Fundamental Models

1) Interaction Model

→ Computation occurs within processes

→ The processes interact by passing messages

- communication (information flow) (Performance → Latency, Bandwidth)
- Co-ordination (Synchronization and Ordering of activities) between Processes.

Synchronous
- Process is executing in a known lower/upper bound time
- message is received within a known bound time
- known local clock drift rate

Asynchronous communication has no bound on
- Process execution speed
- message transmission delay
- clock drift rate

Fundamental Models

1) Interaction Model

→ Computation occurs within processes

→ The processes interact by passing messages

- communication (information flow) (Performance → Latency, Bandwidth)
- Co-ordination (Synchronization and Ordering of activities) between Processes.

Synchronous
- Process is executing in a known lower/upper bound time
- message is received within a known bound time
- known local clock drift rate

Asynchronous communication has no bound on
- Process Execution Speed
- message transmission delay
- clock drift rate

Failure model

- Failure model defines and classifies the faults
- It is important to understand the kind of failure that may occur in a system

1) **Fail Stop** : A process halts & remains halted other process can detect that the process has failed

2) **Crash** : A process halts & remains halted other process is not able to detect this state

3) **Omission** :- A msg inserted in a outgoing msg buffer never arrives at the other ends incoming msg buffer

4) **Arbitrary** : Process Exhibits arbitrary behaviour : it may send/transmit arbitrary messages at arbitrary times, commit mission, stop or take an incorrect step.

5) **Timing Failure** : clock drifts exceeds allowable bounds

Security model

There are several Potential threats a system designer needs to be aware of

(1) Threats to Proasses : An attackers sends a request or respond using false identity

(2) Threats to communication channel : An attacker may listen to message and save

(3) Denial of Service : An attacked may overload a server by making Exessive request

Cryptography and authentication are often use to Provide security