki oleh IDL menyerupai sintaks bahasa pemrograman C++ dan Java., perlu diingat, IDL bukan bahasa pemrograman.

Melalui IDL, Object Implementation (OI) akan memberitahu client, yang akan mengaksesnya, operasi apa saja dan method apa saja yang harus dipanggil client tersebut. Dari definisi IDL, obyek-obyek CORBA dipetakan ke bahasa pemrograman C, C++, Java, dan lain-lain yang memiliki IDL mapping. Bahasa pemrograman yang berbeda dapat mengakses obyek-obyek CORBA dalam berbagai cara yang berbeda. Pemetaan dari IDL ke bahasa pemrograman tertentu harus sama untuk semua implementasi ORB.

Language Mapping ini menyertakan definisi tipe data untuk bahasa pemrograman tertentu dan procedure interface untuk mengakses obyek melalui ORB. Ini meliputi hal-hal sebagai berikut.

1. Struktur dari client stub interface (tidak dibutuhkan untuk bahasa OOP)
2. Dynamic Invocation Interface
3. Implementation Skeleton
4. Object Adapters
5. Direct ORB Interface

Language Mapping juga mendefinisikan interaksi antara pemanggilan obyek dan langkah kontrol pada client dan implementasi. Pemetaan yang paling umum menyediakan synchronous call, dimana rutin mengembalikan nilai pada saat operasi suatu obyek selesai dilakukan. Pemetaan tambahan memungkinkan sebuah call di-inisiasi dan control dikembalikan kepada program.

1.1 Dynamic Invocation/Skeleton (DI)

IDL interface yang digunakan oleh sebuah client ditentukan pada saat client dikompilasi. Hal tesebut mengakibatkan seorang programmer hanya dapat menggunakan server-server yang terdiri dari obyek-obyek yang mengimplementasikan interface-s-interface tersebut.

Bila suatu aplikasi membutuhkan interface-interface yang tak didefiniskan saat kompilasi, maka diperlukan DII (Dynamic Invocation Interface) atau pun DSI (DynamicSkeleton Interface). DII memungkinkan suatu aplikasi/client memanggil operasi-operasi dari sembarang interface. DSI menyediakan suatu cara untuk mengirim request dari sebuah ORB ke sebuah Object Implementation (0I) tanpa harus mengetahui tipe dari obyek pada saat kompilasi.

1.2 Komponen Dynamic Invocation Interface (DII)

CORBA mendukung DII dan SII. Operasi invocation dapat dilakukan menggunakan static interface ataupun dynamic interface. Static Invocation Interface(SII) ditentukan pada saat kompilasi dan dihubungkan dengan client mengunakan stub. Sedaangkan Dynamic Invocation Interface (DII) memungkinkan apliaksi di sisi client untuk menggunakan server object tanpa perlu mengetahui tipe obek-obyek tersebut saat kompilasi. DII memungkinkan client untuk mendapatkan sebuah instance dari obyek CORBA dan membuat invocation pada obyek tersebut dengan menciptakan request yang sifatnya dinamis. DII menggunakan Interface Repository (IR) untuk memvalidasi dan mengambil identifier operasi pada suatu request yang dibuat.

1.3 Komponen Interface Repository (IR)

Client menggunakan Interface Repository (IR) untuk mempelajari tentang interface-obyek yang tidak diketahui dan client menggunakan DII untuk memanggil methods suatu obyek. Empat tahap yang diperlukan saat penggunaan Dynamic Invocation Interface (DII):

1. mengidentifikasikan target obyek yang akan dipanggil,
2. mendapatkan target interface dari obyek tersebut,
3. membangun invocation,
4. mengirim request da mendapatkan respon.

Aplikasi-aplikasi client yang menggunakan Dynamic Invocation Interface (DII) tidak lebih efisien dari yang menggunakan SII, tetapi ada dua keuntungan menggunakan DII, yaitu:

- Aplikasi client dapat melakukan permintaan kepada setiap operasi meskipun tersebut tidak diketahui pada saat aplikasi dikompilasi,
- Aplikasi client tidak harus dikompilasi ulang untuk mengakses 0I yang diaktivasi ulang.

Interface Repository (IR) merupakan online database yang berisi tentang meta informasi tentang tipe dari obyek ORB. Meta informasi yang disimpan meliputi informasi tentang modul, interface, operasi, atribut, dan eksepsi dari obyek.

Interface Repository (IR) menyediakan cara lain untuk menentukan interface ke suatu obyek. Interface ini dapat ditambahkan kelayanan IR. Dengan menggunakan IR, sebuah client akan mencari obyek yang tidak diketahui pada saat kompilasi, menemukan informasi tentang interface obyek tersebut dan implementasi suatu aktivasi dan deaktivasi.

ORB biasa menggunakan IR untuk:

1. Menyediakan interoperability antar implementasi ORB yang berbeda,
2. Menyediakan type checking dari signature sebuah request yang melalui SII dan DII.
3. Mengecek kebenaran grafik inheritance,
4. Mengelola instalasi dan distribusi interface definition dalam sebuah jaringan,
5. Mengeizinkan designer apliaksi untuk memodifikasi interface definition, dan

mengizinkan language compiler untuk mengkompile stub dan skeleton dari IR bahkan langsung dari file IDL.

Uraian sub topik ke-2

C. Latihan

a. Jelaskan apa pengertian dari CORBA…. ?
b. Jelaskan komponen komponen dari CORBA…?
c. Jelaskan hubungan antara CORBA dengan PDT…?

D. Kunci Jawaban

a. Jawaban latihan soal ke-1

CORBA adalah sebuah arsitektur software yang berbasis Object Oriented dengan paradigma client-server. Dalam terminologi tersebut, sebuah objek berkomunikasi dengan objek lain dengan cara pengiriman pesan (message passing). Diterjemahkan dalam modelclient-server, satu objek berperan sebagai si pengirim pesan (client) dan yang lain bertindak sebagai penerima dan pemroses pesan (server).

b. Jawaban latihan soal ke-2

Komponen CORBA yang terletak di sisi Server

1. Server Side ORB Interface
2. Static IDL Skeleton
3. Dynamic Skeleton Interface
4. Object Adapter
5. Server Side Implementation

Komponen CORBA pada sisi Client:

1. Client Application

2. Client IDL Stubs
3. Dynamic Invocation Interface
4. Interface Repository
5. Client Side ORB Interface

c. Jawaban latihan soal ke-n

Interoperabilitas sudah banyak dikenal orang. Salah satunya adalah protokol komunikasi data yang kita kenal dengan istilah TCP/IP. Namun ada satu hal yang belum banyak dikenal, yaitu interoperabilitas pada level perangkat lunak aplikasi. Dalam konteks sistem komputer terdistribusi, walaupun komponen aplikasi dibuat dengan bahasa pemrogaman yang berbeda, menggunakan development tools yang berbeda, dan beroperasi di lingkungan yang beragam pula, mereka harus tetap dapat saling bekerjasama.

Dari kebutuhan tersebut lah maka berdasarkan "kesepakatan" antara sejumlah vendor dan pengembanga perangkat lunak terkenal semacam IBM, Hewlett-Packard, dan DEC, yang tergabung dalam sebuah konsorsium bernama Object Management Group (OMG) lahirlah CORBA.

E. Daftar Pustaka

1. Couloris et. al. 2012. Distributed Systems Concepts and Design, Fifth Edition. Addison Wesley.
2. Van Steen and Tanenbaum, 2017. Distributed Systems: Prinsiples and Paradigms. 3e. Prentice-HallSumber

LINK JURNAL

- https://komputasi.files.wordpress.com/2018/03/mvsteen-distributed-systems-3rd-preliminary version-3-01pre-2017-170215.pdf
- https://www.amazon.com/CORBA-Reference-Guide-Understanding-Architecture/dp/0201633868/ref=sr_1_1?dchild=1&keywords=cobra+-+common+object+request+broker+architecture&qid=1599621369&s=books&sr=1-1

MODUL PEMROSESAN DATA TERSEBAR

(PT1611)

MODUL SESI 12

DISTRIBUTED FILE SYSTEM

DISUSUN OLEH

HERMANSYAH, S.Kom., M.Kom.

UNIVERSITAS ESA UNGGUL

2020

DISTRBUTED FILE SYSTEM SECARA UMUM

A. Kemampuan Akhir Yang Diharapkan

Setelah mempelajari modul ini, diharapkan mahasiswa mampu :

1. Mahasiswa memahami mekanisme pertukaran file pada sistem DDP
2. Mahasiswa memahami beberapa teknik pertukaran file pada beberapa arsitektur sistem DDP
3. Sub

B. Uraian dan Contoh

1. Sub sub topik ke-1

Distributed File System Secara Umum.

1. Pendahuluan
   - Pada bab ini akan digambarkan arsitektur dan implementasi dari dasar sistem file terdistribusi.
   - Tujuan utama dari sistem file terdistribusi yaitu mencontoh fungsi dari sistem file non-terdistribusi
   - pada program klien yang berjalan di komputer-komputer dalam suatu jaringan. Dimulai dengan pembahasan mengenai sistem storage terdistribusi dan non-terdistribusi. Sistem file awalnya dikembangkan untuk sistem komputer terpusat dan komputer desktop sebagai fasilitas sistem

Operasi yang menyediakan antarmuka pemrograman yang bagus dalam storage disk. Setelah itu,

- mereka menambahkan fasilitas seperti kontrol akses dan mekanisme file-locking yang membuatnya menjadi lebih berguna dalam pengiriman data dan program. Sistem file terdistribusi mendukung

- pengiriman informasi dalam bentuk file dan sesumber hardware dalam bentuk storage lewat
- intranet. File service yang telah dirancang dengan baik menyediakan akses ke file yang disimpan
- pada server dengan performance yang sama atau bahkan lebih baik dari file yang disimpan pada
- local disk. Desainnya disesuaikan dengan performance dari jaringan lokal dan oleh karena itulah
- menjadi yang paling efektif dalam menyediakan pengiriman storage untuk digunakan di intranet

Tabel 1. Struktur Record Atribut File

- Panjang file
- Membuat timestamp
- Membaca timestamp
- Menulis timestamp
- Atribut timestamp
- Jumlah reference
- Pemilik
- Tipe file
- Daftar kontrol akses

1.1 Karakteristik Sistem file Terdistribusi

 Transpansi

File service biasanya merupakan service yang harus diload paling berat dalam sebuah intranet, sehingga fungsionalitas dan performancenya sangat penting.

o Transparansi akses

o Transparansi lokasi

o Transparansi mobilitas

o Transparansi performance

o Transparansi pengukuran

 Update file konkuren

Perubahan pada sebuah file oleh seorang klien seharusnya tidak menganggu operasi dari klien lain yang pada saat bersamaan mengakses atau mengubah file yang sama.

 Replikasi file

Beberapa file service mendukung penuh replikasi, tetapi kebanyakan mendukung caching file atau portion file secara lokal, bentuk replikasi yang terbatas.

 Keheterogenan sistem operasi dan hardware

Antarmuka service sebaiknya didefinisikan sehingga software klien dan server dapat diimplementasikan untuk sistem operasi dan komputer yang berbeda.

 Toleransi kesalahan

Server bisa menjadi stateless, sehingga dapat di-restart dan service di-restore Kembali setelah mengalami failure tanpa perlu me-recover state sebelumnya.

Konsistensi

Ketika file-file direplikasi atau di-cache pada site yang berbeda, ada delay yang tak bisa dihindari pada propagasi modifikasi dari satu site ke set lain yang membawa copy, dan ini bisa menghasilkan beberapa deviasi dari one-copy semantic.

Keamanan

Secara virtual, semua sistem file menyediakan mekanisme kontrol akses berdasarkan kegunaan dari daftar kontrol akses.

Efisiensi

File service terdistribusi sebaiknya menawarkan fasilitas yang paling tidak, sama bagusnya dengan yang ditemukan pada sistem file konvensional, dan sebaiknya mendapat level performance yang dapat diperhitungkan.

2. **File Service Architecture**

Pembagian tanggung jawab antar modul didefinisikan sebagai berikut ini :

- **Layanan file flat**

  Layanan file flat berkonsentrasi pada pengimplementasian operasi dari konten suatu file.

- **Layanan direktori**

  Layanan direktori menyediakan pemetaan antara nama teks untuk file dan UFIDnya.

- **Modul klien**

  Modul klien berjalan pada tiap komputer klien, mengintegrasi dan mengextend operasi dari layanan file flat dan layanan direktori dibawah antarmuka pemrograman aplikasi tunggal yang bisa digunakan oleh program tingkat pengguna di komputer klien.

- **Antarmuka layanan file flat**

  Merupakan antarmuka RPC yang digunakan oleh modul klien. Tidak digunakan secara langsung oleh program tingkat pengguna.

Tabel 2. Operasi pelayanan file flat

Read(FileId, i, n) > *Data*

-Throws BadPosition

Jika $1 \leq i \leq$ *Length(File)*: membaca sequence sebanyak n item dari file yang dimulai dari item i dan memasukkannya ke *Data*

Write(FileId, i) -> *Data*

-Throws BadPosition

Jika 1 ≤ i ≤ *Length(File)+1*: menulis sequence Data ke file, dimulai dari item i, meng-extend file jika diperlukan

Create() -> FileId Membuat file baru dengan panjang 0 dan mengirimkan UFID

untuknya

Delete(FileId) Menghapus file dari tempat penyimpanan file

GetAttributes(FileId) -> Attr Mengembalikan atribut file untuk file tersebut

SetAttributes(FileId, Attr) Men-set atribut file (hanya atribut yang berwarna putih pada tabel 3)

Kontrol akses

Pada sistem file UNIX, hak askes pengguna bergantung pada mode akses (baca atau tulis) yang di-request pada panggilan pembuka dan file hanya dibuka jika pengguna benar-benar memiliki hak.

Antarmuka layanan direktori

Tujuan utama dari layanan direktori yaitu untuk menyediakan layanan untuk menerjemahkan nama teks ke UFID.

Tabel 3. Operasi pelayanan direktori

Lookup(Dir, Name) -> FileId

throws *Not Found*

Mengalokasikan nama teks pada direktori dan mengembalikan relevant UFID. Jika *Name* tidak ada di direktori, dibuat suatu perkecualian.

AddName(Dir, Name, File)

throws *Name Duplicate*

Jika *Name* tidak ada di direktori, tambahkan (*Name, File)* ke direktori dan meng-update record atribut file.

Jika *Name* sudah ada di direktori: dibuat perkecualian.

UnName(Dir, Name)

-throws *Not Found*

Jika *Name* ada di direktori: entry yang mengandung *Name* dihapus dari direktori.

Jika *Name* tidak ada di direktori: dibuat perkecualian.

GetNames(Dir, Pattern) -> NameSeq Mengembalikan semua nama teks pada direktori yang

cocok dengan reguler expression *Pattern.*

Sistem file hierarki

Sistem file hierarki seperti salah satu yang UNIX sediakan terdiri atas banyak direktori

disusun dalam str uktur pohon. Tiap direktori membawa nama file dan direktori lain yang bisa diakses dari situ.

Pengelompokkan file

Kelompok file merupakan sekumpulan file yang berlokasi pada sebuah server. Sebuah server bisa membawa beberapa kelompok file, dan kelompok-kelompok tersebut dapat dipindah antar server, tetapi sebuah file tidak bisa pindah ke grup lain.

Uraian sub topik ke-1

2. Sistem File Network

3. **Sistem File Sun Network**

Sistem file virtual

NFS menyediakan transparansi akses: program pengguna dapat mengakses operasi file untuk file lokal ataupun remote tanpa perbedaan yang berarti.

Integrasi klien

Modul klien NFS memainkan peran dari modul klien dalam model arsitektur kita, yaitu menyediakan antarmuka yang tepat guna untuk program aplikasi konvensional.

Kontrol dan autentikasi akses

Tidak seperti sistem file UNIX konvensional, server NFS *stateless* dan tidak menjaga file tetap terbuka demi kepentingan klien.

Antarmuka server NFS

Representasi singkat menenai antarmuka RPC disediakan oleh NFS server.

Layanan mount

Mounting dari sub-tree sistem file remote oleh klien disupport dengan proses layanan mount yang terpisah yang berjalan pada level pengguna pada tiap komputer server NFS.

Translasi nama path

Sistem file UNIX menerjemahkan dari multi-part file pathname ke i-node reference secara satu demi satu kapanpun panggilan sistem *open*, *creat*, ataupun *stat*.

Automounter

Automounter ditambahkan ke implementasi UNIX dari NFS dengan tujuan untuk mount direktori remote secara dinamis kapanpun titik mount kosong direferensi oleh klien.

Server caching

Caching pada klien dan komputer server merupakan fitur yang sangat diperlukan dari implementasi NFS dengan tujuan untuk mendapatkan performance yang sepurna.

Client caching

Modul klien NFS men-cache hasil operasi dari read, write, getattr, lookup, dan reader dengan tujuan mengurangi jumlah permintaan yang masuk ke server. Beberapa langkah
untuk mengurangi traffic panggilan gettatr ke server:

3. setiap kali nilai baru dari Tmserver diterima di client, itu diterapkan ke semua entri cache yang berasal dari file yang bersangkutan.
    1. Nilai attribut saat ini dikirim “piggybacked” bersama dengan hasil dari tiap operasi
        a. pada sebuah file, dan apabila nilai Tmserver telah diubah, client menggunakannya untuk update entri cache yang berkaitan dengan file tersebut.
    2. Algoritma yang adaptif untuk mengeset freshness garis t internal di atas mengurangi jauh traffic untuk lebih banyak file.
    3. Optimisasi lain
    4. Prosedur validasi tidak menjamin konsistensi file pada level yang sama yang disediakan
    5. pada sistem UNIX konvensional, karena update terbaru tidak selalu nampak ke client
    6. yang men-sharing sebuah file.

Mengamankan NFS dengan Kerberos

Dalam standar implementasi NFS yang asli, identitas user termasuk dalam tiap permintaan/reques dalam form sebuah numerical identifier yang
terenkripsi/tersandikan. NFS tidak melakukan pengecekan lebih jauh untuk autentifikasi identifier yang disediakan. Hal ini menandakan tingkat kepercayaan yang tinggidalam
integritas client komputer dansoftware oleh NFS, sedangkan sasaran dari Kerberos dan sistem security authenticity-based lainnya adalah untuk mengurangi rentang kepercayaan yang diasumsikan terhadap suatu komponen. Ketika NFS digunakan dalam

suatu lingkungan yang “ter-kerberos”, NFS dapat menerima reques hanya dari client yang identitasnya dapat ditampilkan telah dikonfirmasi oleh kerberos. Pada setiap permintaan pengaksesan file, server NFS mengechek identitas user serta alamat pengirim dan memberikan akses hanya jika cocok denga yang tersimpan di server.

Performa

NFS biasanya tidak memaksimalkan performa pinalty dibanding denga akses ke file yang disimpan dalam local disk. Selain itu masih ada 2 lagi permasalahan:

- frekuensi penggunaan “gettatr call” dalam urutan untuk fetch timestamp dari server untuk validasi chace.
- Relatif kurang dari segi performa dalam operasi write karena write-throught telah digunakan pada server.

NFS summary

Transparansi akses. Modul client NFS menyediakan antarmuka pemrograman aplikasi ke proses lokal yang identik dengan interface OS lokal.

Transparansi lokasi. Setiap client menetapkan “file name space” dengan menambahkan direktori yang di-mountn dalan remote filesystem ke local name spacenya.

File system harus di export oleh node yang memuatnya dan remoted-mounted oleh client sebelum dapat diakses oleh proses yang berjalan di client.

Transparansi mobilitas.

File sistem mungkin saja dapat dipindahkan diantara server

yang ada, walaupun demikian remote mount table pada setiap client harus di-update kemudian secara terpisah untuk meng-enable client untuk mengakses file system di lokasi yang baru. *Scability*. NFS server dapat di bangun untuk menghendel beban yang sangat besar dengan cara efektif dan cost yang efektif. *File replication.* Read-only file dapat di replikasi di beberapa server NFS, tetapi NFS tidak dapat mendukung file replikasi dengan update.

Hardware dan OS yang heterogen.

NFS telah diimplementasikan ke hampir semua OS serta hardware flatform dan juga didukung oleh berbagai filling sistem.

Toleransi kesalahan.

Dalam NFS, client mengakses remore file mirip dengan akses file lokal. Ketika server fails, servis yang disediakan ditunda sampai server direstart, ketika telah direstart, client akan melanjutkan proses dari titik terjadinya kesalahan.

Keamanan.

Integrasi NFS dengan kerberos adalah langkah utama yang dilakukan sebagai kebutuhan keamanan yang hanya muncul dari koneksi banyak intranet ke internet.

4. Andrew File System

AFS menyediakan akses transparan ke remote shared file untuk program UNIX yang berjalan di workstation. Akses ke AFS file menggunakan file UNIX normal primitif, meng-enable programUNIX yang ada to aksesfile tanpa modifikasi atau rekompilasi. Perbedaan mencolok antara NFS dan AFS terletak pada desain dan implementasinya. AFS

didesain dengan performa baik untuk jumlah penggunak aktif yang lebih besar daripada didtem file terdistribusi lainnya. AFS memiliki dua karakteristik desain yang luar biasa:

- whole-file serving : seluruh isi direktori dan file di transmisikan ke komputer lient oleh server AFS.
- caching : setiap kali copy dari sebuah file atau chunk telah ditransfer ke komputer client, maka akan disimpan di cache di local disk. Cache tersebut mengandung ratusan file yang telah digunakan oleh komputer tersebut dan bersifat permanen.

Skenario yang mengilustrasikan operasi AFS:

- ketikaproses user di komputer client menyetakan sebuah open sistem call pada sebuah file yang merupakan shared file dan tidak ada copy dari file tersebut pada local chace, server memuat dimana file diletakkan dan dikirim poermintaan untuk copy dari file tersebut
- copian tersebut disimpan di local UNIX file sistem pada komputer client.
- Subsequent read, write dan operasi lainnya pada file oleh proses pada komputer client diterapkan pada copian tersebut.

Ketika proses di komputer client menyatakan sebuah close system call, jika isi copian tersebut telah terupdate, maka akan dikirim kembali nke server. Server akan mengupdate isi dan timestamp file. Dan kop[ian pada local disk akan tetap, mungkin saja akan digunakan lagi pada komputer tersebut.

4.1 Implementasi

AFS mengimplementasikan 2 komponen software yang disebut Vice dan Venus. Vice adalah nama untuk software yang berjalan di server dan venus untuk yang berjalan di client.

File yang tersedia bagi proses di workstation dapat berasal dari local maupun shared file. Local file di hendel sebagai normal UNIX file. File tersebut disimpan di disk worksstation dan hanya dapat digunakan oleh proses local. Shared file tersimpan di server dan copiannya dicache pada local disk workstation.

Kernel UNIX ditiap workstation dan server adalah modifikasi dari BSD UNIX. Desain modifikasi ini untuk menangkap open, close dan file sistem call lainnya ketika merujuk pada shared file dan melewatkannya ke proses pada venus pda komputer client/worstation.

Sebuah partisi pada local disk pada tiap workstation digunakan sebagai cache, yang memuat copian dari shared file. Venus akan mengatur penggunaan cache ini, membuang file yang paling tidak dibutuhkan bisa ada file yang akan diterima dari server sedangkan cache sudah full.

Lokasi database

Tiap server mengandung kopian dari sebuah lokasi database yang direplikasi yang memberikan mapping dari volume name ke server.

Thread

Implementasi dari vice dan venus menggunakan sebuah non-pre-emptive thread pakege untuk meng-enable permintaan untuk diproses bersamaan pada beberapa client dan server. Pada client, table menggambarkan isi dari cache dan volume database pada memory yang dishare dengan thread venus.

Read-only replicas.

Volume yang mengandung file-file yang sering dibaca namun jarang diubah, seperti UNIX/bin, dapat direplikasi sebagai read-only volume pada beberapa server.

Bulk transfer. AFS mentransfer file antara client dan server dalam paket-paket 64-kilobyte. Penggunaan ukuran paket dalam ukuran yang besar adalah sebuah bantuan penting untuk performa, meminimalisir efek dari network latncy. Hal ini dapat mengoptimalkan pengguanaan jaringan.

Partial file caching.

Kebutuhan untuk mentransfer seluruh isi file ke client bahkan *ketika permintaan aplikasi adalah hanya membaca sebagian kecil dari file adalah suatu ketidakefisienan penggunaan* resource. AFS versi 3 telah menghilangkan requerment tersebut, mengizinkan data ditransfer dan di cache dalam blok 64-kbyte dan tetap mempertahankan konsistensi semantik dan fitur lain dari protokol AFS.

Performa.

Tujuan utama dari AFS adalah pada skalabilitas, jadi performa dengan jumlah user yang banyak adalah perhatian khusus.

Wide-area support. AFS versi 3 telah mendukung multiple administratif cell, masing masing dengan server, client, system administrator dan user masing-masing. Tiap cell adalah lingkungan yang autonomos, tetapi

penggabungan cell-cell dapat dapat bekerjasama dalam menyajikan user secara seragam, seamless file name space.

Uraian sub topik ke-2

C. Latihan

a. Jelaskankarakteristik dari File System.…?
b. Jelaskan apa yang dimaksud transparansi obilitas pada NFS,,,?
c. Sebutkan kelebihan dari distributed file system…/

D. Kunci Jawaban

a. Jawaban latihan soal ke-1

Karakteristik Sistem file

Sistem file bertanggung jawab pada pengorganisasian, penyimpanan, permintaan kembali, penamaan, sharing, dan proteksi terhadap file. Sistem file menyediakan antarmuka pemrograman yang mengkarakterisasikan abstraksi file, membebaskan pemrogram dari kefokusannya pada detail alokasi storage dan layout. File disimpan dalam disk atau media penyimpanan non-volatile lain

b. Jawaban latihan soal ke-2

Transparansi mobilitas.

File sistem mungkin saja dapat dipindahkan diantara server yang ada, walaupun demikian remote mount table pada setiap client harus di-update kemudian secara terpisah untuk meng-enable client untuk mengakses file system di lokasi yang baru. *Scability*. NFS server dapat di bangun untuk menghendel beban yang sangat besar dengan cara efektif dan cost yang efektif. *File replication.* Read-only file dapat di replikasi di beberapa server NFS, tetapi NFS tidak dapat mendukung file replikasi dengan update

c. Jawaban latihan soal ke-n

Systrm File terdistribusi memberikan beberapa layanan kepada para pengguna diantaranya adalah :

o Transparansi akses

o Transparansi lokasi

o Transparansi mobilitas

o Transparansi performance

E. Daftar Pustaka

1. Couloris et. al. 2012. Distributed Systems Concepts and Design, Fifth Edition. Addison Wesley.
2. Van Steen and Tanenbaum, 2017. Distributed Systems: Prinsiples and Paradigms. 3e. Prentice-Hall

Link Journal ;

https://scholar.google.com/citations?user=TvjaNqkAAAAJ&hl=en#d=gs_md_cita-d&u=%2Fcitations%3Fview_op%3Dview_citation%26hl%3Den%26user%3DTvjaNqkAAAAJ%26citation_for_view%3DTvjaNqkAAAAJ%3Au-x6o8ySG0sC%26tzom%3D-420

https://komputasi.files.wordpress.com/2018/03/mvsteen-distributed-systems-3rd-preliminary-version-3-01pre-2017-170215.pdf

DAFTAR LINK JOURNAL

Mata Kuliah :

Pemrosesan Data Tersebar

Kode Matakuliah : PT 1611

Pertemuan	LINK jurnal
1.	
2	
3	
4	
9	
10	
11	
12	
13	

14

5

6

7

8

MODUL PEMROSESAN DATA TERSEBAR

(PTI 611)

MODUL SESI 13

SISTEM TERDISRIBUSI BERBASIS WEB

DISUSUN OLEH

HERMANSYAH S.Kom., M.Kom.

UNIVERSITAS ESA UNGGUL

2020

Web Site pada Organisasi Tradisional.

Kemampuan Akhir Yang Diharapkan

Setelah mempelajari modul ini, diharapkan mahasiswa mampu :

1. Mahasiswa memahami mekanisme komunikasi di sistem web pada DDP
2. Mahasiswa memahami konsep client side, server side dan mekanisme komunikasi di sistem web pada DDP
3.

B. Uraian dan Contoh

1. Web Site Pada Organisasi tradisional

Uraian sub topik ke-1

System terdistribusi berbasis web

Pendahuluan :

Pada organisai web tradisional mekanisme kerja dimulai client meminta document, kangkah berikutnya Server membaca dokumen dari file local lalu mererspon permintaan dari client tersebut.

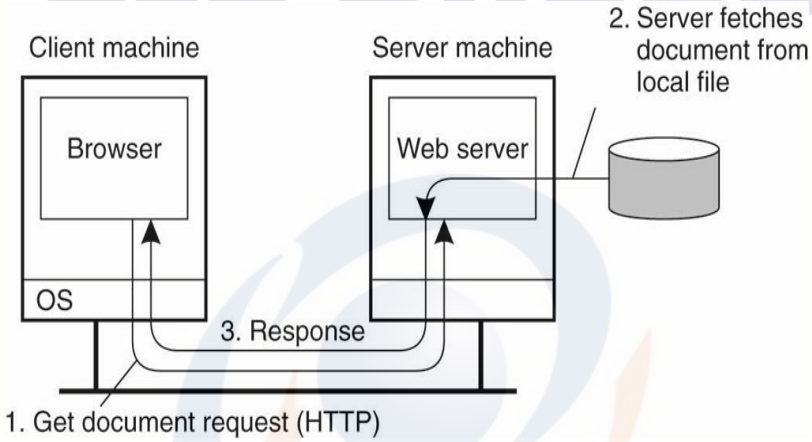


Figure 12-1. The overall organization of a traditional Web site

Pada tradisional ini type data yang diolah seperti tanel berikut :

Type	Subtype	Description
Text	Plain	Unformatted text
	HTML	Text including HTML markup commands
	XML	Text including XML markup commands
Image	GIF	Still image in GIF format
	JPEG	Still image in JPEG format
Audio	Basic	Audio, 8-bit PCM sampled at 8000 Hz
	Tone	A specific audible tone
Video	MPEG	Movie in MPEG format
	Pointer	Representation of a pointer device for presentations
Application	Octet-stream	An uninterpreted byte sequence
	Postscript	A printable document in Postscript
	PDF	A printable document in PDF
Multipart	Mixed	Independent parts in the specified order
	Parallel	Parts must be viewed simultaneously

Figure 12-2. Six top-level MIME types and some common subtypes

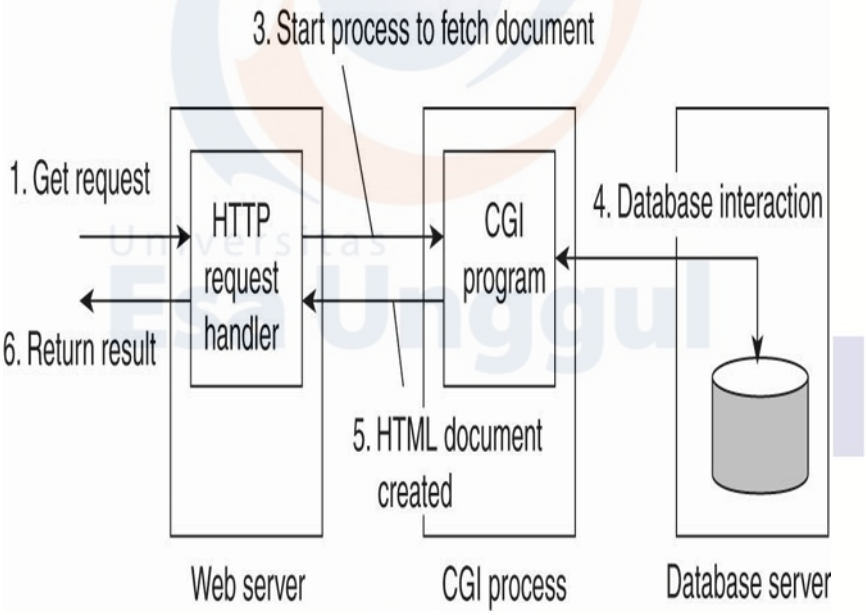


Figure 12-3. The principle of using server-side CGI program

Dasar Layanan Web:

Ada sekelompok sistem berbasis Web yang berkembang pesat yang menawarkan layanan umum untuk aplikasi jarak jauh tanpa interaksi langsung dari pengguna akhir. Organisasi ini mengarah pada konsep layanan Web (Alonso et al., 2004).

θ Sederhananya, layanan Web tidak lain adalah layanan tradisional (misalnya, penamaan, layanan pelaporan cuaca, pemasok elektronik, dll.) Yang tersedia melalui Internet.

Membuat Apa yang membuat layanan Web istimewa adalah ia mematuhi kumpulan standar yang memungkinkannya ditemukan dan diakses melalui Internet oleh aplikasi klien yang mengikuti standar tersebut juga. Inti dari arsitektur layanan Web [lihat juga Booth et al. (2004)]

 Layanan ini mematuhi standar Universal Description, Discovery and Integration (UDDI). UDDI mengatur tata letak database yang berisi deskripsi layanan yang akan memungkinkan klien layanan Web untuk menelusuri layanan yang relevan.

 Layanan dijelaskan melalui Web Services Definition Language (WSDL) yang merupakan bahasa formal yang sangat mirip dengan Interface Definition Languages (IDL) yang digunakan untuk mendukung komunikasi berbasis RPC. Deskripsi WSDL berisi definisi yang tepat dari antarmuka yang disediakan oleh layanan, yaitu, spesifikasi prosedur, tipe data, lokasi (logis) layanan, dll. Masalah penting dari deskripsi WSDL adalah yang dapat secara otomatis diterjemahkan ke sisi klien dan rintisan sisi server, sekali lagi, analog dengan pembuatan rintisan dalam sistem berbasis RPC biasa.

 Akhirnya, elemen inti dari layanan Web adalah spesifikasi bagaimana komunikasi terjadi. Untuk tujuan ini, Simple Object Access Protocol (SOAP) digunakan, yang pada dasarnya adalah kerangka kerja di mana banyak komunikasi antara dua proses dapat distandarisasi. Kami akan membahas SOAP secara mendetail di bawah ini, di mana juga akan menjadi

jelas bahwa memanggil kerangka kerja sederhana tidak benar-benar dibenarkan.

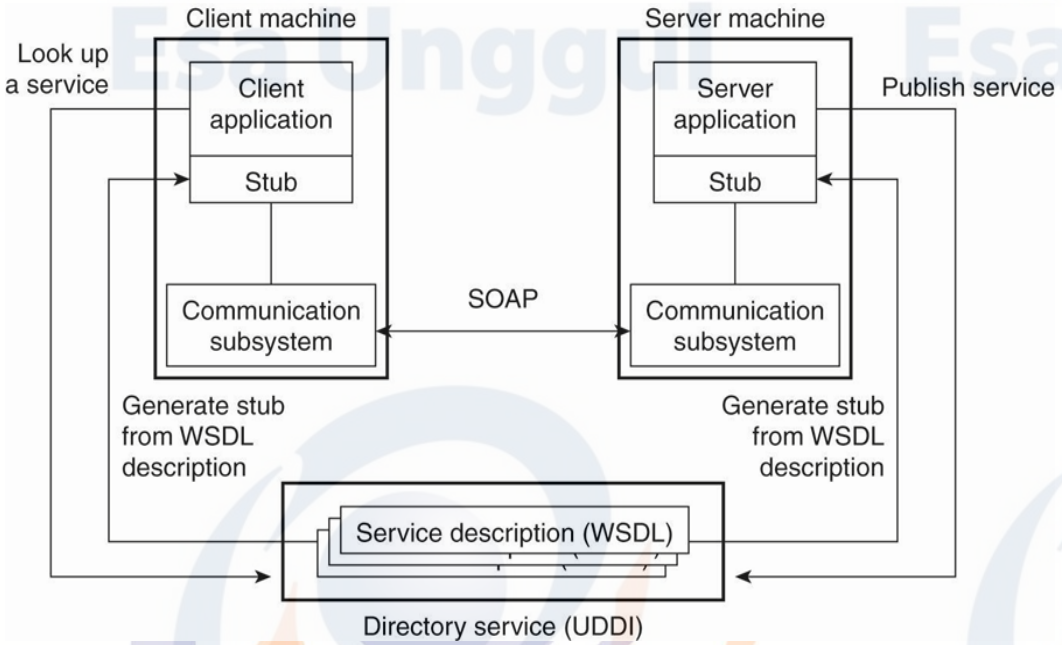


Figure 12-4. The principle of a Web service

2. Komposisi dan Koordinasi Layanan Web

Uraian sub topik ke-2

Komposisi dan Koordinasi Layanan Web

Arsitektur yang dijelaskan sejauh ini relatif mudah: layanan diimplementasikan melalui aplikasi dan pemanggilannya dilakukan sesuai dengan standar tertentu.

Dalam model sejauh ini, layanan Web ditawarkan dalam bentuk pemanggilan tunggal. Dalam praktiknya, struktur pemanggilan yang jauh lebih kompleks perlu dilakukan sebelum layanan dapat dianggap selesai. Misalnya, toko buku elektronik.

1) Memesan buku membutuhkan pemilihan buku, 2) pembayaran, 3) dan memastikan pengirimannya. Dari perspektif layanan, layanan sebenarnya harus dimodelkan sebagai transaksi yang terdiri dari beberapa langkah yang perlu dilakukan dalam urutan tertentu. Dengan kata lain, kita berurusan dengan layanan kompleks yang dibangun dari sejumlah layanan dasar.

Kompleksitas meningkat ketika mempertimbangkan layanan Web yang ditawarkan dengan menggabungkan layanan Web dari penyedia yang berbeda. Contoh tipikal adalah merancang toko berbasis web. Sebagian besar toko secara kasar terdiri dari tiga bagian: bagian pertama yang digunakan untuk memilih barang yang dibutuhkan klien, bagian kedua yang menangani pembayaran barang tersebut, dan bagian ketiga yang menangani pengiriman dan pelacakan barang selanjutnya.

Dalam skenario ini, penting bagi pelanggan untuk melihat layanan yang koheren:

yaitu toko tempat dia dapat memilih, membayar, dan mengandalkan pengiriman yang tepat. Namun, secara internal kita perlu menghadapi situasi di mana mungkin tiga organisasi yang berbeda perlu bertindak secara terkoordinasi. Memberikan dukungan yang tepat untuk layanan gabungan semacam itu merupakan elemen penting dari layanan Web.

Setidaknya ada dua kelas masalah yang perlu diselesaikan. Pertama, bagaimana koordinasi antara layanan Web, mungkin dari organisasi yang berbeda, berlangsung?

Kedua, bagaimana layanan dapat dengan mudah disusun?

Koordinasi di antara layanan Web ditangani melalui protokol koordinasi. Protokol semacam itu mengatur berbagai langkah yang perlu dilakukan agar layanan (komposit) berhasil. Masalahnya, adalah untuk memaksa pihak-pihak yang mengambil bagian dalam protokol tersebut mengambil langkah-langkah yang benar pada saat yang tepat.

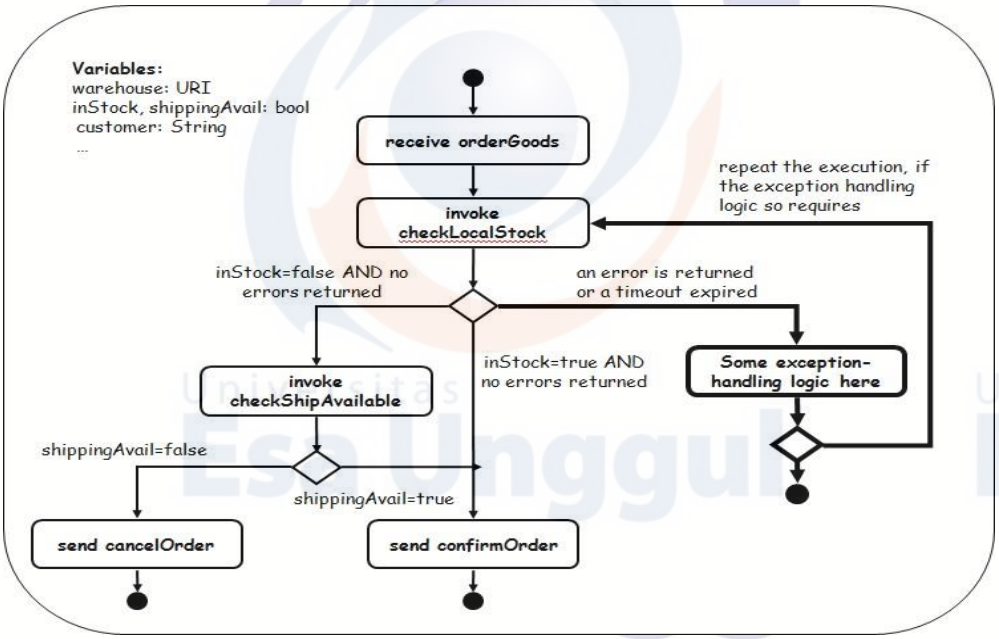
Ada berbagai cara untuk mencapai ini;

 yang paling sederhana adalah memiliki satu koordinator yang mengontrol pertukaran pesan antara pihak-pihak yang berpartisipasi.

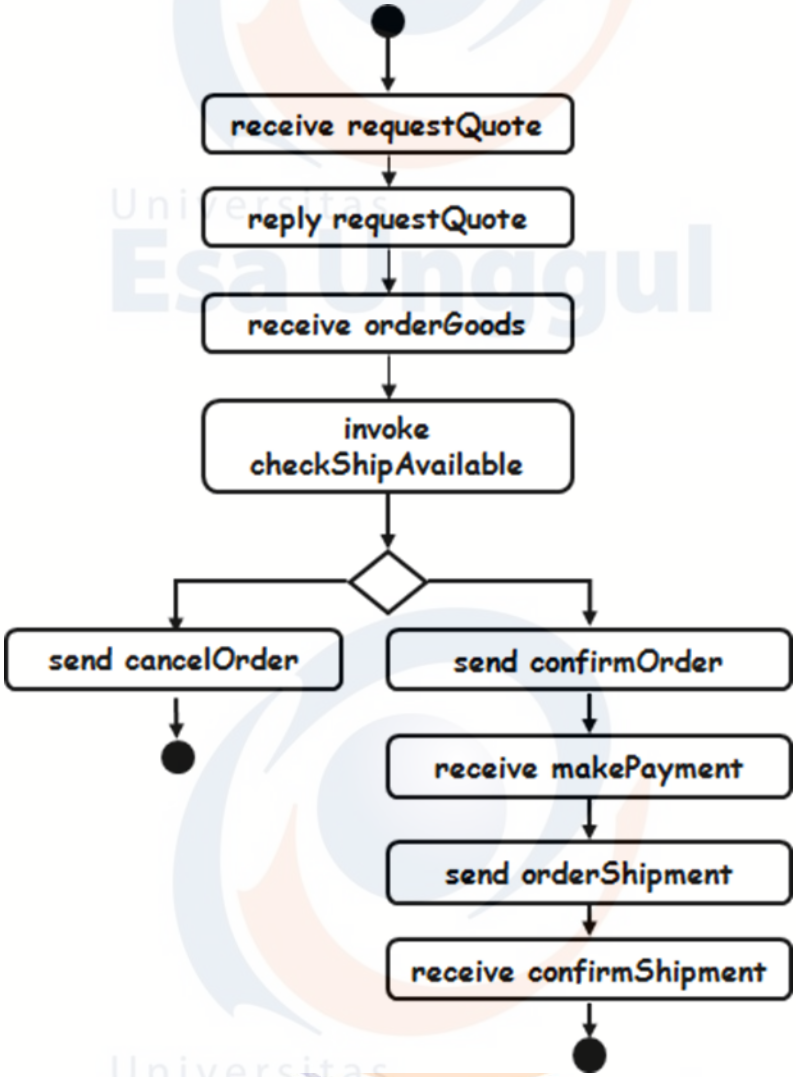
 Namun, meskipun ada berbagai solusi, dari perspektif layanan Web Penting untuk menstandarkan kesamaan dalam protokol koordinasi. Pertama, penting bahwa ketika suatu pihak ingin berpartisipasi dalam protokol tertentu, ia mengetahui dengan proses mana yang harus dikomunikasikan.

 Selain itu, mungkin saja suatu proses terlibat dalam beberapa protokol koordinasi pada saat yang bersamaan. Oleh karena itu, mengidentifikasi contoh protokol juga penting.

 Akhirnya, sebuah proses harus mengetahui peran mana yang harus dipenuhi.



Gambar 12.5, Web Service Composition and Coordination A Sample



Gambar 12.6. Proces pada sisclient

Processes – Clients (1)

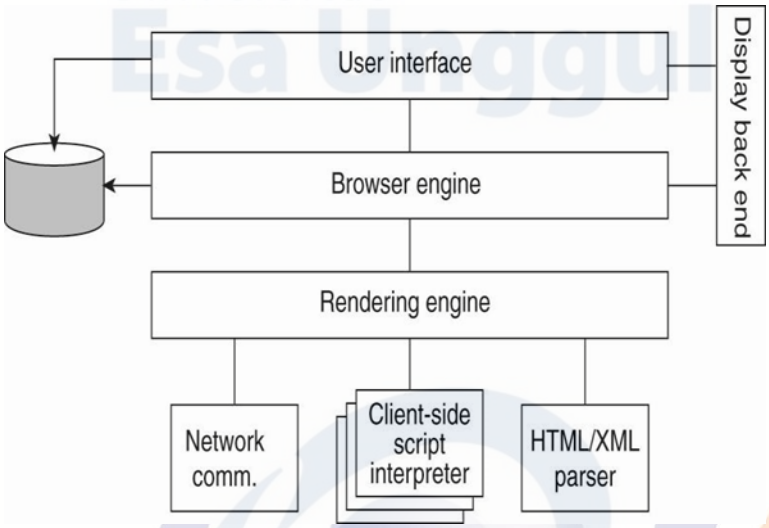
Klien Web terpenting adalah perangkat lunak yang disebut browser Web, yang memungkinkan pengguna menavigasi halaman Web dengan mengambil halaman tersebut dari server dan kemudian menampilkannya di layar pengguna. Browser biasanya menyediakan antarmuka yang menampilkan hyperlink sedemikian rupa sehingga pengguna dapat dengan mudah memilihnya melalui satu klik mouse.

Aspek penting dari browser Web:

 Platform independen.

 Harus mudah dikembangkan sehingga dapat mendukung semua jenis dokumen yang dikembalikan oleh server.

 Proses sisi klien lain yang sering digunakan adalah proxy Web seperti yang ditunjukkan pada Gambar 12.6



Gambar 12.7 Proses pada sisi Server

Processes – Clients

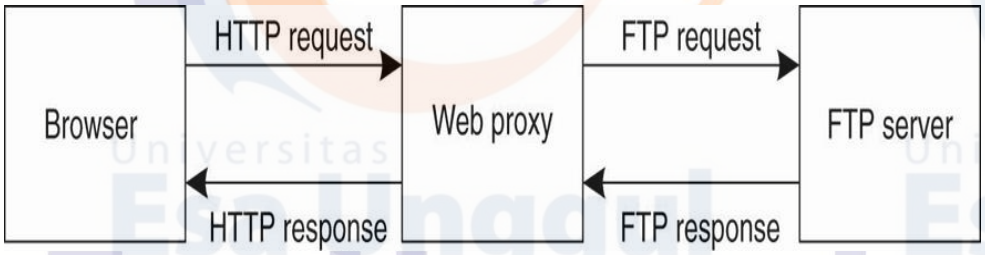


Figure 12-8.. Using a Web proxy when the browser does not speak FTP.

3. Sub sub topik ke-3

Uraian sub topik ke-n

The Apache Web Server

Sejauh ini server Web yang paling populer adalah Apache, yang diperkirakan digunakan untuk menampung sekitar 70% dari semua situs Web.

Lingkungan runtime Apache, yang dikenal sebagai Apache Portable Runtime (APR), adalah pustaka yang menyediakan antarmuka yang tidak bergantung platform untuk penanganan file, jaringan, penguncian, utas, dan sebagainya.

Inti Apache membuat beberapa asumsi tentang bagaimana permintaan yang masuk harus ditangani. Organisasi keseluruhannya ditunjukkan pada Gambar. 12-7. Dasar dari organisasi ini adalah konsep hook, yang tidak lain adalah placeholder untuk kelompok fungsi tertentu.

Sebagai contoh:

 Ada hook untuk menerjemahkan URL ke nama file lokal. Terjemahan seperti itu hampir pasti perlu dilakukan saat memproses permintaan.
 Demikian juga, ada kaitan untuk menulis informasi ke log,
 Pengait untuk memeriksa identifikasi klien,
 Pengait untuk memeriksa hak akses
 Pengait untuk memeriksa tipe MIME mana yang terkait dengan permintaan (misalnya, untuk memastikan bahwa permintaan dapat ditangani dengan benar).

Seperti yang ditunjukkan pada Gambar. 12-7, pengait diproses dalam urutan yang telah ditentukan sebelumnya. Di sinilah kami secara eksplisit melihat bahwa Apache memberlakukan aliran kontrol tertentu terkait pemrosesan permintaan. Fungsi yang terkait dengan hook semuanya disediakan oleh modul terpisah.

Kluster Server Web

Masalah penting yang terkait dengan sifat klien-server dari Web adalah bahwa server Web dapat dengan mudah menjadi kelebihan beban. Solusi praktis yang digunakan dalam banyak desain adalah dengan mereplikasi server pada sekelompok server dan menggunakan mekanisme terpisah, seperti front end, untuk mengarahkan permintaan klien ke salah satu replika.

Aspek penting dari organisasi ini adalah desain ujung depan karena dapat menjadi hambatan kinerja yang serius, apa yang akan dilalui oleh semua lalu lintas.

Secara umum, perbedaan dibuat antara ujung depan yang beroperasi sebagai transportasi
switch layer, dan yang beroperasi pada level layer aplikasi.
Setiap kali klien mengeluarkan permintaan HTTP, itu menyiapkan koneksi TCP ke server. Sakelar lapisan-transportasi hanya meneruskan data yang dikirim bersama koneksi TCP ke salah satu server, bergantung pada beberapa pengukuran beban server. Respons dari server itu dikembalikan ke sakelar, yang kemudian akan meneruskannya ke klien yang meminta.

Kelemahan utama dari transport-layer switch adalah bahwa switch tidak dapat memperhitungkan konten permintaan HTTP yang dikirim sepanjang koneksi TCP. Paling banter, ini hanya dapat mendasarkan keputusan pengalihannya pada beban server.

Web Server Clusters
Figure 12-8. The principle of using a server cluster in combination with a front end to implement a Web service.

Web Server Clusters
menerapkan distribusi permintaan yang peka konten, yang dengannya front end pertama-tama memeriksa permintaan HTTP yang masuk, lalu memutuskan ke server mana permintaan itu harus diteruskan.
Distribusi sadar konten memiliki beberapa keunggulan.
 Misalnya, jika front end selalu meneruskan permintaan untuk dokumen yang sama ke server yang sama, server tersebut mungkin dapat menyimpan dokumen ke cache secara efektif sehingga menghasilkan waktu respons yang lebih tinggi.
 Selain itu, dimungkinkan untuk benar-benar mendistribusikan koleksi dokumen di antara server daripada harus mereplikasi setiap dokumen untuk setiap server. Pendekatan ini membuat penggunaan kapasitas penyimpanan yang tersedia

menjadi lebih efisien dan memungkinkan penggunaan server khusus untuk menangani dokumen khusus seperti audio atau video.

Masalah dengan distribusi sadar konten adalah front end perlu melakukan banyak pekerjaan. Idealnya, seseorang ingin memiliki efisiensi handoff TCP dan fungsionalitas distribusi sadar konten.

Yang perlu kita lakukan adalah mendistribusikan pekerjaan ujung depan, dan menggabungkannya dengan sakelar lapisan transportasi, seperti yang diusulkan dalam Aron et al. (2000). Dalam kombinasi dengan handoff TCP, ujung depan memiliki dua Tugas:

Pertama, ketika sebuah permintaan pertama kali masuk, ia harus memutuskan server mana yang akan menangani sisa komunikasi dengan klien. Kedua, ujung depan harus meneruskan pesan TCP klien yang terkait dengan koneksi TCP yang diserahkan.

Kedua tugas ini dapat didistribusikan seperti yang ditunjukkan pada Gambar 12-9. Petugas operator bertanggung jawab untuk memutuskan ke server mana koneksi TCP harus diserahkan. Distributor memonitor lalu lintas TCP yang masuk untuk koneksi yang diserahkan. Sakelar digunakan untuk meneruskan pesan TCP ke distributor.

Ketika klien pertama kali menghubungi layanan Web, pesan penyiapan koneksi TCP-nya diteruskan ke distributor, yang kemudian menghubungi petugas operator untuk membiarkannya memutuskan ke server mana koneksi harus diserahkan. Pada saat itu, sakelar diberitahu bahwa ia harus mengirim semua pesan TCP lebih lanjut untuk koneksi itu ke server yang dipilih.

Web Server Clusters

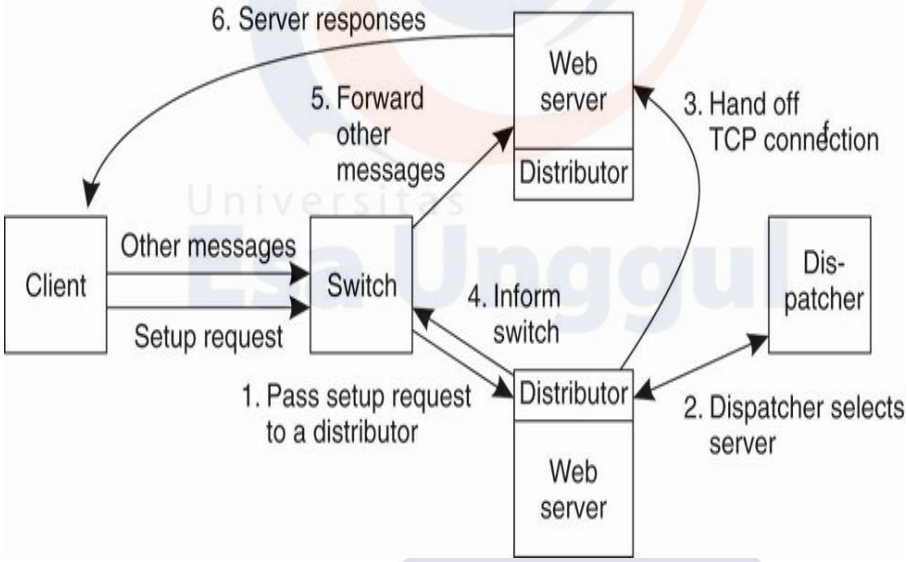


Figure 12-9. A scalable content-aware cluster of Web servers

Web Server Clusters

Ada berbagai alternatif lain dan penyempurnaan lebih lanjut untuk menyiapkan cluster server Web.

Misalnya, alih-alih menggunakan jenis front end apa pun, Anda juga dapat menggunakan DNS round-robin di mana satu nama domain dikaitkan dengan beberapa alamat IP. Dalam kasus ini, ketika menyelesaikan nama host situs Web, browser klien akan menerima daftar beberapa alamat, setiap alamat sesuai dengan salah satu server Web.

Biasanya, browser memilih alamat pertama dalam daftar. Namun, apa yang dilakukan server DNS populer seperti BIND adalah mengedarkan entri dari daftar yang dikembalikan (Albitz dan Liu, 2001). Akibatnya, kami memperoleh distribusi permintaan yang sederhana melalui server di cluster.

Terakhir, dimungkinkan juga untuk tidak menggunakan perantara apa pun tetapi hanya memberikan setiap server Web dengan alamat IP yang sama. Dalam hal ini, kita perlu berasumsi bahwa semua server terhubung melalui LAN siaran tunggal. Apa yang akan terjadi adalah ketika permintaan HTTP tiba, router IP yang

terhubung ke LAN itu akan meneruskannya ke semua server, yang kemudian menjalankan algoritme terdistribusi yang sama untuk secara deterministik memutuskan mana di antara mereka yang akan menangani permintaan tersebut

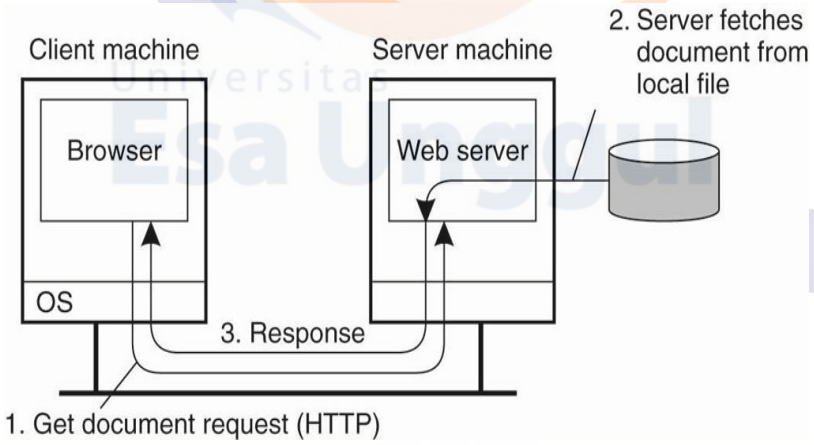
C. Latihan

a. Jelaskan Mekanisme kerja Web pada organisasi tradisinonal…?
b. Jelaskan elemen-elemen inti layanan Web.
c. Jelaskan Pengertian dari Web Browser…?

D. Kunci Jawaban

a. Jawaban latihan soal ke-1

Pada organisai web tradisional mekanisme kerja dimulai client meminta document, kangkah berikutnya Server membaca dokumen dari file local lalu mererspon permintaan dari client tersebut.



b. Jawaban latihan soal ke-2

LayananWeb adalah sisem software yang di disain untuk mendukung interaksi interoperable mesin ke mesin melakui jarigan. Dalamkonteks aplikasi Web biasanya merujuk ke satu set API yag dapat diakses mrlalui internet.

c. Jawaban latihan soal ke-n

Prangkat lunak yang berfungsi untuk menerima dan menyajikan informasi dari internet kepada yang memerlukan.

Komunikasi Dalam Web Terdistribusi

A. Kemampuan Akhir Yang Diharapkan

Setelah mempelajari modul ini, diharapkan mahasiswa mampu :

1. Memahami dan Mengerti cara dan teknik komuniasi Dalam Jaringan Web Terdistribusi
2. Memahami dan Mengerti Bgagaimana Meng-Hosting Web dalam Jaringan Terdistribus

B. Uraian dan Contoh

1. Komunikasi

Uraian sub topik ke-1

Communication

Ketika datang ke sistem terdistribusi berbasis web, hanya ada beberapa protokol komunikasi yang digunakan.

Pertama, untuk sistem Web tradisional, HTTP adalah protokol standar untuk bertukar pesan.

Kedua, saat mempertimbangkan Layanan Web, SOAP adalah cara default untuk pertukaran pesan.

Communication HTTP Connections

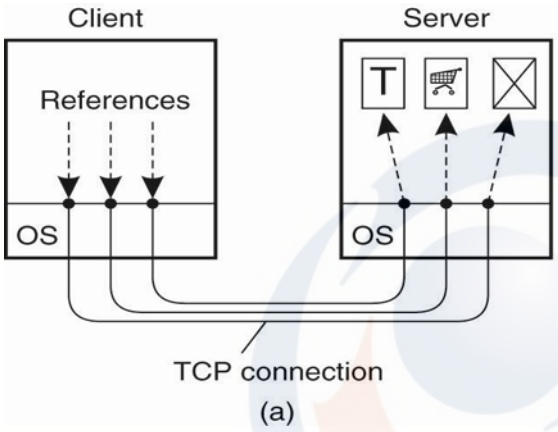
Dalam HTTP versi 1.0 dan yang lebih lama, setiap permintaan ke server memerlukan pengaturan koneksi terpisah, seperti yang ditunjukkan pada Gambar

12-10 (a). Ketika server merespons, koneksi diputus lagi. Koneksi semacam itu disebut tidak persisten.

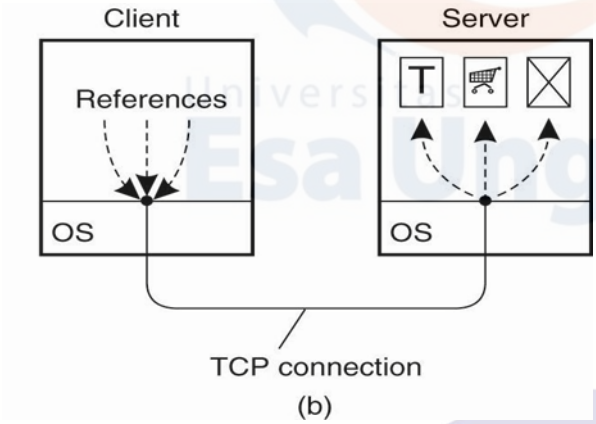
Kelemahan utama dari koneksi non-persisten adalah relatif mahal untuk menyiapkan koneksi TCP. Akibatnya, waktu yang dibutuhkan untuk mentransfer seluruh dokumen dengan semua elemennya ke klien mungkin sangat lama.
Perhatikan bahwa HTTP tidak menghalangi klien menyiapkan beberapa koneksi secara bersamaan ke server yang sama. Pendekatan ini sering digunakan untuk menyembunyikan latensi yang disebabkan oleh waktu penyiapan koneksi, dan untuk mentransfer data secara paralel dari server ke klien. Banyak browser menggunakan pendekatan ini untuk meningkatkan kinerja.

Pendekatan lain yang diikuti dalam HTTP versi 1.1 adalah dengan menggunakan koneksi persisten, yang dapat digunakan untuk mengeluarkan beberapa permintaan (dan tanggapannya masing-masing), tanpa perlu koneksi terpisah untuk setiap pasangan (request / response). Untuk lebih meningkatkan kinerja, klien dapat mengeluarkan beberapa
permintaan berturut-turut tanpa menunggu respon untuk permintaan pertama (juga disebut
sebagai pipelining). Menggunakan koneksi persisten diilustrasikan pada Gambar 12-10 (b).

Communication HTTP Connections



Using non-persistent connections



Using persistent connections

HTTP Methods

Operation	Description
Head	Request to return the header of a document
Get	Request to return a document to the client
Put	Request to store a document
Post	Provide data that are to be added to a document (collection)
Delete	Request to delete a document

Figure 12-11. Operations supported by HTTP.

HTTP Messages (16)

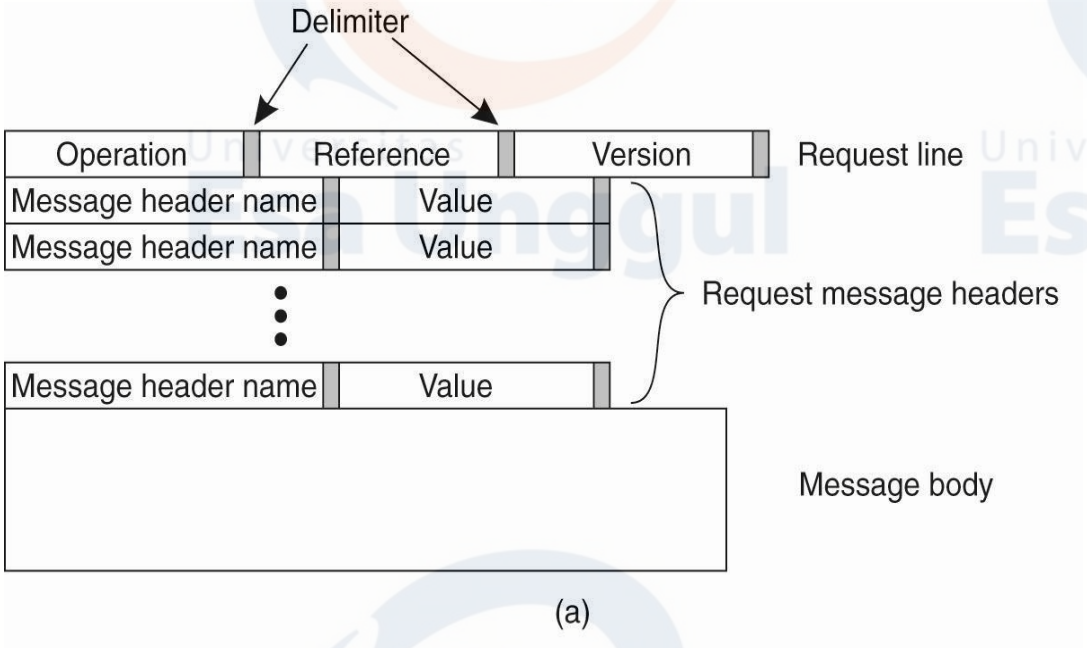
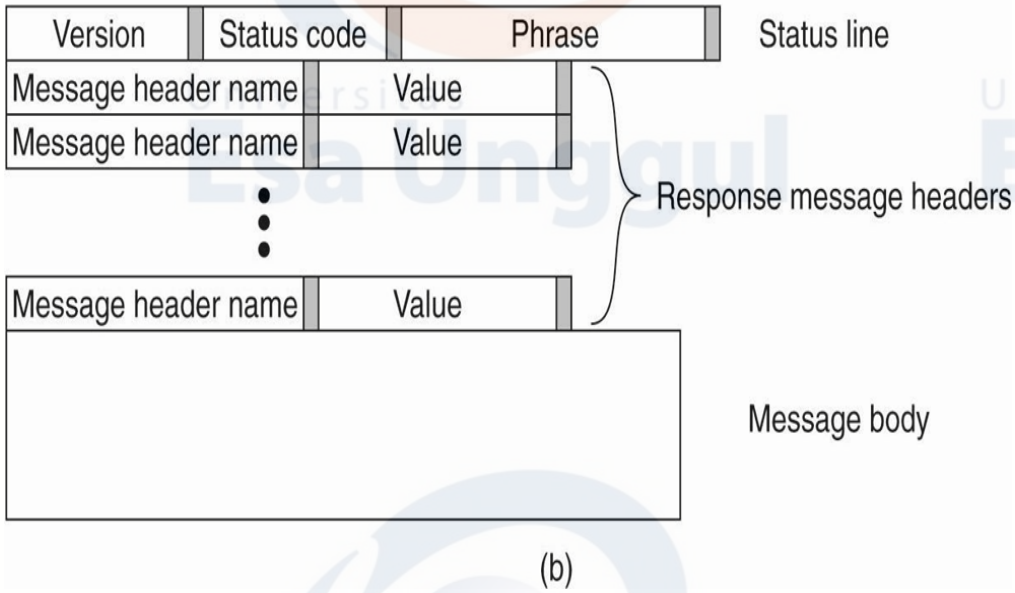


Figure 12-12. (a) HTTP request message

HTTP Messages (2)



Cache Proxy Web

Selain caching di browser dan proxy, juga memungkinkan untuk menempatkan cache yang mencakup suatu wilayah, atau bahkan negara, sehingga mengarah ke

cache Hierarki. Skema semacam itu terutama digunakan untuk mengurangi lalu lintas jaringan, tetapi memiliki kelemahan yaitu berpotensi menimbulkan latensi yang lebih tinggi dibandingkan dengan menggunakan skema non-hierarki. Latensi yang lebih tinggi ini disebabkan oleh kebutuhan klien untuk memeriksa beberapa cache, bukan hanya satu cache dalam skema nonhierarki. Namun, latensi yang lebih tinggi ini sangat terkait dengan popularitas dokumen: untuk dokumen populer, kemungkinan menemukan salinan dalam cache yang lebih dekat ke klien lebih tinggi daripada untuk dokumen yang tidak populer.

Sebagai alternatif untuk membangun cache hierarkis, seseorang juga dapat mengatur cache untuk penerapan kooperatif seperti yang ditunjukkan pada Gambar 12-17. Dalam caching kooperatif atau cache terdistribusi, setiap kali cache miss terjadi di proxy Web, proxy terlebih dahulu memeriksa sejumlah proxy tetangga untuk melihat apakah salah satunya berisi dokumen yang diminta. Jika pemeriksaan seperti itu gagal, proxy meneruskan permintaan ke server Web yang bertanggung jawab untuk dokumen tersebut. Skema ini terutama digunakan dengan cache Web yang dimiliki oleh organisasi atau institusi yang sama yang ditempatkan bersama di LAN yang sama.

Web Proxy Caching

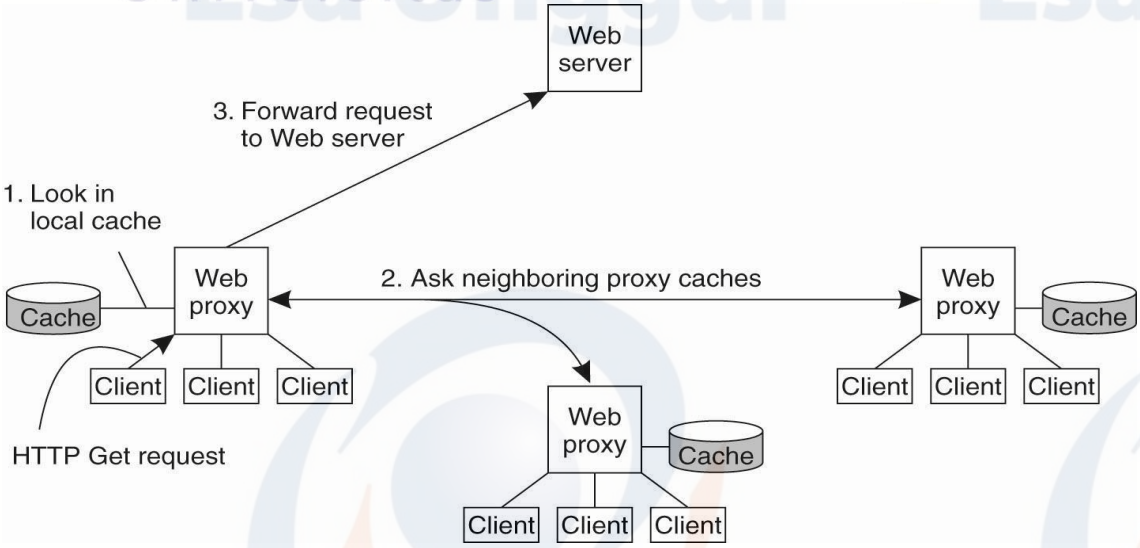


Figure 12-17. The principle of cooperative caching

 Cache kooperatif umumnya terhubung melalui tautan berkecepatan tinggi, waktu transmisi yang diperlukan untuk mengambil dokumen jauh lebih rendah daripada cache hierarkis.

 Selain itu, seperti yang diharapkan, persyaratan penyimpanan tidak terlalu ketat untuk cache kooperatif daripada yang hierarkis.

 Selain itu, mereka menemukan bahwa latensi yang diharapkan untuk cache hierarki lebih rendah daripada cache terdistribusi (Hanya untuk kasus yang disimpan dalam cache ada di web).

Protokol konsistensi cache yang berbeda telah diterapkan di Web. Untuk menjamin bahwa dokumen yang dikembalikan dari cache konsisten, beberapa proxy Web pertama-tama mengirim permintaan HTTP bersyarat ke server dengan header permintaan If-Modified-Because tambahan, yang menentukan waktu modifikasi terakhir yang terkait dengan dokumen yang di-cache. Hanya jika dokumen telah diubah sejak saat itu, server akan mengembalikan seluruh dokumen. Jika tidak, proxy Web dapat mengembalikan versi cache-nya ke klien lokal yang meminta.

2. Replication for Web Hosting System,

Uraian sub topik ke-2

Replication for Web Hosting System

Karena pentingnya Web terus meningkat sebagai sarana bagi organisasi untuk menampilkan diri dan berinteraksi langsung dengan pengguna akhir, kami melihat pergeseran antara memelihara konten situs Web dan memastikan bahwa situs tersebut dapat diakses dengan mudah dan terus menerus. Perbedaan ini telah membuka jalan bagi Jaringan Pengiriman Konten (CDN). Ide utama yang mendasari CDN ini adalah bahwa mereka bertindak sebagai layanan hosting Web, menyediakan infrastruktur untuk mendistribusikan dan mereplikasi dokumen Web dari banyak situs di Internet. Ukuran infrastruktur bisa sangat mengesankan. Misalnya, pada tahun 2006, Akamai dilaporkan memiliki lebih dari 18.000 server yang tersebar di 70 negara.

Ukuran CDN yang sangat besar mengharuskan dokumen yang dihosting didistribusikan dan direplikasi secara otomatis, yang mengarah ke arsitektur sistem yang mengatur sendiri -> Bab. 2.

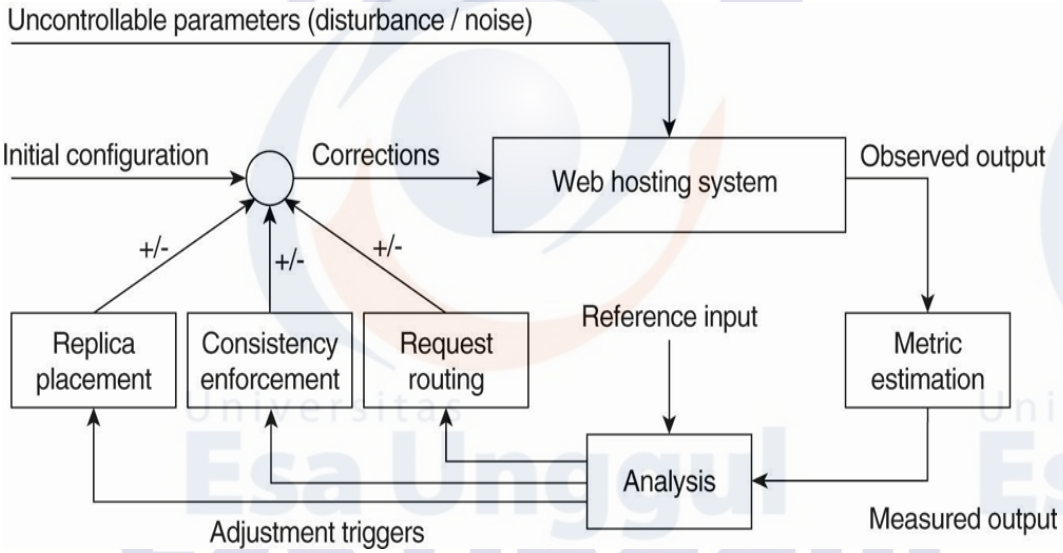
Dalam kebanyakan kasus, CDN skala besar diatur di sepanjang garis loop kontrol umpan balik, seperti yang ditunjukkan pada Gambar. 12-8 dan dijelaskan secara ekstensif dalam Sivasubramanian et al. (2004b).

Pada dasarnya ada tiga jenis aspek yang terkait dengan replikasi dalam sistem hosting Web:

A. Keputusan penempatan replika

B. Penegakan konsistensi

C. Perutean permintaan klien.



Replication of Web Applications

Pertama, untuk meningkatkan kinerja, kami dapat memutuskan untuk menerapkan replikasi penuh dari data yang disimpan di server asal. Skema ini bekerja dengan

baik setiap kali rasio pembaruan rendah dan ketika kueri memerlukan pencarian database yang ekstensif.

Kasus kedua untuk replikasi penuh adalah ketika kueri umumnya kompleks. Dalam kasus database relasional, ini berarti bahwa kueri memerlukan beberapa tabel untuk dicari dan diproses, seperti yang umumnya terjadi pada operasi gabungan. Menentang kueri kompleks adalah kueri sederhana yang umumnya hanya memerlukan akses ke satu tabel untuk menghasilkan respons. Dalam kasus terakhir, replikasi parsial dimana hanya sebagian dari data yang disimpan di server edge mungkin sudah cukup.

Masalah dengan replikasi parsial adalah mungkin sangat sulit untuk secara manual memutuskan data mana yang diperlukan di server edge. Sivasubramanian et al. (2005) mengusulkan untuk menangani ini secara otomatis dengan mereplikasi catatan sesuai dengan prinsip yang sama seperti Globule mereplikasi halaman Web-nya (Bab 2). Ini berarti bahwa server asal menganalisis jejak akses untuk catatan data yang kemudian dijadikan dasar keputusannya untuk menempatkan catatan.

Ingatlah bahwa di Globule, pengambilan keputusan didorong dengan memperhitungkan biaya untuk melaksanakan operasi baca dan perbarui begitu data ada (dan mungkin direplikasi). Biaya dinyatakan dalam fungsi linier sederhana.

Alternatif untuk replikasi parsial adalah dengan menggunakan cache yang sadar konten. Ide dasar dalam kasus ini adalah bahwa server tepi memelihara database lokal yang sekarang disesuaikan dengan jenis kueri yang dapat ditangani di server asal.

Untuk menjelaskan, dalam sistem database lengkap, kueri akan beroperasi pada database di mana datanya telah diatur ke dalam tabel sehingga, misalnya, redundansi diminimalkan. Database semacam itu juga dikatakan telah

dinormalisasi. Dalam database seperti itu, kueri apa pun yang mengikuti skema data dapat diproses; meskipun, mungkin dengan biaya yang cukup besar.

Dengan cache yang peka konten, server edge mempertahankan database yang diatur sesuai dengan struktur kueri. Artinya, kueri diasumsikan mengikuti sejumlah templat yang terbatas, yang secara efektif berarti bahwa berbagai jenis kueri yang dapat diproses dibatasi. Dalam kasus ini, setiap kali kueri diterima, server edge mencocokkan kueri dengan templat yang tersedia, dan kemudian mencari di database lokalnya untuk membuat respons, jika memungkinkan. Jika data yang diminta tidak tersedia, kueri diteruskan ke server asal setelah respons di-cache sebelum mengembalikannya ke klien.

Akibatnya, apa yang dilakukan server tepi adalah memeriksa apakah kueri dapat dijawab dengan data yang disimpan secara lokal. Ini juga disebut sebagai pemeriksaan penahanan kueri.

C. Latihan

1. Jelaskan fungsi Replication of Web Applications
2. Jelaskan Fungsi komunikasi dalam jaringan web terdistribusi

D. Kunci Jawaban

1. Jawaban latihan soal ke-1

   Pertama, untuk meningkatkan kinerja, menerapkan replikasi penuh dari data yang disimpan di server asal. ketika kueri memerlukan pencarian database yang ekstensif.

   Kasus kedua untuk replikasi penuh adalah ketika kueri umumnya kompleks. Dalam kasus database relasional, ini berarti bahwa kueri memerlukan beberapa tabel untuk dicari dan diproses, seperti yang umumnya terjadi pada operasi gabungan.

2. Jawaban latihan soal ke-2

Sebagai media dalam lalu lintas data melaluin jaringan computer, tata bisa berupa pesan, dokumen, gambar, film dan sebagainya

E. Daftar Pustaka

1. Couloris et. al. 2012. Distributed Systems Concepts and Design, Fifth Edition. Addison Wesley.
2. Van Steen and Tanenbaum, 2017. Distributed Systems: Prinsiples and Paradigms. 3e. Prentice-Hall

Link Juornal :

https://scholar.google.com/citations?user=TvjaNqkAAAAJ&hl=en

https://ieeexplore.ieee.org/abstract/document/749137

MODUL PEMROSESAN DATA TERSEBAR

(FTI-611)

MODUL SESI 14

DISTRIBUTED COORDINATOR BASED SYSTEM

DISUSUN OLEH

HERMANSYAH S.Kom., M.Kom.

UNIVERSITAS ESA UNGGUL

2020

KOORDINASI TERDISTRIBUSI

A. Kemampuan Akhir Yang Diharapkan

Setelah mempelajari modul ini, diharapkan mahasiswa mampu :

1. Mahasiswa dapat memahami mekanisme koordinasi dan mengimplementasikan sistem DDP ke dalam kasus nyata
2. Mampu mengimplementasikan berbagai sistem DDP pada kasus nyata

B. Uraian dan Contoh

1. Koordidasi Terdistribusi

Distributed Coordinator Based System

Koordinasi Terdistribusi

Sistem terdistribusi adalah suatu kesatuan dari elemen-elemen yang saling berinteraksi secara sistematis dan teratur untuk mendistribusikan data, informasi, obyek dan layanan dari dan kepada pengguna yang terkait didalamnya dengan melakukan pengiriman pesan (message passing). Agar tidak terjadi konflik saat mendistribusikan data, maka diperlukan sinkronisasi dan koordinasi antar komputer. Dalam sistem terdistribusi berbasis koordinasi, fokusnya adalah pada bagaimana koordinasi antara proses berlangsung. Jika ada lebih dari satu proses yang siap running, maka Sistem Operasi akan menentukan salah satu proses untuk running lebih dulu.

Aktivitas Koordinasi Terdistribusi

1. Pengurutan Event
   - Memori & clock tdk tunggal

   Tidak mungkin menyatakan urutan dua kejadian Hanya dapat ditentukan partial ordering (pengurutan sebagian) relasi Happened-Before (Hukum sebab-akibat : suatu pesan dapat diterima setelah pesan tersebut dikirim.

Jika A dan B adalah event pada proses yg sama, dan A dieksekusi sebelum B, maka A → B)

2. Mutual Exclusion

Pendekatan Tersentralisasi (Centralized) Salah satu proses dipilih sebagai koordinator utk mengatur entri ke Client - Server

- Menggunakan pesan request-reply-release untuk masuk ke Client Server
- (+): menjamin mutual exclusion, dpt menjamin fairness (no starvation)
- (--): jika koordinator gagal → perlu dipilih kembali

Pendekatan Terdistribusi Penuh (Fully Distributed)

- Untuk masuk ke Client Server, proses mengirimkan pesan request (Pi, TS) ke semua proses
  - Pengiriman reply oleh Pi ke Pk :
  - Jika Pi sedang berada di CS, reply ke Pk ditunda
  - Jika Pi tidak akan masuk ke CS, reply langsung dikirim ke Pk
  - Jika Pi akan masuk ke CS dan TS(Pi) < TS(Pk) maka reply ke Pk ditunda
  - (+): menjamin mutex, bebas deadlock dan starvation
  - (--): jumlah pesan minimum 2(n-1), proses harus tahu identitas semua proses lain, tidak berfungsi jika ada proses yg gagal, mengganggu proses lain yg tidak akan masuk ke CS

Pendekatan Token Passing

- Menggunakan satu token yg beredar diantara proses
- Hanya proses yg memiliki token saat itu yg dapat masuk ke CS
- Syarat: adanya lingkaran lojik yg menghubungkan semua proses

(+): menjamin mutex, bebas starvation

(--): jika token gagal → perlu digenerate kembali, jika proses gagal → perlu dibentuk ring lojik baru

3. Atomisitas

• Tiap situs memiliki koordinator transaksi yg berfungsi menjamin atomisitas eksekusi transaksi, dengan cara:

– memulai eksekusi transaksi

– memecah menjadi beberapa sub-transaksi dan mendistribusikannya pada situs-situs yg cocok utk dieksekusi

– mengkoordinasikan terminasi transaksi (commit, atau abort)

• Tiap situs menyimpan log untuk tujuan recovery

Protokol Two-Phase Commit (2PC)

• Semua situs yg mengeksekusi transaksi T harus memiliki hasil akhir yg sama (commit atau abort)

• JikaT adalah transaksi yg diinisiasi pada situs Si dengan koordinator Ci , maka setelah transaksi selesai Ci memulai protokol 2PC:

– Fase1: Ci mengirimkan pesan ke semua situs yg mengeksekusi T untuk mengetahui transaksi commit atau abort

– Fase2: Ci menentukan hasil akhir transaksi setelah menerima respon dari semua situs; transaksi commit jika semua situs memberi respon commit

Penanganan Kegagalan pada 2 PC

• Kegagalan pada salah satu situs yg berpartisipasi

– Masalah: situs yg selesai melakukan recovery harus memeriksa log untuk menentukan status transaksi

– Jika commit, situs melakukan redo(T)

– Jika abort, situs melakukan undo(T)

• Kegagalan pada coordinator

– Masalah: situs yg berpartisipasi harus menentukan nasib T

– Jika salah satu situs berisi record atau , maka coordinator akan mengikuti hasilnya

– Jika ada situs yg belum berisi maka koordinator tidak dapat memutuskan

• Kegagalan pada jaringan

– Masalah: pesan yg dikirimkan tidak sampai

– Jika beberapa link terputus dapat dilakukan partisi jaringan

• Pendekatan Koordinator Tunggal

– Ada manajer lock tunggal yg berada pada salah satu situs utk menangani permintaan lock/unlock data

– Read dapat dilakukan pada situs mana saja yg menyimpan data

– Write dilakukan pada semua replikasi

• Protokol Mayoritas

– Tiap situs memiliki lock manajer yg mengelola data dan duplikat data yg disimpan pd situs tersebut.

– Untuk melakukan lock terhdap data Q yg direplikasi pada beberapa situs, transaksi mengirim request lock ke > ½ situs yg menyimpan Q

- Lock manajer menentukan lock yg dapat diberikan

- Transaksi thd data tdk dimulai sebelum kunci dari mayoritas replika diperoleh

– (+): penanganan terdesentralisasi

– (--): penanganan deadlock perlu modifikasi, rumit

Uraian sub topik ke-1

2. Time and Coordination Pada Sistem Terdistribusi

1. Logical Clock

Logical clock adalah software counter yang bertambah secara monoton dimana nilainya tidak perlu menanggung hubungan tertentu ke suatu physical clock.

Hampir seluruh komputer memiliki sebuah circuit untuk menunjukkan waktu. Pada kenyataannya circuit tersebut bukanlah penunjuk waktu (jam) yang sebenarnya. Kata yang tepat untuk mendeskripsikan circuit tersebut adalah timer. Timer pada suatu komputer pada umumnya merupakan suatu

crystal quartz yang termekanisasi. Jika dihadapkan pada suatu tekanan, kristal tersebut akan berosilasi pada frekuensi tertentu bergantung pada jenis kristal dan bagaimana kristal tersebut dipotong serta seberapa besar tekanan yang diberikan. Terdapat 2 register yang berasosiasi dengan kristal tersebut. Sebuah counter dan holding register. Setiap interript akan diregenerasi dan counter akan kembali terisi oleh nilai yang terdapat pada holding register. Dengan begini sangat memungkinkan untuk memrogram sebuah timer untuk meregenerasi 60 interrupt tiap detiknya atau sesuai dengan frekuensi yang diinginkan. Setiap interrupt disebut dengan satu clock tick.

Synchronisation

Sinkronisasi adalah proses pengaturan jalannya beberapa proses pada saat yang bersamaan. Secara garis besar mungkin sinkronisasi adalah menyamakan sesuatu secara bersamaan. Sinkronisasi adalah suatu proses pengendalian akses dari sumber daya terbagi pakai (shared resource) oleh banyak thread sedemikian sehingga hanya satu thread yang dapat mengakses sumber daya tertentu pada satu waktu.

Proses Koordinasi pada sistem Terdistribusi

Sistem tedistribusi memungkinkan kita untuk saling mengkoordinasikan dan saling bekerja sama dalam melakukan aktifitas secara lebih efisien dan lebih efektif. Tujuan utama dari system terdistribusi dapat direpresentasikan dengan : resource sharing , openness, concurrency, scalability, fault-tolerance dan transparency.

Proses koordinasi nya

- Dijalankan secara bersamaan (execute concurrently)
- Interaksi untuk bekerjasama dalam mencapai tujuan yang sama
- Mengkoordinasikan aktifitas dan pertukaran informasi yaitu pesan yang dikirim melalui jaringan komunikasi

Jika kita melihat sistem terdistribusi sebagaikoleksi (mungkin proses multithreaded, maka bagian komputasi dari sistem terdistribusi dibentuk oleh proses, masing-masing terkait dengan aktivitas komputasi spesifik,

yang pada prinsipnya, dilakukan secara independen dari kegiatan lainnya proses. Dalam model ini, bagian koordinasi sistem terdistribusi menangani komunikasi kerjasama antara proses. Membentuk perekat yang mengikat kegiatan yang dilakukan oleh proses menjadi keseluruhan.

1. Perbedaan Model Sinkronisasi dan Asinkronisasi

Sistem basis data terdistribusi dapat menyimpan duplikat dari data yang sama dalam site yang berbeda agar perolehan informasi yang semakin cepat dan toleransi kesalahan. Proses ini disebut replikasi. Replikasi pada relasi bersifat redundan pada dua atau lebih situs. Replikasi pada relasi disebut replikasi penuh bila relasi tersebut disimpan pada semua situs. Basis data disebut redundan penuh jika tiap-tiap site mengandung duplikat dari keseluruhan basis data.

Replikasi dilakukan karena memiliki kelebihan sebagai berikut:

•jika situs asli yang menyimpan relasi R mengalami kegagalan, relasi R tetap dapat diakses melalui replikanya

•query pada relasi R dapat berjalan secara paralel di simpul (situs) yang berbeda

•lebih sedikit transfer data, yaitu tidak perlu lagi mengambil data suatu relasi melalui jaringan karena sudah ada replika dalam situs lokal.

Sementara itu, dalam melakukan replikasi, ada dua strategi, yaitu

o Sinkron yaitu: sebelum seluruh proses transaksi update dinyatakan selesai, data yang telah dimodifikasi disinkronkan ke setiap duplikatnya; proses ini harus menunggu hingga data di tempat penyimpanan duplikat selesai ditulis sebelum dilakukan perubahan lainnya sehingga menjadi lebih kompleks

o Asinkron yaitu: copy data diperbaharui secara periodik berdasarkan data utama yang diperbaharui; proses penulisan data selesai tanpa perlu menunggu penulisan data di tempat penyimpanan duplikat selesai; proses ini memang meningkatkan kinerja sistem namun risikonya, inkonsistensi data bisa terjadi.

2. Pembahasan tentang bagaimana server mengelola Share Data

3. Konsep dan operasi Shared Data antara server dan client

Dalam sistem terdistribusi, beberapa komputer yang berbeda saling terhubung satu sama lain melalui jaringan sehingga komputer yang satu dapat mengakses dan menggunakan sumber daya yang terdapat dalam situs lain. Misalnya, user di komputer A dapat menggunakan laser printer yang dimiliki komputer B dan sebaliknya user di situs B dapat mengakses file yang terdapat di komputer A.

2. Konsep Sharing Client – Server

Jaringan client atau server adalah jaringan dimana komputer client bertugas melakukan permintaan data dan server bertugas melayani permintaan tersebut.

Client

- User akan membuat permintaan melalui software client. Aplikasi ini berfungsi :
- Memberikan interface bagi user untuk melakukan jobs.
- Format request data ke bentuk yang dapat dimengerti oleh server
- Menampilkan hasil yang diminta pada layar

Server

Jaringan client atau server, server khusus digunakan untuk pemrosesan, penyimpanan dan manajemen data. Server bertugas menerima request dari client, mengolahnya, dan mengirimkan kembali hasilnya ke client.

Untuk itu, server membutuhkan komputer khusus dengan spesifikasi hardware yang jauh lebih baik dan bertenaga dibandingkan hardware untuk client karena komputer harus mampu melayani :

- Request secara simultan dalam jumlah besar
- Aktivitas manajemen jaringan
- Menjamin keamanan pada resource jaringan

3. Proses Layanan pada Saat Terjadi Crash atau Fault Tolerance & Data Transaction dan Urutan Operasi yang Dijalani Oleh Server

Sebuah kecelakaan (atau sistem crash) dalam komputasi adalah suatu kondisi di mana sebuah komputer atau program, baik aplikasi atau bagian dari sistem operasi, berhenti berfungsi dengan baik, sering keluar setelah menghadapi kesalahan. Seringkali program menyinggung mungkin muncul untuk membekukan atau hang sampai layanan pelaporan kecelakaan dokumen rincian kecelakaan itu. Jika program adalah bagian penting dari kernel sistem operasi, seluruh komputer dapat kecelakaan. Hal ini berbeda dari hang atau membekukan dimana aplikasi atau OS terus berjalan tanpa respon jelas untuk masukan.

Banyak crash adalah hasil dari eksekusi instruksi mesin tunggal, tetapi penyebab ini berlipat ganda. Penyebab khas adalah ketika program counter diatur ke alamat yang salah atau buffer overflow menimpa sebagian kode program karena bug sebelumnya. Dalam kedua kasus, itu cukup umum untuk prosesor untuk mencoba untuk mengeksekusi data atau nilai memori acak. Karena semua nilai data adalah mungkin tetapi hanya beberapa nilai instruksi valid, ini sering mengakibatkan pengecualian instruksi ilegal.

4. Konsep Dasar Replication

Replikasi adalah suatu teknik untuk melakukan copy dan pendistribusian data dan objek-objek database dari satu database ke database lain dan melaksanakan sinkronisasi antara database sehingga konsistensi data dapat terjamin. Dengan menggunakan teknik replikasi ini, data dapat didistribusikan ke lokasi yang berbeda melalui koneksi jaringan lokal maupun internet. Replikasi juga memungkinkan untuk mendukung kinerja aplikasi, penyebaran data fisik sesuai dengan penggunaannya, seperti pemrosesan transaksi online dan DSS (Desiscion Support System) atau pemrosesan database terdistribusi melalui beberapa server.

Uraian sub topik ke-2

C. Latihan

a. Jelaskan Apa yang dimaksud koordinasi terdistribusi..?
b. Jelaskan Perbedaan Layanan Syncronization dan Asyncronisation…….?

c. Jelaskan konsep dasar Replication….?

D. Kunci Jawaban

a. Jawaban latihan soal ke-1

b. Jawaban latihan soal ke-2

Dalam melakukan replikasi, ada dua strategi, yaitu

- **Sinkron** yaitu: sebelum seluruh proses transaksi update dinyatakan selesai, data yang telah dimodifikasi disinkronkan ke setiap duplikatnya; proses ini harus menunggu hingga data di tempat penyimpanan duplikat selesai ditulis sebelum dilakukan perubahan lainnya sehingga menjadi lebih kompleks
- **Asinkron** yaitu: copy data diperbaharui secara periodik berdasarkan data utama yang diperbaharui; proses penulisan data selesai tanpa perlu menunggu penulisan data di tempat penyimpanan duplikat selesai; proses ini memang meningkatkan kinerja sistem namun risikonya, inkonsistensi data bisa terjadi.

c. Jawaban latihan soal ke-3

Replikasi adalah suatu teknik untuk melakukan copy dan pendistribusian data dan objek-objek database dari satu database ke database lain dan melaksanakan sinkronisasi antara database sehingga konsistensi data dapat terjamin.

A. Kemampuan Akhir Yang Diharapkan

Setelah mempelajari modul ini, diharapkan mahasiswa mampu :

1. Memahami dan mengerti pengaturan lalu lintas Jaringan.
2. Memahami dan mengerti perbedaan jaringan Syncronus dan asynchronous.

B. Uraian dan Contoh

1. Perbedaan Logical Clock dan Sychronisatin

Pengetahuan Logical Clock & Synchronisation

1. Logical Clock

Logical clock adalah software counter yang bertambah secara monoton dimana nilainya tidak perlu menanggung hubungan tertentu ke suatu physical clock.

Hampir seluruh komputer memiliki sebuah circuit untuk menunjukkan waktu. Pada kenyataannya circuit tersebut bukanlah penunjuk waktu (jam) yang sebenarnya. Kata yang tepat untuk mendeskripsikan circuit tersebut adalah timer. Timer pada suatu komputer pada umumnya merupakan suatu crystal quartz yang termekanisasi. Jika dihadapkan pada suatu tekanan, kristal tersebut akan berosilasi pada frekuensi tertentu bergantung pada jenis kristal dan bagaimana kristal tersebut dipotong serta seberapa besar tekanan yang diberikan. Terdapat 2 register yang berasosiasi dengan kristal tersebut. Sebuah counter dan holding register. Setiap interript akan diregenerasi dan counter akan kembali terisi oleh nilai yang terdapat pada holding register. Dengan begini sangat memungkinkan untuk memrogram sebuah timer untuk meregenerasi 60 interrupt tiap detiknya atau sesuai dengan frekuensi yang diinginkan. Setiap interrupt disebut dengan satu clock tick.

Synchronisation

Sinkronisasi adalah proses pengaturan jalannya beberapa proses pada saat yang bersamaan. Secara garis besar mungkin sinkronisasi adalah menyamakan sesuatu secara bersamaan. Sinkronisasi adalah suatu proses pengendalian akses dari sumber daya terbagi pakai (shared resource) oleh banyak thread sedemikian sehingga hanya satu thread yang dapat mengakses sumber daya tertentu pada satu waktu.

Proses Koordinasi pada sistem Terdistribusi

Sistem tedistribusi memungkinkan kita untuk saling mengkoordinasikan dan saling bekerja sama dalam melakukan aktifitas secara lebih efisien dan lebih efektif. Tujuan utama dari system terdistribusi dapat direpresentasikan dengan : resource sharing , openness, concurrency, scalability, fault-tolerance dan transparency.

Proses koordinasi nya

- Dijalankan secara bersamaan (execute concurrently)
- Interaksi untuk bekerjasama dalam mencapai tujuan yang sama
- Mengkoordinasikan aktifitas dan pertukaran informasi yaitu pesan yang dikirim melalui jaringan komunikasi

Jika kita melihat sistem terdistribusi sebagaikoleksi (mungkin proses multithreaded, maka bagian komputasi dari sistem terdistribusi dibentuk oleh proses, masing-masing terkait dengan aktivitas komputasi spesifik, yang pada prinsipnya, dilakukan secara independen dari kegiatan lainnya proses. Dalam model ini, bagian koordinasi sistem terdistribusi menangani komunikasi kerjasama antara proses. Membentuk perekat yang mengikat kegiatan yang dilakukan oleh proses menjadi keseluruhan.

1. Perbedaan Model Sinkronisasi dan Asinkronisasi

Sistem basis data terdistribusi dapat menyimpan duplikat dari data yang sama dalam site yang berbeda agar perolehan informasi yang semakin cepat dan toleransi kesalahan. Proses ini disebut replikasi. Replikasi pada relasi bersifat redundan pada dua atau lebih situs. Replikasi pada relasi disebut replikasi penuh bila relasi tersebut disimpan pada semua situs. Basis data disebut redundan penuh jika tiap-tiap site mengandung duplikat dari keseluruhan basis data.

Replikasi dilakukan karena memiliki kelebihan sebagai berikut:

•jika situs asli yang menyimpan relasi R mengalami kegagalan, relasi R tetap dapat diakses melalui replikanya

•query pada relasi R dapat berjalan secara paralel di simpul (situs) yang berbeda

•lebih sedikit transfer data, yaitu tidak perlu lagi mengambil data suatu relasi melalui jaringan karena sudah ada replika dalam situs lokal.

Sementara itu, dalam melakukan replikasi, ada dua strategi, yaitu

o Sinkron yaitu: sebelum seluruh proses transaksi update dinyatakan selesai, data yang telah dimodifikasi disinkronkan ke setiap duplikatnya; proses ini harus menunggu hingga data di tempat penyimpanan duplikat selesai ditulis sebelum dilakukan perubahan lainnya sehingga menjadi lebih kompleks

o Asinkron yaitu: copy data diperbaharui secara periodik berdasarkan data utama yang diperbaharui; proses penulisan data selesai tanpa perlu menunggu penulisan data di tempat penyimpanan duplikat selesai; proses ini memang meningkatkan kinerja sistem namun risikonya, inkonsistensi data bisa terjadi.

2. Pembahasan tentang bagaimana server mengelola Share Data

3. Konsep dan operasi Shared Data antara server dan client

Dalam sistem terdistribusi, beberapa komputer yang berbeda saling terhubung satu sama lain melalui jaringan sehingga komputer yang satu dapat mengakses dan menggunakan sumber daya yang terdapat dalam situs lain. Misalnya, user di komputer A dapat menggunakan laser printer yang dimiliki komputer B dan sebaliknya user di situs B dapat mengakses file yang terdapat di komputer A.

2. Konsep Sharing Client – Server

Jaringan client atau server adalah jaringan dimana komputer client bertugas melakukan permintaan data dan server bertugas melayani permintaan tersebut.

Client

- User akan membuat permintaan melalui software client. Aplikasi ini berfungsi :
- Memberikan interface bagi user untuk melakukan jobs.
- Format request data ke bentuk yang dapat dimengerti oleh server
- Menampilkan hasil yang diminta pada layar

Server

Jaringan client atau server, server khusus digunakan untuk pemrosesan, penyimpanan dan manajemen data. Server bertugas menerima request dari client, mengolahnya, dan mengirimkan kembali hasilnya ke client.

Untuk itu, server membutuhkan komputer khusus dengan spesifikasi hardware yang jauh lebih baik dan bertenaga dibandingkan hardware untuk client karena komputer harus mampu melayani :

- Request secara simultan dalam jumlah besar
- Aktivitas manajemen jaringan
- Menjamin keamanan pada resource jaringan

3. Proses Layanan pada Saat Terjadi Crash atau Fault Tolerance & Data Transaction dan Urutan Operasi yang Dijalani Oleh Server

Sebuah kecelakaan (atau sistem crash) dalam komputasi adalah suatu kondisi di mana sebuah komputer atau program, baik aplikasi atau bagian dari sistem operasi, berhenti berfungsi dengan baik, sering keluar setelah menghadapi kesalahan. Seringkali program menyinggung mungkin muncul untuk membekukan atau hang sampai layanan pelaporan kecelakaan dokumen rincian kecelakaan itu. Jika program adalah bagian penting dari kernel sistem operasi, seluruh komputer dapat kecelakaan. Hal ini berbeda dari hang atau membekukan dimana aplikasi atau OS terus berjalan tanpa respon jelas untuk masukan.

Banyak crash adalah hasil dari eksekusi instruksi mesin tunggal, tetapi penyebab ini berlipat ganda. Penyebab khas adalah ketika program counter diatur ke alamat yang salah atau buffer overflow menimpa sebagian kode program karena bug sebelumnya. Dalam kedua kasus, itu cukup umum

untuk prosesor untuk mencoba untuk mengeksekusi data atau nilai memori acak. Karena semua nilai data adalah mungkin tetapi hanya beberapa nilai instruksi valid, ini sering mengakibatkan pengecualian instruksi ilegal.

4. Konsep Dasar Replication

Replikasi adalah suatu teknik untuk melakukan copy dan pendistribusian data dan objek-objek database dari satu database ke database lain dan melaksanakan sinkronisasi antara database sehingga konsistensi data dapat terjamin. Dengan menggunakan teknik replikasi ini, data dapat didistribusikan ke lokasi yang berbeda melalui koneksi jaringan lokal maupun internet. Replikasi juga memungkinkan untuk mendukung kinerja aplikasi, penyebaran data fisik sesuai dengan penggunaannya, seperti pemrosesan transaksi online dan DSS (Desiscion Support System) atau pemrosessan database terdistribusi melalui beberapa server.

1. Time And Coordinaton

Time and Coordination adalah mengkordinasikan waktu dalam transfer data, agar tidak terjadi ketimpangan pada proses transfer data. Selain itu juga, berguna untuk mengukur penundaan antara komponen terdistribusi, menyinkronkan aliran data misalnya: suara dan video, dan sebagai penanda keakuratan waktu untuk mengidentifikasi atau mengotentikasi transaksi bisnis dan serializability dalam database terdistribusi dan keamanan protocol.

1.1 Time

Time adalah pengembangan dari sistem multiprogram.Beberapa job yang berada pada memory utama dieksekusi oleh CPU secara bergantian.CPU hanya bisa menjalankan program yang berada pada memory utama. Perpindahanantar job terjadi sangat sering sehingga user dapat berinteraksi dengan setiap programpada saat dijalankan. Suatu job akan dipindahkan dari memori ke disk dan sebaliknya.

Time juga disebut dengan sistem komputasi interaktif, dimanasistem komputer menyediakan komunikasi on-line antara user dengan sistem. Usermemberikan instruksi pada sistem operasi atau program secara langsung dan menerimarespon segera. Perangkat input berupa keyboard dan perangkat output berupa displayscreen, seperti cathode-ray tube (CRT) atau monitor. Bila sistem operasi selesaimengeksekusi satu perintah, makan sistem akan mencari pernyataan berikutnya dariuser melalui keyboard. Sistem menyediakan editor interaktif untuk menulis programdan sistem debug untuk membantu melakukan debugging program.

Uraian sub topik ke-1

2. Coordination

1.2 Coordination

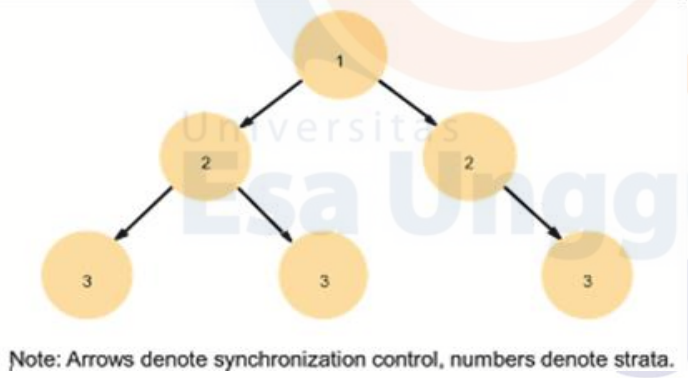
Coordnaion adalah Sekumpulan algoritma yang tujuannya bermacam-macam namun men-share tujuannya, sebagai dasar dalam sistem terdistribusi : berupa sekumpulan proses untuk mengkoordinasikan tindakan atau menyetujui satu atau beberapa nilai. Contohnya pada kasus mesin seperti pesawat ruang angkasa. Hal itu perlu dilakukan, komputer mengendalikannya agar setuju pada kondisi tertentu seperti apakah misi dari pesawat luar angkasa dilanjutkan atau telah selesai. Komputer tersebut harus mengkoordinasikan tindakannya secara tepat untuk berbagi hal yang penting dalam Coordination and Agreement adalah apakah system terdistribusi asinkron atau sinkron. Algoritma –algoritma yang digunakan juga harus mempertimbangkan kegagalan yang terjadi, dan bagaimana caranya untuk berhubungan satu sama lain ketika sedang mendesaian algoritma. Selanjutnya di makalah ini juga akan dijelaskan mengenai masalah dalam mendistribusikan mutual exclusion, election, multicast communication, dan mengenai masalah dalam persetujuan(agreement).

1.3 Contoh Time And Coordination Protokol Waktu Jaringan (Network Time Protocol)

Metode Cristian dan algoritma Berkeley pada dasarnya digunakan untuk komunikasi intranet. Protokol Waktu Jaringan (NTP) mendefinisikan arsitektur untuk pelayanan waktu dan protocol untuk distribusi informasi waktu lewat internet.

Tujuan dan fitur NTP, antara lain:

- To provide a service enabling clients across the Internet to be synchronized accurately to UTC: NTP menyediakan layanan agar klien di internet dapat bersinkronisasi dengan UTC.
- To provide a reliable service that can survive lengthy losses of connectivity: NTP menyediakan layanan yang bisa bertahan di jaringan mengalami loss karena jarak.
- To enable clients to resynchronize sufficiently frequently to offset the rates of drift found in most computers: NTP memungkinkan klien untuk sinkronisasi ulang secara berkala.
- To provide protection against interference with the time service, whether malicious or accidental: NTP menyediakan perlindungan terhadap interferensi dari layanan waktu, baik galat maupun ketidaksengajaan.



Gambar 1. Contoh sinkronisasi subnet di NTP

Layanan NTP tersebar pada banyak server di internet. Server utama tersambung langsung ke sumber waktu, seperti penerima sinyal radio UTC. Server sekunder disinkronisasi dengan server primer. Server-servernya tersambung dalam hierarkikal logika yang disebut synchronization subnet seperti Gambar 3. Semakin atas levelnya akan semakin akurat clock-nya. Galat terjadi setiap melewati satu level.

Server-server NTP bersinkronasi satu sama lain dengan tiga cara, antara lain multicast, procedure-call, dan symmetric.

1. Multicast

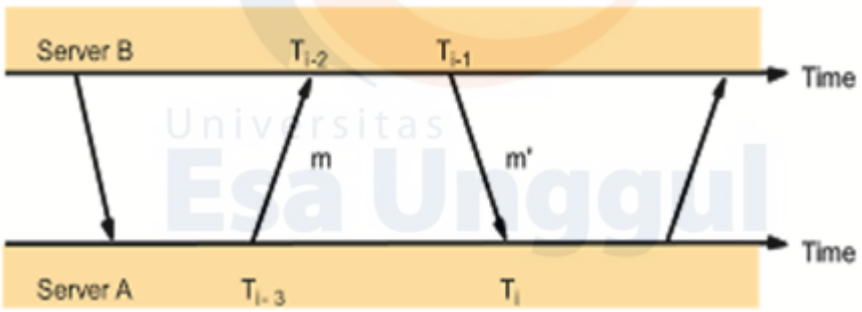
Multicast ditujukan untuk LAN berkecepatan tinggi. Satu atau lebih server secara periodik menyebar waktu clock ke server di komputer lain yang tersambung di LAN. Mode ini akurasinya rendah tetapi cocok untuk berbagai kepentingan.

2. Procedure-call

Procedure-call hamper sama dengan algoritma Cristian. Server menerima request dari komputer lain dan membalasnya dengan pembacaan clock saat pengiriman. Mode ini cocok ketika keakurasian tinggi dibutuhkan atau ketika multicast tidak dappat dilakukan.

3. Symmetric

Mode symmetric ditujukan untuk server yang mensuplai waktu dalam LAN atau pada level tertinggi dari sebuah synchronization subnet.



Gambar 2. Message Exchange between a pair NTP peers

Pada mode procedure-call dan symmetric mode, memroses pertukaran bagian-bagian pesan. Tiap pesan memiliki catatan waktu dari peristiwa yang baru saja terjadi, yaitu waktu local ketika pesan tersebut dikirimkan. Seperti pada Gambar 3, pesan m menyimpan catatan waktu setiap akan ditransmisikan, yaitu Ti-3 dan Ti-1, dan ketika diterima, yaitu Ti-2 dan Ti. Kemudian NTP menghitung jeda waktu antara dua clock komputer.

2. Share Data

2.1. Konsep dan operasi Shared Data antara server dan client

Dalam sistem terdistribusi, beberapa komputer yang berbeda saling terhubung satu sama lain melalui jaringan sehingga komputer yang satu dapat mengakses dan menggunakan sumber daya yang terdapat dalam situs lain. Misalnya, user di komputer A dapat menggunakan laser printer yang dimiliki komputer B dan sebaliknya user di situs B dapat mengakses file yang terdapat di komputerA.

Konsep Sharing Client – Server

Jaringan client atau server adalah jaringan dimana komputer client bertugas melakukan permintaan data dan server bertugas melayani permintaan tersebut.

Client

Ø User akan membuat permintaan melalui software client. Aplikasi ini berfungsi :

Ø Memberikan interface bagi user untuk melakukan jobs.

Ø Format request data ke bentuk yang dapat dimengerti oleh server

Ø Menampilkan hasil yang diminta pada layar Server

Jaringan client atau server, server khusus digunakan untuk pemrosesan, penyimpanan dan manajemen data. Server bertugas menerima request dari client, mengolahnya, dan mengirimkan kembali hasilnya ke client.

Untuk itu, server membutuhkan komputer khusus dengan spesifikasi hardware yang jauh lebih baik dan bertenaga dibandingkan hardware untuk client karena komputer harus mampu melayani :

Ø Request secara simultan dalam jumlah besar

Ø Aktivitas manajemen jaringan

Ø Menjamin keamanan pada resource jaringan

2.2 Proses Layanan pada Saat Terjadi Crash atau Fault Tolerance & Data Transaction dan Urutan Operasi yang Dijalani Oleh Server

Sebuah kecelakaan (atau sistem crash) dalam komputasi adalah suatu kondisi di mana sebuah komputer atau program, baik aplikasi atau bagian dari sistem operasi, berhenti berfungsi dengan baik, sering keluar setelah menghadapi kesalahan. Seringkali program menyinggung mungkin muncul untuk membekukan atau hang sampai layanan pelaporan kecelakaan dokumen rincian kecelakaan itu. Jika program adalah bagian penting dari kernel sistem operasi, seluruh komputer dapat kecelakaan. Hal ini berbeda dari hang atau membekukan dimana aplikasi atau OS terus berjalan tanpa respon jelas untuk masukan.

Banyak crash adalah hasil dari eksekusi instruksi mesin tunggal, tetapi penyebab ini berlipat ganda. Penyebab khas adalah ketika program counter diatur ke alamat yang salah atau buffer overflow menimpa sebagian kode program karena bug sebelumnya. Dalam kedua kasus, itu cukup umum untuk prosesor untuk mencoba untuk mengeksekusi data atau nilai memori acak. Karena semua nilai data adalah mungkin tetapi hanya beberapa nilai instruksi valid, ini sering mengakibatkan pengecualian instruksi ilegal.

2.3. Konsep Dasar Replication

Replikasi adalah suatu teknik untuk melakukan copy dan pendistribusian data dan objek-objek database dari satu database ke database lain dan melaksanakan sinkronisasi antara database sehingga konsistensi data dapat terjamin. Dengan menggunakan teknik replikasi ini, data dapat didistribusikan ke lokasi yang berbeda melalui koneksi jaringan lokal maupun internet. Replikasi juga memungkinkan untuk mendukung kinerja aplikasi, penyebaran data fisik sesuai dengan penggunaannya, seperti pemrosesan transaksi online dan DSS (Desiscion Support System) atau pemrosessan database terdistribusi melalui beberapa server.

Replikasi adalah proses menyalin dan memelihara objek database dalam beberapa database yang membentuk suatu sistem database terdistribusi. Replikasi dapat meningkatkan kinerja dan melindungi ketersediaan aplikasi karena data pilihan alternatif akses ada. Sebagai contoh, sebuah aplikasi biasanya dapat mengakses database lokal daripada server jauh untuk meminimalkan lalu lintas jaringan dan mencapai kinerja maksimum. Selanjutnya, aplikasi dapat terus berfungsi jika

server lokal mengalami kegagalan, tetapi server lain dengan data direplikasi tetap dapat diakses.Gambar 2. Message Exchange between a pair NTP peers

Pada mode procedure-call dan symmetric mode, memroses pertukaran bagian-bagian pesan. Tiap pesan memiliki catatan waktu dari peristiwa yang baru saja terjadi, yaitu waktu local ketika pesan tersebut dikirimkan. Seperti pada Gambar 3, pesan m menyimpan catatan waktu setiap akan ditransmisikan, yaitu Ti-3 dan Ti-1, dan ketika diterima, yaitu Ti-2 dan Ti. Kemudian NTP menghitung jeda waktu antara dua clock komputer.

Uraian sub topik ke-2

C. Latihan

1. Tujuan Utama dari System terdistribusi dan koordinasi adalah :
2. Jelaskan konsep kerja proses Client server untuk sisi Clientnya,,,?
3. Berikan Juga penjelasan tentang kerjanya server pada sistem client-server…?

D. Kunci Jawaban

1. Jawaban latihan soal ke-1

   Tujuan utama dari system terdistribusi dapat direpresentasikan dengan : resource sharing , openness, concurrency, scalability, fault-tolerance dan transparency.

   Proses koordinasi nya

   - Dijalankan secara bersamaan (execute concurrently)
   - Interaksi untuk bekerjasama dalam mencapai tujuan yang sama
   - Mengkoordinasikan aktifitas dan pertukaran informasi yaitu pesan yang dikirim melalui jaringan komunikasi

2. Jawaban latihan soal ke-2

   Client

- Ø User akan membuat permintaan melalui software client. Aplikasi ini berfungsi :
- Ø Memberikan interface bagi user untuk melakukan jobs.
- Ø Format request data ke bentuk yang dapat dimengerti oleh server
- Ø Menampilkan hasil yang diminta pada layar Server

3. Jawaban latihan soal ke-3

server membutuhkan komputer khusus dengan spesifikasi hardware yang jauh lebih baik dan bertenaga dibandingkan hardware untuk client karena komputer harus mampu melayani :

- Ø Request secara simultan dalam jumlah besar
- Ø Aktivitas manajemen jaringan
- Ø Menjamin keamanan pada resource jaringan

E. Daftar Pustaka

1. Couloris et. al. 2012. Distributed Systems Concepts and Design, Fifth Edition. Addison Wesley.
2. Van Steen and Tanenbaum, 2017. Distributed Systems: Prinsiples and Paradigms. 3e. Prentice-Hall

Link :

https://aditrisno.blogspot.com/2015/04/time-coordination-sistem-terdistribusi.html

https://komputasi.files.wordpress.com/2018/03/mvsteen-distributed-systems-3rd-preliminary-version-3-01pre-2017-170215.pdf

http://repository.fue.edu.eg/xmlui/handle/123456789/3526

Tugas OnLine pertemuan 11

Buatlah ringkasan tentang Distributed Object Based System mrnurut anda dan sebutkan contoh dari aplikasi tersebut dan berikan penjelasan dan cara kerjanya.

Tugas Online P ertemuan 12

Buatlah sebuah makalah makalah tentang Network File System (NFS), tentang cara kerjanya, attribute, jenis dan operasi yang dapat dilakukan terhadap file tersebut.

Tugas OnLine Pertemuan ke 13

Buatlah sebuah “WEB SITE” interactive tentang pemerintahan Daerah, misalnya pemerintahan daerah Kabupaten Mukomuko Provinsi Bengkulu, dimana web tersebut mentajikan Informasi Informasi aktivitas aktivitas pemerintahan daerah termasuk kegiatan Anggota DPRD dalam satu tahun anggaran. Catatan buat Web Site secara berkelompok dan bagi tugas masing masing dengan modul yang disesuaikan. Satu kelompok maksimum 4 orang.

‘

Tugas OnLine Pertemuan ke 14

nodifikasi web site Yang telah dibuat pada tugas 13 dengatr fitur tertentu termasuk security, database yang diperlukan serta interface lainnya, sehingga web site anda menjadi lebih menarik dan nteraktif dari sebelumnya.