Assignment Title:

Real-World Applications of Parallel Computing and Networked Systems

Name: **Souvik Roy**
Batch: **25SUB4508_WiproNGA_LSP**
User ID: **56133**

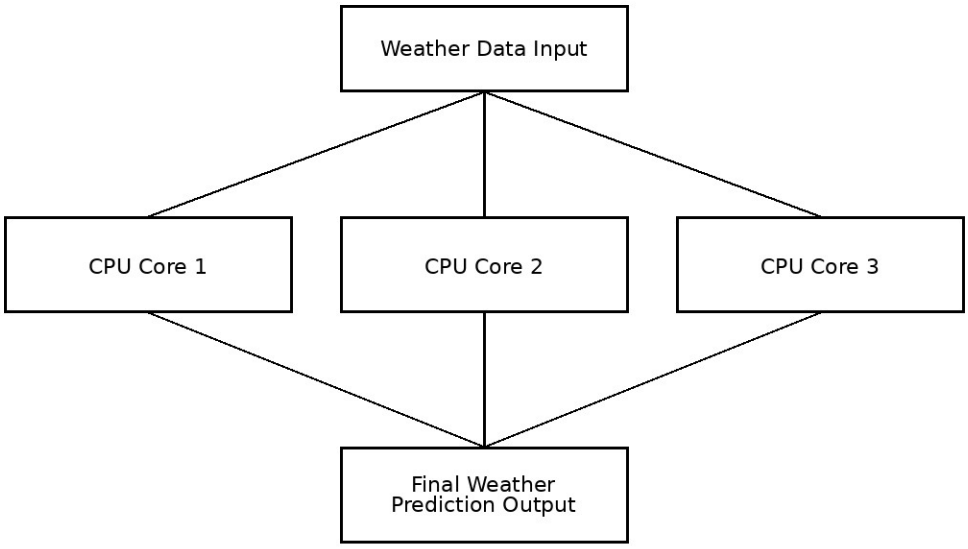
1. Real-World Application of Parallel Computing

Parallel computing refers to a computing approach where a large and complex task is divided into smaller parts that are executed simultaneously using multiple processors or CPU cores. This technique significantly improves processing speed and efficiency. A practical real-world application of parallel computing is weather forecasting.

Use of Parallel Computing in Weather Forecasting

Weather forecasting systems process massive amounts of data collected from satellites, radars, weather stations, and ocean sensors. Instead of processing this data sequentially, the system divides the workload into smaller regions and parameters. Each CPU core processes its assigned data in parallel. Once all cores complete their calculations, the results are combined to generate accurate and timely weather predictions.

Parallel Computing Architecture for Weather Forecasting



Importance of Parallel Computing in This Context

Parallel computing is essential in weather forecasting because predictions must be generated within strict time limits. Faster processing helps issue early warnings for cyclones, floods, and extreme weather conditions. This improves public safety, supports disaster management, and saves lives.

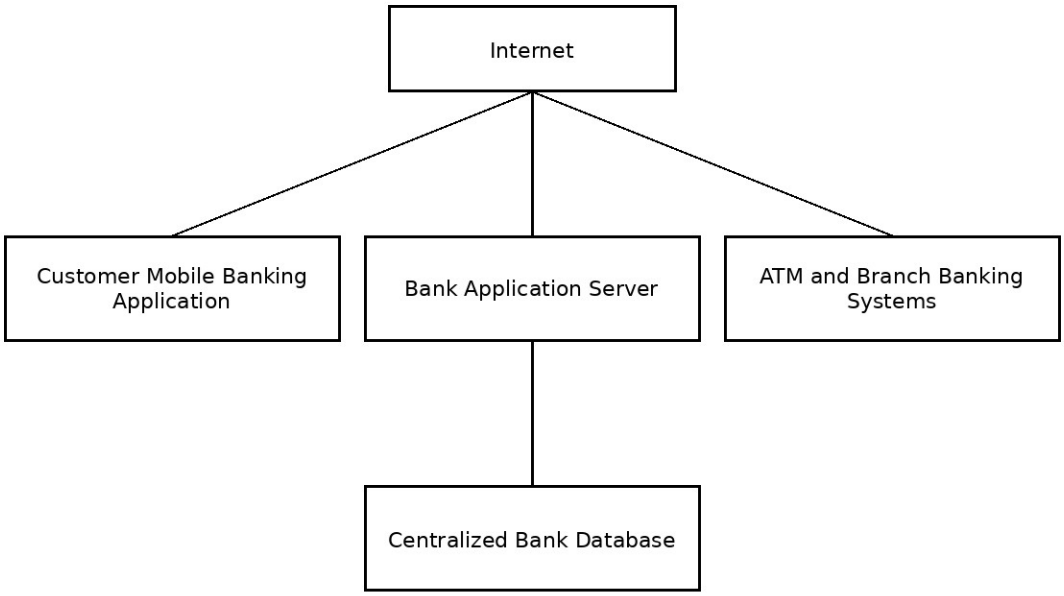
2. Real-World Application of Networked Systems

A networked system is a collection of interconnected computers and devices that communicate and share data over a network. A commonly used real-world example of a networked system is online banking.

Use of Networked Systems in Online Banking

Online banking systems connect customer mobile applications, ATM machines, and bank branch computers to centralized bank servers through the internet. When a customer initiates a transaction, the request is securely transmitted to the bank server. The server verifies the transaction details and updates the centralized database in real time.

Networked System Architecture for Online Banking



Importance of Networked Systems in This Context

Networked systems enable customers to access banking services anytime and from anywhere. They ensure real-time data consistency across all platforms, secure communication, and reliable transaction processing. Without networked systems, modern digital banking services would not be possible.

3. Conclusion

Parallel computing and networked systems are fundamental technologies in modern computing. Parallel computing enables fast and efficient processing of data-intensive applications such as weather forecasting, while networked systems support large-scale services like online banking. Together, these technologies improve performance, reliability, and user experience in real-world applications.

Introduction to Network Security Challenges

• Network security challenges refer to the risks and threats that can affect the safe transmission of data across computer networks.

• In today's digital environment, networks support critical services such as online banking, education platforms, healthcare systems, and cloud applications, making security extremely important.

• Unauthorized access is one of the major challenges, where attackers try to enter a network without permission, leading to data theft or misuse of resources.

• Malware attacks, including viruses, worms, and ransomware, can spread rapidly through connected devices and disrupt normal network operations.

• Phishing attacks trick users into sharing sensitive information like passwords and banking details, often through fake emails or websites.

• Denial-of-Service (DoS) attacks overload network servers with excessive traffic, causing services to slow down or become completely unavailable.

• The use of wireless networks and cloud services introduces additional security concerns such as weak encryption, insecure access points, and misconfigured systems.

• Lack of user awareness is also a challenge, as human errors like weak passwords or clicking on unknown links can compromise network security.

• To address these challenges, organizations use security measures such as firewalls, encryption, intrusion detection systems, regular software updates, and user training.

• Understanding network security challenges helps in protecting sensitive data, maintaining trust, and ensuring the smooth and reliable functioning of networked systems.

Basic Security Measures (Firewalls and VPNs)

• Basic security measures are essential practices used to protect computer networks from cyber threats, unauthorized access, and data breaches.

• A firewall is one of the most important network security tools. It acts as a security gate between a trusted internal network and external networks such as the internet.

• Firewalls continuously monitor incoming and outgoing network traffic and allow or block data packets based on predefined security rules.

• By filtering traffic, firewalls help prevent hackers, malware, and unauthorized users from accessing internal systems.

• Firewalls can be implemented as hardware devices, software applications, or a combination of both, depending on security requirements.

• A Virtual Private Network (VPN) is another key security measure that provides a secure communication channel over the internet.

• VPNs encrypt data before transmission, ensuring that sensitive information such as passwords, personal data, and financial details remain protected from interception.

• VPNs are commonly used when accessing networks through public or unsecured Wi-Fi connections, reducing the risk of cyberattacks.

• In addition to security, VPNs also enhance privacy by masking the user's IP address and location.

• Together, firewalls and VPNs form a strong first layer of network defense by controlling access and securing data transmission.

• Implementing these basic security measures is crucial for maintaining network integrity, protecting sensitive data, and ensuring safe and reliable network communication.

References

Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks (5th ed.). Pearson Education.
Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson.
Stallings, W. (2013). Data and Computer Communications (10th ed.). Pearson.
Forouzan, B. A. (2017). Data Communications and Networking (5th ed.). McGraw-Hill Education.
Hennessy, J. L., & Patterson, D. A. (2019). Computer Architecture: A Quantitative Approach (6th ed.). Morgan Kaufmann.
IEEE Standards Association. IEEE Std 802.3™-2022 (Ethernet).
IEEE Standards Association. IEEE Std 802.11™-2020 (Wireless LAN).