A distributed system is one in which components located at networked computers communicate and coordinate their actions only by passing messages.

Distributed system characteristics:

- Multiple autonomous components
- Components are not shared by all users
- Resources may not be accessible
- Multiple points of control and failure
- Software runs in concurrent processes on different processors.

Computers that are connected by a network may be spatially separated by any distance. They may be on separate continents, in the same building, or in the same room. Our definition of distributed systems has the following significant consequences:

- Concurrency
- No global clock
- Independent failures.
The capacity of the system to handle shared resources can be increased by adding more resources to the network. No global clock exists, so when programs need to cooperate they coordinate their actions by exchanging messages. Close coordination often depends on a shared idea of the time at which the programs action occurs. But it turns out that there are limits to the accuracy with which the components (computers) in a network can synchronize their clocks - there is no single global notion of the correct time.

Irreducible Failure:

All computer systems can fail, and it is the responsibility of system designers to plan for the consequences of possible failures. Distributed systems can fail in new ways. Faults in the network results in the isolation of the computers that are connected to it, but
That doesn’t mean that they running stop. Each component of the system can fail independently, leaving the others still running. The consequences of this characteristic of distributed systems will be a recurring theme of this problem.

Examples of distributed systems:

The goal of this section is to provide motivational examples of contemporary distributed systems illustrating both the pervasive role of distributed systems and great diversity of the associated applications.

Networks are everywhere and underpin many everyday services that we now take for granted; the Internet and the associated World Wide Web (WWW), web search, online gaming, email, social networks, e-commerce, etc.

Distributed systems are undergoing a period of significant change and this can be traced back to a number of influential periods or trends.
the emergence of pervasive networking technology

the emergence of ubiquitous computing coupled with the desire to support users mobility in distributed systems.

the increasing demand for multimedia services.

the view of distributed systems and utility.

Internet

The modern internet is a vast interconnected collection of computer networks of many different types, with the range of types increasing all the time and now including, for example, a wide range of wireless communication technologies such as WiFi, WiMax, Bluetooth and third generation mobile phone networks. The net result is that networking has become a pervasive resource and devices can be connected at any time and in any place.
Intranet:

- A portion of the internet that is separately administered and has a boundary that can be configured to enforce local security policies.

- Composed of several LAN's linked by backbone connections.

- Be connected to the Internet via a router.

- Issues in the design of components for use in Intranet:
  - File Services
  - Firewall
  - The cost of software installation and support
Mobile and ubiquitous computing: Distributed systems are undergoing a period of significant change and this can be traced back to a number of influential trends.

- Pervasive networking and the modern Internet
- Distributed multimedia systems
- Distributed computing as a Utility

Trends in distributed systems:

Pervasive networking and the modern Internet

The Internet is also a very large distributed system. It enables users, wherever they are, to make use of services such as the www, email and file transfer.

The set of services is open-ended—it can be extended by the addition of new servers and new types of service.
The figure shows a collection of intra-organizational sub-networks operated by companies and other organizations and typically protected by firewalls. The role of a firewall is to protect an intranet by preventing unauthorized messages from leaving or entering.

A firewall is implemented by filtering incoming and outgoing messages. Filtering might be done by source and destination, or a firewall might allow only those messages related to email and web access to pass into or out of the intranet that it protects.

Mobile and Ubiquitous Computing:

Technological advances in device miniaturization and wireless networking have led increasingly to the integration of small and powerful computing devices into distributed systems. These devices include:

- Laptop computers
- Handheld devices, including mobile phones, smart phones, GPS-enabled devices, pagers, PDAs, video cameras, and digital cameras
* Wearable devices, such as smart watches

* Devices enabled in appliances such as washing machine, hi-fi systems, cars and refrigerators.

Mobile computing is the performance of computing tasks while the user is on the move, or visiting places other than their usual environment. In mobile computing users who are away from their 'home' intranet are still provided with access to resources via the devices they carry with them.

Ubiquitous computing is the harnessing of many small, cheap computational devices that are present in users' physical environments, including the home, office and even natural settings.
Distributed Multimedia Systems.

A distributed multimedia system should be able to perform the same function for continuous media type such as audio and video: that is, it should be able to store and locate audio or video files, to transmit them across the network, to support the presentation of the media types to the users and optionally also to share the media types across a group of users.

Benefits:

Distributed multimedia computing are considerable in that a wide range of new services and applications can be provided on the desktop, including access to live or pre-recorded television broadcasts, access to Gaines libraries, video on demand, music libraries or related to technologies as Skype, a peer-to-peer alternative to VoIP telephony.

Distributed computing as a utility.

With the increasing maturity of distributed systems infrastructure, a number of companies are promoting the view of distributed resources.
as a commodity or utility drawing the
analogy between distributed resources and other
utilities such as electricity. This model
applies to both physical resources and more
logical services.

**Physical resources:**

Physical resources such as storage
and processing can be made available to
networked computers, removing the need to own
such resources on their own. At one end of the
spectrum, a user may opt for a remote
storage facility for file storage requirements and/or for backups.

**Software services:**

Software services can also be made
available across the global Internet using this
approach. Indeed, many companies now
offer a comprehensive range of services for
effective rental, including services such as
email and distributed calendars.
Resource sharing and the Web:

The benefits of resource sharing that they may easily overlook their significance. We routinely share hardware resources such as printers, data resources such as files, and resources with more specific functionality such as search engines.

The users are sharing of the higher-level resources that play a part in their applications and in their everyday work and social activities.

Service:

We use the term service for distinct part of a computer system that manages a collection of related resources and presents their functionality to users and applications.

Example: File service.

Server:

It refers to a running program on a networked computer that accepts requests from programs running on other computers to perform a service and responds appropriately.
Client and Server:

The terms 'client' and 'server' refer to processes rather than the computers that they execute upon, although in everyday parlance those terms also refer to the computers themselves.

The World Wide Web (WWW):

The WWW is an evolving system for publishing and accessing resources and services across the Internet. Through commonly available web browsers, users retrieve and view documents of many types, listen to audio streams and view video streams, and interact with an unlimited set of services.

The web is an open system; it can be extended and implemented in new ways without distributing its existing functionality. The operation is based on communication standards and document standards that are freely published and widely implemented.
The web is open with the respect of type of resources that can be published and shared on it. At its simplest, these resources on the web is a web page or some other type of content that can be stored in a file and presented to the user, such as program files, media files and documents in Post-Script or PDF.

The web is based on three main standard technological components:

1. HTML
2. URL
3. Client-server architecture.

1. HTML:

The HTML is used to specify the node and image that make up the contents of a web page, and to specify how they are laid out and formatted for presentation to the user.

A web page contains such structured items as headings, paragraphs, tables and images. HTML is also used to specify links and which resources are associated with them.
2. URL:

The purpose of Uniform Resource Locator is to identify a resource. Indeed, the term used in web architecture document is URL.

3. HTTP:

The HTTP defines the ways in which browsers and other types of client interact with web servers.

- Request-reply instruction
- Content types
- One resource per request
- Simple access control.
Challenges:

Heterogeneity:
The Internet enables users to access services and run applications over a heterogeneous collection of computers and networks. Heterogeneity applies to all of the following:

* networks
* computer hardware
* OS
* programming languages
* implementation by different developers.

The Internet consists of many different sorts of networks. Their differences are measured by the fact that all of the computers attached to them use the IP to communicate with one another.

Middleware:
The term middleware applies to a software layer that provides a programming abstraction as well as managing the heterogeneity of the underlying networks, hardware, OS and programming languages.

EX: CORBA, RMI
A middleware provides a uniform computational model for use by the programmers of servers and distributed applications. Possible models include remote object invocation, remote event notification, remote file access, and distributed transaction processing.

Heterogenity and mobile code

The term mobile code is used to refer to code that can be sent from one computer to another and run at the destination.

Ex: Java applets

The virtual machine approach provides a way of making code executable on any hardware.

Openness:

The openness of a computer system is a characteristic that determines whether the system can be extended and re-implemented in various ways.
The openness of distributed systems is determined primarily by the degree to which new resource sharing services can be added and be made available for use by a variety of client programs.

* Open systems are characterized by the fact that their key interfaces are published.
* Open distributed systems are based on the provision of a uniform communication mechanism and published interfaces to access to shared resources.
* Open distributed systems can be constructed from heterogeneous hardware and software, possible from different vendors.

Security

Security for information resources has three components.

1. Confidentiality
2. Integrity
3. Availability
The Internet allows a program on one computer to communicate with a program on another computer irrespective of its location. Security risks are associated with allowing free access to all of the resources in an intranet.

Although a firewall can be used to form a barrier around an intranet, restricting the traffic that can enter and leave, this does not deal with ensuring the appropriate use of resources by users within an intranet, or with the appropriate use of resources on the Internet, that are not protected by firewalls.

The following two security challenges:

1. Denial of service attacks
2. Security of mobile code.
Scalability:

A system is described as scalable if it will remain effective when there is a significant increase in the number of resources and the number of users.

The design of scalable distributed systems presents the following challenges:

* Controlling the cost of physical resources.
* Controlling the performance loss.
* Preventing software resources running out.
* Avoiding performance bottlenecks.

Failure Handling:

Failures in a distributed system are partial failures where some components fail while other components continue to function. Therefore, the handling of failures is particularly difficult.

* Detecting failures.
* Masking failures.
* Tolerating failures.
* Recovery from failures.
* Redundancy.
Concurrency:

Both services and applications provide resources that can be shared by clients in a distributed system. There is, therefore, a possibility that several clients will attempt to access a shared resource at the same time.

The process that manages a shared resource could handle one client request at a time. But that approach limits throughput. Therefore, services and applications generally allow multiple client requests to be processed concurrently.

Transparency:

Transparency is defined as the concealment from the user and the application programmer of the separation of components in a distributed system, so that the system is perceived as a whole rather than as a collection of independent components. The implications of transparency are a major influence on the design of the system software.