CMP521 ASSIGNMENT#3

1. Utilize the Cambridge Distributed Processing System as an example to illustrate the concept of security, email and database research applications in distributed computer systems.

A: The **Cambridge Distributed Processing System** (CDPS) is a research-oriented platform developed at the University of Cambridge. It serves as an excellent example to discuss various aspects of distributed systems, including security, email, and database research applications. Let's break it down:

1. **Security in CDPS**:
    - In a distributed system like CDPS, ensuring security is paramount. Here are some security considerations:
        - **Authentication and Authorization**: CDPS must authenticate users and authorize their access to resources. This involves verifying identities, managing access control lists, and ensuring secure communication channels.
        - **Encryption**: CDPS should encrypt data transmission between nodes to prevent eavesdropping or tampering.
        - **Access Control**: CDPS administrators define policies to control who can perform specific actions (read, write, execute) on shared resources.
        - **Intrusion Detection**: CDPS monitors for suspicious behavior, detecting potential attacks or unauthorized access.
        - **Firewalls and Network Segmentation**: CDPS segments its network to isolate critical components and protect against external threats.
        - **Secure Communication Protocols**: CDPS uses secure protocols (e.g., TLS/SSL) for inter-node communication.
2. **Email in CDPS**:
    - CDPS likely includes an email subsystem for communication among its distributed nodes. Here's how it might work:
        - **Distributed Mail Servers**: CDPS could have multiple mail servers distributed across different locations. These servers handle email storage, retrieval, and delivery.
        - **Message Queues**: CDPS nodes use message queues to exchange emails asynchronously. These queues ensure reliable delivery even if some nodes are temporarily unavailable.
        - **Redundancy and Failover**: CDPS ensures email availability by replicating data and having backup servers.
        - **Spam Filtering and Security**: CDPS employs spam filters, virus scanners, and encryption to protect email content.
3. **Database Research Applications in CDPS**:
    - CDPS likely hosts distributed databases for research purposes:
        - **Replication and Sharding**: CDPS may replicate databases across nodes for fault tolerance and distribute data shards for scalability.

- **Consistency Models**: CDPS researchers study consistency models (e.g., eventual consistency, strong consistency) and their impact on distributed databases.
- **Query Optimization**: Researchers explore efficient query processing and optimization techniques.
- **Distributed Transactions**: CDPS investigates distributed transaction management, ensuring atomicity, consistency, isolation, and durability (ACID properties).
- **NoSQL Databases**: CDPS might experiment with NoSQL databases (e.g., key-value stores, document stores) for specific use cases.
- **Data Distribution Strategies**: CDPS researchers analyze data partitioning, replication strategies, and load balancing.

2. Differentiate between thin using the PC as diskless PC, Thin client, normal PC Workstation, and thick client?

1. A: **Diskless Workstation (Thin Client)**:
    - A **diskless workstation** (also known as a **thin client**) is a client computer that connects to a networked server. Here's what sets it apart:
        - **Minimal Hardware**: A diskless workstation contains only the essential hardware components necessary for the user to interact with the system. It typically includes a monitor, motherboard, network card, keyboard, and mouse.
        - **No Local Storage**: Unlike traditional PCs, thin clients lack local hard disk storage. Instead, they rely on another computer (usually a server) to provide the operating system and software applications.
        - **Processing Offloaded**: Thin clients offload most of the processing work to the server. They handle input/output and basic display tasks but don't perform heavy computations locally.
        - **Cost-Efficient**: Thin clients are cost-effective because they sip power, have no moving parts (like fans or hard disk platters), and are less likely to fail due to their simplicity.
2. **Normal PC (Thick Client)**:
    - A **normal PC** (also called a **thick client**) is what most of us are familiar with:
        - **Local Processing**: Thick clients perform application processing locally. They have their own operating system, storage, and processing power.
        - **Installed Applications**: Applications are installed directly on the PC, and it doesn't rely on a remote server for software execution.

        - **Higher Hardware Specs**: Thick clients typically have more powerful processors, memory, and storage.
        - **Independence**: They can function even when disconnected from the network.
        - **Common Usage**: Regular desktops and laptops fall into this category.

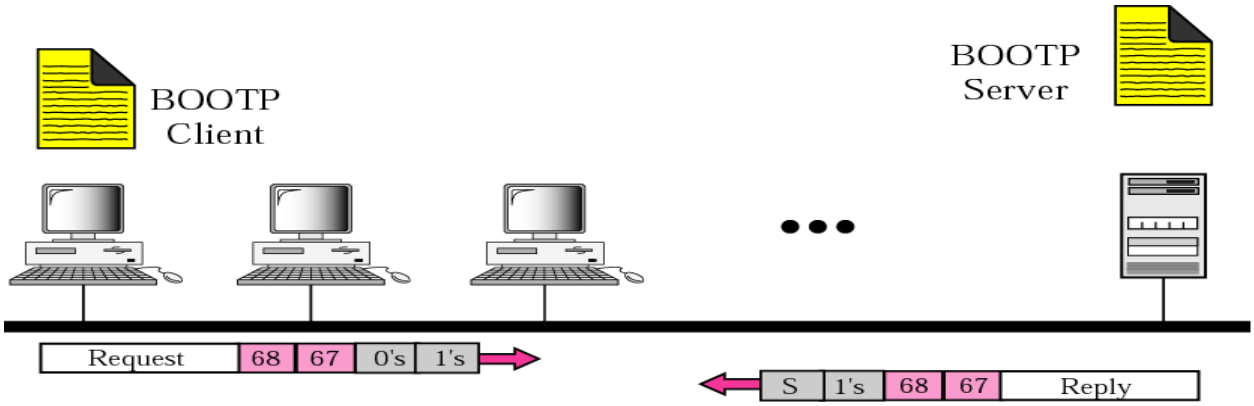
3. **Workstation**:
    - A **workstation** is a high-performance computer designed for specialized tasks, such as 3D modeling, video editing, scientific simulations, or CAD work.
        - **Powerful Hardware**: Workstations boast powerful CPUs, GPUs, and ample RAM.
        - **Optimized for Specific Workloads**: They're tailored for specific professional applications.
        - **Not Necessarily Thin or Thick**: Workstations can be either thin or thick clients, depending on their intended use.
4. **Thick vs. Thin: Pros and Cons**:
    - **Thick Clients**:
        - **Pros**: High processing power, independence from the network, and flexibility.
        - **Cons**: Higher cost, maintenance overhead, and potential security risks.
    - **Thin Clients**:
        - **Pros**: Cost-efficiency, centralized management, lower failure rates, and reduced energy consumption.

3. Define the meaning of A4 (authentication, Authorization, Accounting, and Auditing?

A: **Authentication** is the process of identifying a user and granting them access to the network. **Authentication**, authorization kicks in. It enforces network policies, granular access control, and user privileges.
Accounting is the final piece. It's all about measuring what's happening within the network.
Auditing is essential in cloud computing

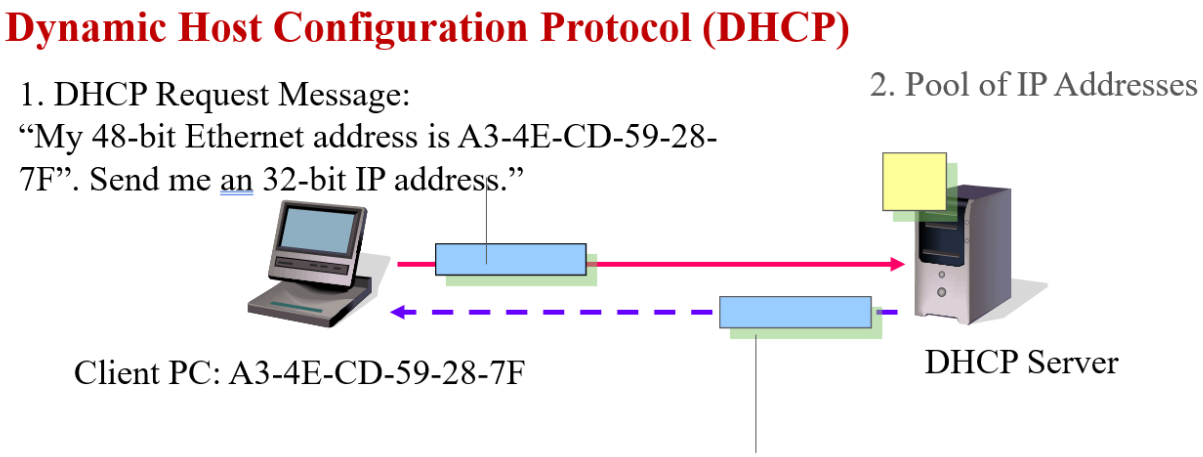
4. Use Drawing and explain the functions of the BOOT Server (Boot Strap BOOTP) protocol for booting diskless PC?

A:



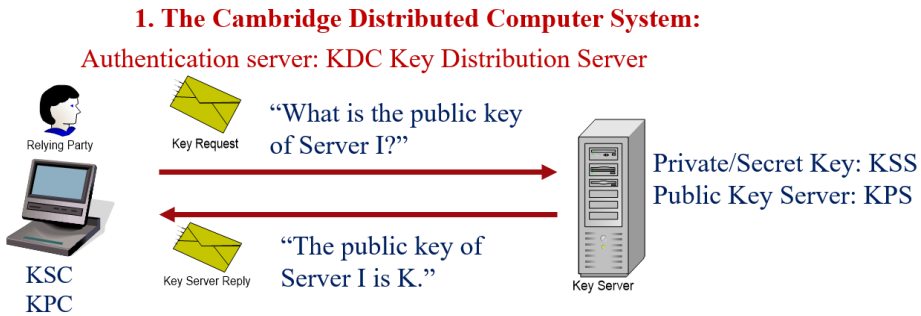
5. Use Drawing and explain the functions of the DYNAMIC HOST protocol?

A:



3. DHCP Response Message:
"Computer at A3-4E-CD-59-28-7F, your 32-bit IP address is 172.16.16.2
11010000101111101010101100000010".

6. Use Drawing and explain the functions of the KDC (Key Distribution Center) authentication Server



7. Use Drawing and explain the functions of the Network Management Server

1. A: **Configuration and Monitoring**:
    - **Collecting Data**: An NMS gathers data from connected network devices such as switches, routers, access points, and client devices. It keeps an eye on their performance, status, and configuration.
    - **Fine-Grained Control**: Network administrators use the NMS to control how these devices operate and interact with each other. For example, they can adjust settings, apply firmware updates, or modify access rules.
2. **Proactive Issue Identification**:
    - The NMS analyzes the collected data to proactively identify performance issues. It's like having a watchful guardian for your network.
    - **Security Monitoring**: It keeps an eye on security-related events, detecting anomalies or potential threats.
    - **Segmentation Oversight**: If you've set up network segments (VLANs), the NMS ensures they're functioning correctly.
3. **Troubleshooting and Accelerated Resolution**:
    - When something goes wrong (and it always does), the NMS helps troubleshoot.
    - **Root Cause Analysis**: It pinpoints where the issue lies—whether it's a misconfigured switch, a congested link, or a flaky access point.
    - **Alerts and Notifications**: The NMS sends alerts to administrators, allowing them to take action promptly.

8. Utilize the underground monitoring and control in coal mines as an example to sensors data sharing.

A: **Wireless Underground Sensor Networks (WUSN)**

In modern underground coal mining (UMC), safety is paramount. One way to enhance safety is through **Wireless Underground Sensor Networks (WUSN)**. These networks consist of sensor nodes strategically placed within the mine to collect critical environmental data. Here's how it works:

1. **Sensor Deployment**:
    - Sensor nodes are installed throughout the mine. These nodes continuously monitor various parameters, such as temperature, humidity, gas concentrations (including methane), and air quality.
    - The sensors are wireless, eliminating the need for cumbersome cables and allowing flexibility in placement.
2. **Data Collection and Transmission**:
    - The sensor nodes collect real-time data from their surroundings.
    - This data is transmitted wirelessly to a central base station located above ground.
    - The base station acts as a hub, aggregating data from all sensors.
3. **Monitoring and Decision Making**:

- The collected data is analyzed to assess the mine's environmental conditions.
- Decision-making algorithms, often based on fuzzy logic or other intelligent techniques, process this data.
- For example, if methane levels exceed safe limits, the system can trigger alarms or ventilation adjustments.

Examples of Sensor Data Sharing in Coal Mines:

1. **Fire Monitoring**:
   - Fires are a significant hazard in coal mines due to the presence of flammable gases and dust.
   - WUSNs play a crucial role in fire detection and prevention.
   - By sharing real-time sensor data, the system can identify abnormal temperature spikes or gas concentrations associated with fires.
2. **Ventilation Control**:
   - Proper ventilation is essential to maintain breathable air and disperse hazardous gases.
   - Sensors continuously monitor air quality, humidity, and gas levels.
   - The data is shared with ventilation control systems, which adjust airflow accordingly.
   - Efficient ventilation prevents toxic gas buildup and ensures miners' safety.

9. Draw and explain the Sensors networking Organizing a sensor network database, while storing and processing data a) only at the operator's site or b) only at the sensors

1. A: **`storing and Processing Data Only at the Operator's Site:`**
   - In this scenario, all sensor data is transmitted to a central location (the operator's site) for storage, analysis, and decision-making.
   - **Advantages**:
     - **Centralized Control**: The operator has full control over data management, security, and processing.
     - **Consolidated Storage**: All data resides in one place, making it easier to manage backups, access controls, and scalability.
     - **Advanced Analytics**: Powerful servers at the operator's site can perform complex analytics on the aggregated data.
   - **Challenges**:
     - **Network Overhead**: Transmitting all sensor data over the network consumes bandwidth and energy. This can be inefficient, especially if sensors are widespread.
     - **Latency**: Real-time decisions may suffer due to data transmission delays.
     - **Single Point of Failure**: If the operator's site experiences issues (e.g., power outage, hardware failure), the entire system is affected.
2. **Storing and Processing Data Only at the Sensors**:

- In this scenario, each sensor stores and processes its own data locally.
- **Advantages**:
  - **Reduced Network Load**: Sensors transmit only relevant information (e.g., anomalies, events), minimizing network traffic.
  - **Low Latency**: Decisions can be made quickly since data processing occurs at the source.
  - **Decentralized Resilience**: No single point of failure; even if one sensor fails, others continue functioning.
- **Challenges**:
  - **Limited Processing Power**: Sensors often have limited computational resources (memory, CPU). Complex analytics may not be feasible.
  - **Data Consistency**: Ensuring consistent data across sensors can be challenging.
  - **Data Aggregation**: Aggregating data for system-level insights becomes harder.
  - **Security**: Local storage raises security concerns (e.g., physical tampering, unauthorized access).

3. **Hybrid Approaches**:
   - Many practical systems combine both approaches:
     - **Edge Computing**: Some processing occurs at the sensors (edge devices), while critical decisions or long-term storage happen centrally.
     - **Distributed Databases**: Data is distributed across multiple nodes (sensors and central servers), balancing trade-offs.
     - **Event-Driven Architecture**: Sensors trigger events based on thresholds, reducing unnecessary data transmission.
4. **Context Matters**:
   - The choice depends on the specific use case, network architecture, and requirements:
     - **Critical Applications**: For safety-critical systems (e.g., earthquake detection), low latency and redundancy are crucial, favoring local processing.
     - **Energy Constraints**: Energy-efficient networks (e.g., IoT devices powered by batteries) may lean toward centralized processing.
     - **Scalability**: Consider how the system scales as the number of sensors grows.

10. Utilize the bank of America as an example of fully redundant distributed system.

A: **Bank of America** is a global financial institution that relies on robust technology infrastructure to provide seamless banking services. Here are some aspects where they demonstrate redundancy and resilience:

1. **Telecommunications and Connectivity**:
    - **Fully Redundant Telecommunication Riser Facility**:
        - Bank of America Plaza (a prominent building housing Bank of America offices) operates a **fully redundant, fully managed telecommunication riser facility**.
        - **Fiber Optic Backbone**: The building features a pre-built fiber optic cabling system connecting every floor. This backbone ensures quick and easy access to over 30 major telephone carriers on-site.
2. **Electrical Infrastructure**:
    - **Limitless Electrical Capacity**:
        - Bank of America Plaza boasts an impressive electrical infrastructure.
        - **Multiple Feeders**: Its fully redundant electrical system receives power from independent ONCOR power generating stations via diverse feeders on the ERCOT grid.
        - **Switchgear and Substations**: The building has redundant switchgear and multiple 500 KW substations, ensuring uninterrupted 480-volt service.
3. **Cooling System**:
    - **N+1 Cooling System**:
        - The building features six individual cooling towers and three chillers with a combined 3,950-ton capacity.
        - These components operate strategically as an N+1 system, allowing maintenance bypass during servicing and emergency failover if any part goes offline.

********** G O O D L U C K **********