Important Instructions:

1) **Open this MS-Word document and start writing answers below each respective question given on page 2.**
2) **Answers the question in the same sequence in which they appear.**
3) **Provide to the point and concrete answers. Some of the questions are open ended and therefore must be answered using your own opinion and thoughts but backed with logical reasons.**
4) **First read the questions and understand what is required of you before writing the answer.**
5) **Attempt the paper yourself and do not copy from your friends or the Internet. Students with exactly similar answers or copy paste from the Internet will not get any marks for their assignment.**
6) **You can contact me for help if you have any doubt in the above instructions or the assignment questions.**
7) **All questions must be attempted.**
8) **Do not forget to write your name, university ID, class and section information.**
9) **Rename you answer file with your university ID# before uploading to SIC.**
10) **When you are finished with writing your answers and are ready to submit your answer, convert it to PDF and upload it to SIC unzipped, before the deadline mentioned on SIC.**

Mid-Summer Semester Examination 2020
Course: - Distributed Computing

Deadline: - Mentioned on SIC **Marks: - 30**

Program: - MS (CS) **Dated: 20 August 2020**

Student Name: __AWAID ULLAH___Student ID#:___12714___

Class and Section: _MS(CS)__

Question1: **Provide an example of a modern Distributed System not discussed in the course; discuss how this system solves certain challenges by employing distributed architecture. (5)**

Question2: **Provide an example from your own practical experience that how a Distributed System can be used as a utility? (5)**

Question3: **What kind of problems can arise if a Distributed System is designed without proper consideration to Quality of Service? (5)**

Question4: **With the help of an example explain the difference between a Physical Model and Architectural Model. (5)**

Question6: **The following are some of the threats and attacks on Distributed Systems. Provide potential solutions as how may be these threats and attacks be mitigated? (10)**

1. **Leakage**
2. **Tampering**
3. **Vandalism**
4. **Eavesdropping.**
5. **Denial of Service**

Question1: Provide an example of a modern Distributed System not discussed in the course; discuss how this system solves certain challenges by employing distributed architecture.

Answer: -

A distributed system is the collection of autonomous computers that are connected using a communication network and they communicate with each other by passing messages. The different processors have their own local memory. They use a distribution middleware. They help in sharing different resources and capabilities to provide users with a single and integrated coherent network.

Distributed computing is a field of computer science that studies distributed systems and the computer program that runs in a distributed system is called a distributed program. A distributed system requires concurrent Components, communication network and a synchronization mechanism. A distributed system allows resource sharing, including software by systems connected to the network.

Examples of distributed systems

1. Intranets, Internet, WWW, email.
2. Telecommunication networks: Telephone networks and Cellular networks.
3. Network of branch office computers -Information system to handle automatic processing of orders,
4. Real-time process control: Aircraft control systems,
5. Electronic banking,
6. Airline reservation systems,
7. Sensor networks,
8. Mobile and Pervasive Computing systems.

Electronic Banking

E-banking is a product designed for the purposes of online banking that enables you to have easy and safe access to your bank account. E-banking is a safe, fast, easy and efficient electronic service that enables you access to bank account and to carry out online banking services, 24 hours a day, and 7 days a week.

Faster Performance

A distributed database management system relies on multiple processors distributed throughout the network, and this is a plus. The distributed nature of the network allows each processor to take on part of the data access chores, rather than relying on a single processor to handle all the requests at once. This system allows banks to access the data they need faster and more reliably than they would with a centralized system.

Lower Costs

A distributed database management system allows each bank branch to have its own copy of the latest customer data. The bank's copy of the customer's account data allows the bank to record and process each transaction locally, rather than sending it forward to a central server. The ability to process transactions locally saves on communication costs. If a problem occurs with the local system, it can be addressed at the local level, which also saves time and money.

Easier Growth

A centralized database management system often lacks the flexibility to handle substantial growth. When such a system needs to expand its capabilities, the bank may need to purchase new equipment, upgraded software or both. The distributed database management system structure supports modular growth. As a bank expands into new geographic areas or offers new financial services, database managers can add the new functionality to the distributed database system without affecting the current system's functions.

Question2: Provide an example from your own practical experience that how a Distributed System can be used as a utility?

ANSWER:-

Users can now use the services provided by companies such as Amazon and Google to access complex data centers and even computing infrastructure. Users can actually get services through virtual nodes (virtual operating systems) instead of physical nodes. You can also use this method to provide software services on the global Internet. Many companies now provide a full range of services for effective leasing, including email and calendar services. The term cloud computing is used to capture this computing view of utilities. Cloud is defined as a collection of Internet-based computing applications, storage and services that are sufficient to meet the needs of most users, thereby enabling them to have no local data storage and application software. The term also promotes a view of all services from physical or virtual infrastructure to software, usually pay-per-use rather than purchase. Note that cloud computing reduces the need for user equipment, allowing very simple desktop or portable devices to access potentially a wide range of resources and services. Clouds are usually implemented on clusters of computers to provide the scale and performance required for these

services. A cluster computer is a collection of interconnected computers that work together to provide unique, integrated high-performance computing functions. The blade server is the smallest computing element, for example, contains processing and storage capacity (main memory).The blade system consists of a large number of potential blade servers contained in a blade chassis. The chassis provides other items such as power, cooling, persistent storage (disk), network, and display. Using this solution, a single blade server can be smaller and cheaper to produce than a basic PC. The overall goal of cluster computers is to provide a series of cloud services, including high-performance computing functions, mass storage (data center) and richer application services (such as Web search).

Examples

Computation time (CPU time) is the leading resource along with the memory usage. Not limited to physical equipment, the files and network connections, and other resources as well as virtual memory space are also considered computer resources.

CPU time
Physical memory and virtual memory
Hard drive space and access time
Network bandwidth
Environment variable, etc. are also some of the computer resources.

Question3: What kind of problems can arise if a Distributed System is designed without proper consideration to Quality of Service?

ANSWER:-

1. Heterogeneity

The Internet enables users to access services and run applications over a heterogeneous collection of computers and networks. Internet consists of many different sorts of network their differences are masked by the fact that all of the computers attached to them use the Internet protocols to communicate with one another. For e.g. a computer attached to an Ethernet has an implementation of the Internet protocols over the Ethernet, whereas a computer on a different sort of network will need an implementation of the Internet protocols for that network.

2. Openness

The openness of a computer system is the 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.

3. Security

Many of the information resources that are made available and maintained in distributed systems have a high intrinsic value to their users. Their security is therefore of considerable importance. Security for information resources has three components: confidentiality, integrity, and availability.

4. Scalability

Distributed systems operate effectively and efficiently at many different scales, ranging from a small intranet to the Internet. 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.

5. Failure handling

Computer systems sometimes fail. When faults occur in hardware or software, programs may produce incorrect results or may stop before they have completed the intended computation. Failures in a distributed system are partial – that is, some components fail while others continue to function. Therefore the handling of failures is particularly difficult.

6. 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. Object that represents a shared resource in a distributed system must be responsible for ensuring that it operates correctly in a concurrent environment. This applies not only to servers but also to objects in applications. Therefore any programmer who takes an implementation of an object that was not intended for use in a distributed system must do whatever is necessary to make it safe in a concurrent environment.

7. Transparency

Transparency can be achieved at two different levels. Easiest to do is to hide the distribution from the users. The concept of transparency can be applied to several aspects of a distributed system.

a) Location transparency: The users cannot tell where resources are located
b) Migration transparency: Resources can move at will without changing their names
c) Replication transparency: The users cannot tell how many copies exist.
d) Concurrency transparency: Multiple users can share resources automatically.
e) Parallelism transparency: Activities can happen in parallel without users knowing.

8. Quality of service

Once users are provided with the functionality that they require of a service, such as the file service in a distributed system, we can go on to ask about the quality of the service provided. The main nonfunctional properties of systems that affect the quality of the service experienced by clients and users are reliability, security and performance. Adaptability to meet changing system configurations and resource availability has been recognized as a further important aspect of service quality.

9. Reliability

One of the original goals of building distributed systems was to make them more reliable than single-processor systems. The idea is that if a machine goes down, some other machine takes over the job. A highly reliable system must be highly available, but that is not enough. Data entrusted to the system must not be lost or garbled in any way, and if files are stored redundantly on multiple servers, all the copies must be kept consistent. In general, the more copies that are kept, the better the availability, but the greater the chance that they will be inconsistent, especially if updates are frequent.

10. Performance

Always the hidden data in the background is the issue of performance. Building a transparent, flexible, reliable distributed system, more important lies in its performance. In particular, when running a particular application on a distributed system, it should not be appreciably worse than running the same application on a single processor. Unfortunately, achieving this is easier said than done.

Question4: With the help of an example explain the difference between a Physical Model and Architectural Model.

ANSWER:-

Physical Model

The physical model is the representation of the underlying hardware elements of the distributed system, which abstracts the specific details of the computing and network technology used; the distributed system is a system in which the hardware or software components located on the networked computers communicate and only communicate through messages. Coordinate their actions. This leads to the smallest physical model of a distributed system, which is a set of scalable computer nodes interconnected by a computer network for the required delivery of messages. In addition to this basic model, there are three generations of distributed systems. The first is distributed systems, Internet-scale distributed systems, contemporary distributed systems.

Architectural Model

An architectural model in a distributed system is concerned with the placement of its parts and the relationships between them.

System structure based on individually specified components and their interrelationships.

The purpose is to ensure that the structure can meet current and possible future needs.

The main consideration is to make the system reliable, manageable, adaptable and cost-effective. The architectural design of a building has similar aspects-it not only determines its appearance, but also its overall structure and architectural style (classic, modern) and provides a consistent frame of reference for the design

Examples:

Client-server and Peer-to-peer.

In this model, the functions of the individual components of the distributed system is abstracted.

It makes sure that the structure will meet present as well as future demands. Make the system manageable, reliable, adaptable, and cost-effective.

Question6: The following are some of the threats and attacks on Distributed Systems. Provide potential solutions as how may be these threats and attacks be mitigated?

1. Leakage
2. Tampering
3. Vandalism
4. Eavesdropping.
5. Denial of Service

ANSWER:-

The success of the attack depends on the discovery of vulnerabilities in the security of the system. When designing the Internet and its connected systems, security is not a top priority. Threats to distributed systems due to the exposure of its communication channels and interfaces. For many systems, these are the only threats to consider however, there are other threats to systems containing mobile programs and systems whose security is particularly sensitive to information leakage. The main goal of security is to restrict access to information and resources to only those who are authorized to access them. Security threats are divided into three categories:

Leakage: Refers to unauthorized recipients obtaining information.

Tampering: Refers to unauthorized changes to information.

Vandalism: Refers to interference with the normal operation of the system without the benefit of the offender. Attacks on distributed systems depend on accessing existing communication

channels or establishing new channels masquerading as authorized connections. Attack methods can be classified according to the way the channel is abused:
Eavesdropping: obtaining a copy of a message without authorization.
Disguise: Use the identity of another subject to send or receive messages without the permission of the other party.
Mail tampering: intercept and modify its content before forwarding it to the intended recipient.
Replay: Store the intercepted message and send it later. Even with authenticated and encrypted messages, this attack may be effective.
Denial of service: Flooding channels or other resources with messages to deny others access.

1)Leakage

Data leakage is the unauthorized transmission of data from within an organization to an external destination or recipient. The term can be used to describe data that is transferred electronically or physically. Data leakage threats usually occur via the web and email, but can also occur via mobile data storage devices such as optical media, USB keys, and laptops. Without a confidential data breach hitting the headlines. Data leakage, also known as low and slow data theft, is a huge problem for data security, and the damage caused to any organization, regardless of size or industry.

Types of Data Leakage

- The Accidental Breach.
- The Disgruntled or Ill-Intentioned Employee.
- Electronic Communications with Malicious Intent

Data Leakage Prevention

The threat is real, and real threats need serious data leakage prevention. Data loss prevention (DLP) is a strategy that ensures end users do not send confidential or sensitive information outside of the enterprise network. These strategies may involve a combination of user and security policies and security tools. Data loss prevention software solutions allow administrators to set business rules that classify confidential and sensitive information so that it cannot be disclosed maliciously or accidentally by unauthorized end users. Force point's DLP solution allows you to discover and control all sensitive data easily and identify your riskiest users within seconds. Whether you need to apply controls to source code, engineering drawings, financial data or sensitive trade secrets, our solution gives you granular control over the data that matters without affecting productivity and progress.

2) Tampering

Data tampering is the act of deliberately modifying (destroying, manipulating, or editing) data through unauthorized channels. Data exists in two states:

- In transit or at rest. In both instances, data could be intercepted and tampered with.
- Digital communications are all about data transmission.

Example

In the instances where data packets are transmitted unprotected, a hacker can intercept the data packet, modify its contents, and change its destination address. With data at rest, a system application can suffer a security breach and an unauthorized intruder could deploy malicious code that corrupts the data or underlying programming code. In both instances, the intrusion is malicious and the effects on the data always dire. It's one of the biggest security threats that any application, program, or organization can face.

Data tampering Prevention

Data tampering is all about successful illegal system intrusion. So, the first line of defense is handling the 'getting in' part. However, there are other areas of system weaknesses that are also addressed.

Firewalls: -

A firewall is an electronic barrier to a system and its programs. It may be hardware or software designed for network security and uses various specific criteria to control incoming and outgoing traffic. Controlling network traffic is the first line of defense in preventing unauthorized system access. Important files, databases, programs, and applications have to be locked down behind a firewall in parallel with operating systems/platform security.

3) Vandalism

Vandalism is defined as an intentional act that defaces, mars, destroys, alters, or otherwise damages another's property without that person's permission. Examples of vandalism include:

1. Spray painting another's property (examples include vehicles, houses, train cars, and bridges).
2. Keying (or scratching) a vehicle's paint.
3. Knocking over a mailbox or sign
4. Carving initials or drawings into a wood bench, siding, or railing, and
5. Breaking windows.

The effects of vandalism often can be seen in public places like bus Stops, bridges, and tunnels. In such cases, vandalism is considered a "quality of life" crime; the theory is that it undermines the community's sense of safety and well-being. When vandalism is directed at a particular

group, religion, or affiliation it might be labeled a bias or hate crime. So, it should be no surprise that law enforcement authorities and communities take vandalism seriously.

Computer Vandalism

Computer vandalism is a process wherein there is a program that performs hateful function such as extracting a user's password or other data or erasing the hard disk. A vandal differs from a virus, which attaches itself to an existing executable program. The vandal is the full executing entity itself, which can be downloaded from the Internet in the form of an ActiveX control, Java applet, browser plug-in or e-mail attachment.

- Skilled students.
- Inexperienced youths (assisted by the Internet).
- Professional developers.
- Researchers.

How to protect yourself against Computer Vandalism

Anti-malware software is vital in defending your computer, mobile devices and data against computer vandalism, viruses, worms, Trojans and other malware. Most of the Computer Anti-virus Kaspersky, Avira, McAfee, Norton etc. has anti-malware solutions that deliver world-class protection for a wide range of computers and other devices, including:

- Windows PCs
- Linux computers
- Apple Macs
- Smartphones
- Tablets

4) Eavesdropping.

An eavesdropping attack, also known as a sniffing or snooping attack, is a theft of information as it is transmitted over a network by a computer, smartphone, or another connected device. The attack takes advantage of unsecured network communications to access data as it is being sent or received by its user.

- Avoid public Wi-Fi networks.
- Keep your antivirus software updated.
- Use strong passwords.

Eavesdropping is a deceptively mild term. The attackers are usually after Sensitive financial and business information that can be sold for criminal purposes. There also is a booming trade in so-called spouse ware, which allows people to eavesdrop on their loved ones by tracking their smartphone use.

How to Stop an Eavesdropping Attack

1. Eavesdropping attacks can be prevented by using a personal firewall, keeping antivirus software updated, and using a virtual private network (VPN).

5) Denial of Service

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected. Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle