



Institute of Technology of Cambodia  
Department of Information Technology  
and communication



## Distributed Systems

Group: C4

Name of students

1. Sean Reaksmeay
2. Nith Sothey
3. Pheng Menghour
4. Ret Sereymonny

ID of students

e20210686  
e20210601  
e20210737  
e20211460

Lecturer: Mr. Khem Thay

Academic Year 2024-2025

## TP4

1. Comparison – Centralized, Decentralized and Distributed systems
  - What are they?
  - Characteristics
  - Architecture
  - Advantages and disadvantages
  - Limitation
  - An example and explain
2. What problems do you foresee in the direct coupling between communicating entities that is implicit in remote invocation approaches? Consequently, what advantages do you anticipate from a level of decoupling as offered by space and time uncoupling?
3. Describe and illustrate the client-server architecture of one or more major Internet applications (for example the Web, email or netnews).
4. A search engine is a web server that responds to client requests to search in its stored indexes and (concurrently) runs several web crawler tasks to build and update the indexes. What are the requirements for synchronization between these concurrent activities?
5. The host computers used in peer-to-peer systems are often simply desktop computers in users' offices or homes. What are the implications of this for the availability and security of any shared data objects that they hold and to what extent can any weaknesses be overcome through the use of replication?
6. List the types of local resource that are vulnerable to an attack by an untrusted program that is downloaded from a remote site and run in a local computer.
7. Consider a simple server that carries out client requests without accessing other servers. Explain why it is generally not possible to set a limit on the time taken by such a server to respond to a client request. What would need to be done to make the server able to execute requests within a bounded time? Is this a practical option?
8. The Network Time Protocol service can be used to synchronize computer clocks. Explain why, even with this service, no guaranteed bound is given for the difference between two clocks.
9. Describe possible occurrences of each of the main types of security threat (threats to processes, threats to communication channels, denial of service) that might occur in the Internet.

## Answer

### 1. **Centralized Systems:**

- Definition: Centralized systems rely on a single, central server or a small group of central servers for processing and managing data and resources.
- Characteristics: Typically easier to manage, as all data and resources are located in a central location. This also makes it easier to enforce security policies.
- Architecture: Clients connect directly to a single central server for all resources and services.
- Advantages: Simplicity in design, easier to secure and maintain due to a single point of control.
- Disadvantages: Prone to single points of failure, meaning if the central server fails, the entire system could be inaccessible. Scalability can also be limited due to centralized resources.
- Limitations: Limited redundancy and resilience; the system is vulnerable to attacks targeting the central server.
- Example: Traditional client-server models like mainframe-based systems in banks or centralized databases.

### • **Decentralized Systems:**

- Definition: In decentralized systems, multiple independent nodes are involved, each potentially managing its own resources or clients, without a single central point of control.
- Characteristics: They distribute control across multiple nodes, reducing the dependency on any one server.
- Architecture: Comprises several interconnected nodes that may directly communicate without a central authority.
- Advantages: Improved resilience as failure in one node doesn't collapse the entire system.
- Disadvantages: Increased complexity in communication and coordination across nodes.
- Limitations: Requires advanced synchronization and may be slower due to the need for inter-node communication.
- Example: Some blockchain networks are decentralized as they have multiple nodes verifying transactions independently.

### • **Distributed Systems:**

- Definition: Distributed systems spread resources and tasks across multiple nodes that work together to function as a unified system.
- Characteristics: Nodes work collaboratively, often sharing tasks and data, with no central node.
- Architecture: Nodes can serve both as clients and servers; tasks and resources are distributed for resilience and efficiency.
- Advantages: High scalability and fault tolerance; if one node fails, others can continue to operate.
- Disadvantages: Complexity in design and data consistency issues due to distributed architecture.

- Limitations: Requires sophisticated mechanisms for data synchronization and fault tolerance.
  - Example: Large-scale systems like Google's data centers or distributed databases.
2. **Direct Coupling Issues:** In direct coupling, components are tightly bound, meaning that one component's failure directly impacts the other. This rigid structure limits flexibility, hampers scalability, and increases dependencies.
    - **Advantages of Decoupling (Space and Time):** Decoupling allows for asynchronous communication, where components do not have to interact in real-time or know each other's exact state. This flexibility enhances system fault tolerance and facilitates scaling, as components can operate independently.
  3. **Web Architecture:**
    - The web uses a client-server model, where browsers (clients) make requests to web servers for resources like HTML pages, images, or data.
    - HTTP (Hypertext Transfer Protocol) is the primary protocol, enabling communication between web clients and servers.
    - This model allows clients to perform read-only tasks (viewing pages) and interactive tasks (e.g., submitting forms), while the server handles session management, authentication, and database transactions.
    - **Email Architecture:**
      - Email also follows a client-server model, where email clients (like Outlook or Gmail) connect to email servers using protocols like IMAP, SMTP, and POP3.
      - Clients send email requests to an SMTP server, which routes the emails to the recipient's server.
      - The model provides asynchronous communication, where messages are queued and stored on the server for clients to retrieve at their convenience.
  4. Synchronization in Search Engines:
    - **Requirements:** Search engines have concurrent tasks: handling client search requests while updating their indexes through web crawlers.
    - **Synchronization Mechanism:** To prevent data inconsistency, search engines use techniques like locking or concurrency control. For example, index updates by web crawlers can be temporarily halted or queued when a search request needs to access the same data.
  5. Peer-to-Peer Systems and Implications on Availability and Security:
    - **Availability:** Desktop computers in peer-to-peer (P2P) systems often go offline or have power and resource limitations, making data availability unpredictable.
    - **Security:** Since desktop systems lack robust security measures, data on them is more vulnerable to unauthorized access.
    - **Replication for Overcoming Issues:** Replication distributes copies of data across multiple nodes, enhancing availability and resilience against node failures or malicious attacks.

6. Local Resources Vulnerable to Untrusted Programs:
  - **File System:** Untrusted programs can access or modify files, potentially causing data corruption.
  - **Network Interfaces:** Programs might misuse network resources, creating security vulnerabilities or even performing malicious network activities.
  - **Memory and System Calls:** Untrusted programs could attempt to access restricted memory or issue unauthorized system commands, which could lead to instability or data breaches.
7. Response Time Limits for Simple Servers:
  - **Unpredictable Response Time:** A simple server's response time can vary due to unpredictable workloads and resource availability. For example, network delays, CPU load, or memory limitations can all impact response time.
  - **Bounded Response Time Implementation:** Implementing strict time limits would require task prioritization and resource allocation. However, this can be impractical, as the server's workload or request type may vary, impacting the actual response time.
8. Limitations of Network Time Protocol (NTP):
  - **Lack of Guaranteed Precision:** NTP aims to synchronize clocks, but delays in data transmission, especially in distributed networks, introduce variances in timing.
  - **Resulting Time Differences:** Due to these factors, exact synchronization can't be guaranteed, so clock differences may still occur even with NTP in place.
9. Internet Security Threat Types:
  - **Process Threats:** Malicious code may exploit processes running on servers or devices to gain unauthorized access or execute harmful operations.
  - **Communication Channel Threats:** Intercepting data on communication channels can lead to man-in-the-middle attacks, where attackers access or alter sensitive information.
  - **Denial of Service (DoS):** In a DoS attack, malicious users flood a system with requests, exhausting resources and preventing legitimate access.