Emerging Technology

- **Define the terms below and, where possible, give examples and cases: Virtual Machine; Bring Your Own Device (BYOD); Parallel computing; Hadoop Distributed computing**.

A **virtual machine (VM)** is an emulated computer system that runs on top of a physical host machine. It operates as a separate entity with its operating system, storage, and hardware resources. VMs allow multiple operating systems to run on a single physical host, providing isolated and secure environments for applications and data. VMware is an example of popular virtualisation software (Daniels, 2009).

Bring Your Device (BYOD) refers to the trend where employees bring their devices, such as smartphones, laptops, and tablets, for work purposes, allowing employees to use their preferred devices for work tasks and increasing mobility and flexibility in the workplace. However, it also poses security and management challenges for IT departments, which must ensure that the personal devices used for work meet security standards and comply with company policies (Afreen, 2014).

Parallel computing is a type of computation where multiple processors work together to solve a single computational problem. It involves dividing an enormous computational task into smaller, more manageable parts that can be processed simultaneously, significantly improving processing speed and overall system performance. An example of parallel computing is using a computer cluster to perform complex scientific simulations or data analysis (Li, 2015).

Hadoop is a software framework for storing and processing large amounts of free and open-source data. It allows for the distribution of large data sets across multiple nodes in a cluster, enabling parallel processing and scalability. Hadoop also provides a fault-tolerant system, allowing for the continuation of processing even if one or more nodes

fail. It is commonly used in finance, healthcare, and retail industries for fraud detection, customer sentiment analysis, and recommendation systems (Nandakumar, 2014).

Distributed computing is a field of computer science that deals with spreading computational tasks across multiple networked computers. The goal of distributed computing is to make a sizeable computational charge appear as if a single machine was executing it while many devices in parallel perform the actual processing. This approach enables more efficient processing, increased reliability, and improved scalability compared to traditional centralised computing. Examples of distributed systems include cloud computing and distributed databases (Ivanisenko & Radivilova, 2015).

- **Bring a case example of Artificial Intelligence to the class to discuss the advantages and disadvantages of deploying such technologies in organisations and societies.**

There are many examples of Artificial Intelligence (AI). Some examples of AI include manufacturing robots, self-driving cars, intelligent assistants such as Siri and Alexa, healthcare management, automated financial investing, virtual travel booking agents, social media monitoring, marketing chatbots and many more. One example of artificial intelligence (AI) I will describe is automated financial investing.

Advantages of deploying automated financial investment:

Improved efficiency: Multiple customer inquiries can be handled simultaneously by automated financial investment, reducing wait times, improving response times, and reducing human error.

Cost savings: Automated financial investments may reduce human customer service representatives, potentially lowering staffing costs.

Availability: Automated financial investments can operate around the clock, providing customers with assistance at all times.

Consistency: Standardised responses from automated financial investment can ensure consistent and accurate customer information. It can also help investors stick to their investment plan, allowing them to avoid emotional reactions.

Disadvantages of deploying Automated financial investments:

Costs to implement: Implementing automated financial investing can be costly.

Limited capability: Handling complex or one-of-a-kind customer inquiries is limited by automated financial investments and may necessitate human intervention. Furthermore, tailoring investments to individual needs can be challenging.

Lack of empathy: Automated financial investments cannot understand and respond to emotions, negatively impacting the customer experience.

Potential for errors: Automated financial investments can be difficult to predict market trends, provide incorrect information, or comprehend customer inquiries, resulting in frustration.

Privacy concerns: Customer data collected through automated financial investment must be securely stored and managed to protect customer privacy.

AI technologies can significantly improve efficiency, cost savings, and customer satisfaction when implemented in organisations. However, organisations must carefully consider AI technologies' potential limitations and risks and implement mitigation measures.

When AI technologies are deployed in society, they can provide numerous benefits, such as improved healthcare and increased productivity. However, there are concerns

about the impact of AI on employment and the technology's potential for malicious use. Society must consider the potential consequences of AI technologies and regulate their development and deployment to ensure they are used ethically and responsibly.

Networking - Reference: (Taeihagh, 2021).

- **Define the following terms and, where possible, give examples and cases: Protocol, Hub, Gateway, Bridge, MAC access, Internet and intranet, Protocol:**

A protocol is a set of rules and standards governing communication between devices in a network. It defines the format of the transmitted data, the methods used for sharing it, and the error detection and correction procedures. Examples of protocols include TCP/IP (Transmission Control Protocol/Internet Protocol), which is used for communication over the internet, and HTTP (Hypertext Transfer Protocol), which is used for transmitting web pages.

A hub is a networking device that provides a central connection point for devices in a network. It receives incoming data from one device and retransmits it to all other devices connected to the hub. Hubs operate at the physical layer of the OSI (Open Systems Interconnection) model, providing a simple way to connect multiple devices in a network but lacking the intelligence to manage network traffic.

A gateway is a networking device that bridges two networks, allowing communication between devices on different networks. It operates at the network layer of the OSI model, and it can provide network address translation, security, and protocol conversion functions. An example of a gateway is a router that connects a local area network (LAN) to the internet.

A bridge is a networking device that connects two separate networks, allowing communication between devices on different networks. Unlike a gateway, a bridge

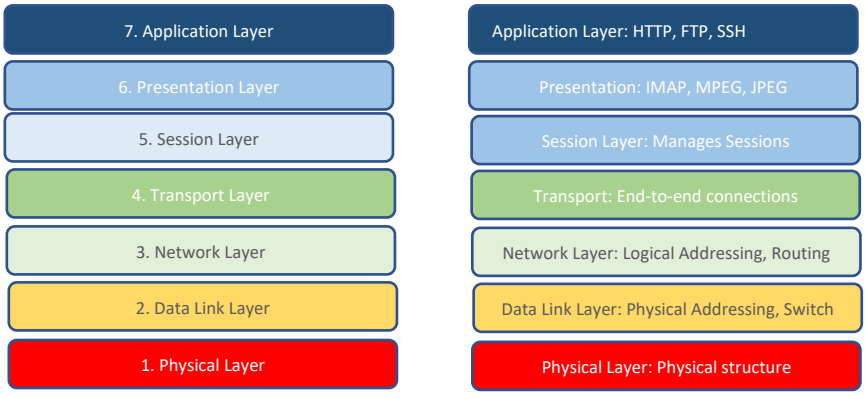
operates at the data link layer of the OSI model, forwarding data based on the MAC (Media Access Control) addresses of devices in the network. Bridges can improve network performance by reducing network traffic and increasing network security.

MAC access refers to using MAC (Media Access Control) addresses in networking. A MAC address is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment. This use of MAC addresses allows devices in a network to communicate with each other and helps ensure network communications' security and integrity.

The internet is a global network of computers and other devices connected to exchange information and communicate. It is open to anyone with a connection and allows for communication and the exchange of information between devices and networks worldwide. On the other hand, an **Intranet** is a private network used within an organisation. It is not accessible from the internet and is used to share information and resources among employees within the organisation. Intranets can include features such as internal websites, file and print services, and communication tools like email and instant messaging.

- **Draw a schematic diagram of the OSI model and show the functionalities at each layer.**

Here is a schematic diagram of the OSI model:



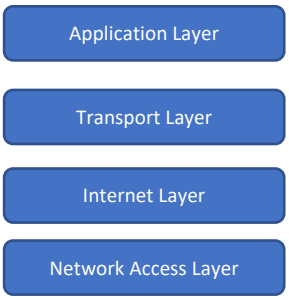
1. **The Application Layer** offers the user services such as email, file transfer, and terminal emulation.
2. **The Presentation Layer** handles data translation and code formatting.
3. **The Session Layer** establishes, manages, and terminates application connections.
4. **The Transport Layer** ensures data is reliably transferred between end systems. The Network Layer handles routing and addressing.
5. **The Data Link Layer** ensures data is reliably transmitted across a physical network link.
6. **The Physical Layer** transmits raw bits across a communication channel.

Here is a brief description of the functionalities at each layer:

1. **Presentation Layer:** This layer deals with the syntax and semantics of data exchanged between applications, including data compression, encryption, and translation.
2. **The session layer** establishes, manages, and terminates sessions between applications on different devices. It also manages authentication and encryption.
3. **Transport Layer:** This layer delivers end-to-end data, ensuring that data is delivered reliably, in sequence, and without errors. It also provides flow control and congestion avoidance.
4. **Network Layer:** This layer provides logical addressing and routing of data between different networks and handles the fragmentation and reassembly of packets.
5. **Data Link Layer:** This layer provides reliable data transfer over a physical link between two devices, including error detection and correction, flow control, and addressing.
6. **Physical Layer:** This layer defines the physical and electrical specifications for transmitting data over physical media, such as cables, wireless, or light signals. It also defines the protocols for data encoding and modulation.

- **Draw a schematic diagram of the TCP/IP protocol and show the functionality of the protocol invoked at each layer of the OSI protocol stack.**

Here is a schematic diagram of the TCP/IP:



Here is a brief description of the functionalities at each layer:

1. **The Application Layer** is responsible for providing services to applications.
2. **The Transport Layer** provides reliable end-to-end communication between applications.
3. **The Internet Layer** is responsible for routing data packets between networks.
4. **Network Access Layer** transmits data frames over a communication channel.

References:

Daniels, J. (2009). Server virtualization architecture and implementation. *XRDS: Crossroads, The ACM Magazine for Students*, *16*(1), pp.8-12.

Afreen, R. (2014). Bring your own device (BYOD) in higher education: Opportunities and challenges. *International Journal of Emerging Trends & Technology in Computer Science*, *3*(1), pp.233-236.

Li, H., Gao, B., Chen, Z., Zhao, Y., Huang, P., Ye, H., Liu, L., Liu, X. & Kang, J. (2015). A learnable parallel processing architecture towards unity of memory and computing. *Scientific reports*, *5*(1), pp.1-8.

Nandakumar, A.N. & Yambem, N. (2014). A survey on data mining algorithms on apache hadoop platform. *International Journal of Emerging Technology and Advanced Engineering*, *4*(1), pp.563-565.

Phan, T., Huang, L. & Dulan, C. (2002), September. Challenge: Integrating mobile wireless devices into the computational grid. In *Proceedings of the 8th annual international conference on Mobile computing and networking* (pp. 271-278).

Taeihagh, A. (2021). Governance of artificial intelligence. *Policy and society*, *40*(2), pp.137-157.

Hegering, H.G., Abeck, S. & Neumair, B. (1999). *Integrated management of networked systems: concepts, architectures and their operational application*. Morgan Kaufmann.