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 Semester Assignment
Course: - Distributed Computing

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

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

Student Name: ZIA-UR-RAHMAN **Student ID#: 12881**

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)**

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.

<u>**Question2:**</u> **Among the trends of Distributed Systems discussed in C1-Lec2, which trend in your opinion will be most dominant in the future and why? (4)**

<u>**Answer:**</u> **-**

<u>Trends in distributed systems</u>

Distributed systems are undergoing a period of significant change and this can be traced back to a number of influential trends:

1. the emergence of pervasive networking technology;
2. the emergence of ubiquitous computing coupled with the desire to support user mobility in distributed systems;
3. the increasing demand for multimedia services; Multimedia Distributed Systems
4. the view of distributed systems as a utility

In my opinion Mobile and ubiquitous computing Is most dominant in the future because next era is the digital era the key tools used in this era is the digital computers and mobile phones, smart phone plays an important role. Now a days we can use mobile use as a computer and have access to internet very easily and reliable, Laptop computers, smart phones and other digital devices.

<u>**Question3:**</u> **Among the challenges of Distributed Systems discussed in C1-Lec2, which problem in your opinion will accompany distributed systems into the future and why? (3)**

<u>**Answer:**</u> **-**

There are many challenges in the distributed system which are follow: -

- ✓ Security
- ✓ Heterogeneity
- ✓ Failure handling
- ✓ Concurrency

<u>Security is the main problem</u>

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

- **Confidentiality**

Refers to the property of a computer system whereby its information is disclosed only to authorized parties.

- **Integrity**

Refers to the characteristic that alterations to a system's assets can be made only in an authorized manner.

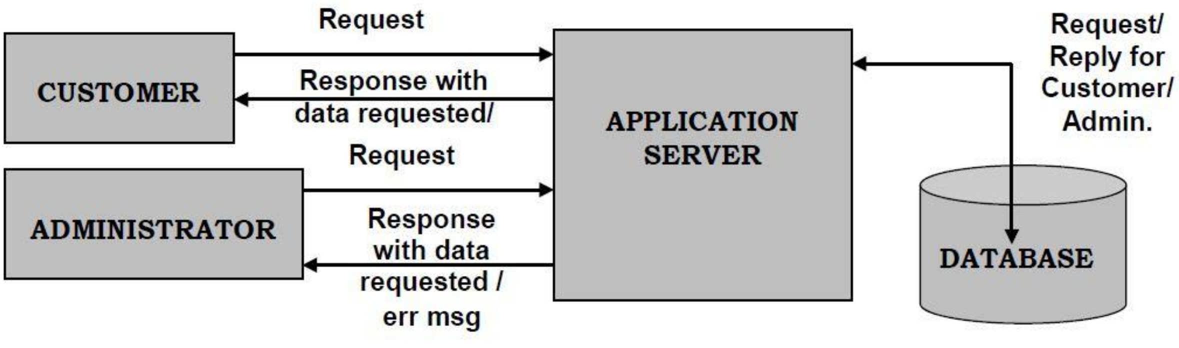
Types of attacks
Passive and active attacks
Passive attacks are browsing inferencing and masquerading while active attacks are viruses' worm's logic bombs integrity attack

Question4: **The design of distributed systems can be described and discussed in three ways i.e Physical Model, Architectural Model and Fundamental Model. Describe the example of distributed system in Question1 with respect to these three models. (5)**

Answer: -

Electronic Banking in the distributed system is described in the three ways i.e Physical Model, Architectural Model and Fundamental Model as described as: -

1. In the Physical Model in the Electronic Banking the hardware composition of a system i.e. the hardware most commonly used in Electronic Banking is Service of the Bank, Smart phone for Electronic Banking, ATM Machine which is used and the Computer used in Bank, it means the physical devices used in Electronic Banking distributed System.
2. In the Architectural Model in the Electronic Banking System described the Architectural of the distributed system that the Encryption techniques used by the bank (including the public-key encryption) should ensure that the privacy of data flowing between the browser and the server system is protected. The message digest technique used by the bank should guarantee the integrity of data moving between the bank customer and the server. Following proposed hybrid architecture model in below Figure, which comprises the hyperelliptic curve cryptosystem over finite field Fp of genus 2 and the MD5 technique, overcomes the security issues called privacy of sensitive data and the integrity of the same data flowing between client and the server.


Request
CUSTOMER
Response with data requested/
Request
ADMINISTRATOR
Response with data requested / err msg
APPLICATION SERVER
Request/ Reply for Customer/ Admin.
DATABASE

3. In the Fundamental Model in the Electronic Banking the Fundamental rights of Client which are security and accuracy and other client security of the transactions of money, use of Electronic banking

access and authentication of client are secure and make sure that grantee to the client that the E-banking safe and secure transaction.

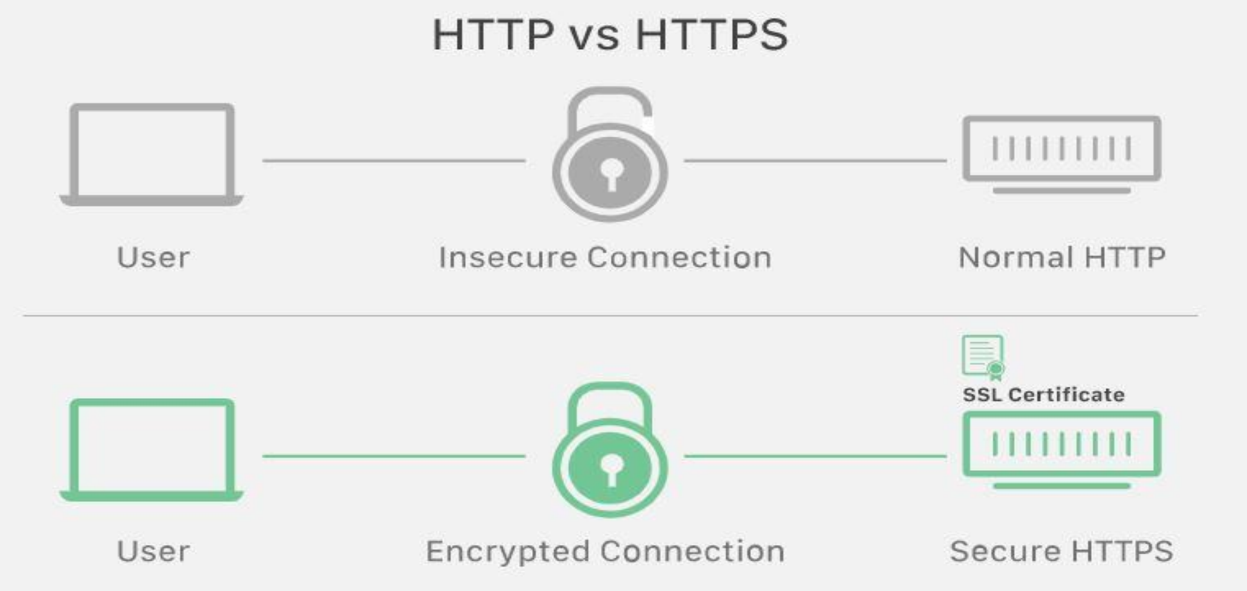
Question5: What is the purpose of Inter Process Communication (IPC) in distributed systems? Given the choice which protocol out of UDP and TCP will you use for your own distributed system and why? (5)

Answer: -

Inter process Communication is a process of exchanging the data between two or more independent process in a distributed environment is called as Inter process communication. Inter process communication on the internet provides both Datagram and stream communication.

For my own Distributed System, I will use Secure Sockets Layer (SSL) protocol. Because Secure Sockets Layer (SSL) protocol is an encryption-based Internet security protocol.

Secure Sockets Layer (SSL) protocol ensuring privacy, authentication, and data integrity in Internet communications. SSL is the predecessor to the modern TLS encryption used today.



How does SSL work?

- In order to provide a high degree of privacy, Secure Sockets Layer (SSL) protocol encrypts data that is transmitted across the web. This means that anyone who tries to intercept this data will only see a garbled mix of characters that's nearly impossible to decrypt.
- Secure Sockets Layer (SSL) protocol initiates an authentication process called a handshake between two communicating devices to ensure that both devices are really who they claim to be.

- Secure Sockets Layer (SSL) protocol also digitally signs data in order to provide data integrity, verifying that the data is not tampered with before reaching its intended recipient.

<u>Question6:</u> 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? (8)

<u>Answer:</u> -

1. <u>Leakage</u>

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

<u>Data Leakage Prevention</u>

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. Forcepoint'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. <u>Tampering</u>

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:

- Spray painting another’s property (examples include vehicles, houses, train cars, and bridges).
- keying (or scratching) a vehicle’s paint.
- knocking over a mailbox or sign
- carving initials or drawings into a wood bench, siding, or railing, and
- 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).

2. Using a strong password and changing it frequently helps, too. And don't use the same password for every site you log onto.
3. Public wi-fi networks such as those that are available free in coffee shops and airports should be avoided, especially for sensitive transactions. They are easy targets for eavesdropping attacks. The passwords for these public networks are readily available, so an eavesdropper can simply log on and, using free software, monitor network activity and steal login credentials along with any data that other users transmit over the network.