وزارة التعليم العالي والبحث العلمي
الجامعة التقنية الجنوبية
المعهد التقني العمارة
قسم. Healthcare Management Technologies Department

الحقيبة التدريسية لمادة Computer

الصف Second

تدريسي المادة

Nahla Qasim Qadeer

software engineering bachelor`s

الفصل الدراسي second

جدول مفردات مادة computer

الأسبوع	المفردات
1	security and Networking: What is a network? types of networks. Basic network component
2	network Security Basics. Understanding network threats.
3	E-Commerce: Concepts of Electronic banking services this include online banking: ATM and debit card services, Phone banking, SMS banking, electronic alert, Mobile banking
4	computer Troubleshooting: Identifying and solving common hardware .. and software problems that computer users encounter
5	Basic troubleshooting techniques and tools for diagnosing and resolving issues.
6	introduction to Al: Definition of Al, History of Al, Al techniques and Approaches.
7	introduction to AL: count: key characteristics of AL, benefits of AL, challenges and ethical considerations
8	The role of al in modern smartphones: a-driven mobile techniques, virtual assistants (Siri, google assistant, Alexa)
9	The role of al in modern smartphones: count adaptive learning real -time translation services
10	applications of and tools of AL: overview of all applications in various industries, education and healthcare
11	applications of and tools of AL: count transportation, Marketing and Advertising
12	applications of tools of AL: count, Finance, robotics and automation, .transportation
13	I and Society: (How Al affects social, Al and international relations, Al and the future of humanity.)
14	Ethical Challenges in Al :(Al ethics, privacy and surveillance, the impact of Al on the job market.)
15	the Future of Al (Future trends in Al, recent research and emerging technologies.)

الهدف من دراسة مادة. computer. (الهدف العام):

تهدف دراسة مادة.. computer ..... للصف.. secondالى:

1) . Advanced network deepening the understanding of advanced network concepts and information security.
2) E- system and e-commerce exploring the technical and economic aspects of e-commerce digital, banking services
3) complex system diagnosis and repair developing advanced analytical capabilities
4) Introduction and application of artificial intelligence understanding the principles of al and its core technologies.

الفئة المستهدفة:

طلبة الصف second / قسم ..... Healthcare Management Technologies Department

التقنيات التربوية المستخدمة:

1. whiteboard and markers
2. interactive whiteboard
3. data protector Data Show
4. computer devices Laptop
5. poster presentations

first week (الاسبوع الأول)

الهدف التعليمي:learning objective-

الأهداف العامة للمادة:General of objectives

provide students with foundational knowledge of networks and their components along with an initial understanding of network security and common threats. The lecture aims to main types of networks and their differentiate between the primary network threats .core components. and their impact.

مدة المحاضرة: Theoretical and practical (3 hours)

الأنشطة المستخدمة:

1 .Interactive classroom activities
2 .Brainstorming questions
3 . Group activities (if required)
4. Homework
5 .Online homework (it is preferable to create online classrooms to integrate in-person learning with online learning, in accordance with modern teaching and learning trends)

Purposes of Assessment

1. What is the fundamental difference between a **Local Area Network (LAN)** and a **Wide Area Network (WAN)** in terms of geographical scope and the technologies typically used for connection?
2. Explain how **Artificial Intelligence (AI)** can contribute to enhancing **network security**, providing one specific example of this application.
3. • after a lesson on "Building a Simple Home Network," display a well-organized network diagram and ask them to compare their own work to the model.

Pre-test

- **Identify and explain** the basic components of a network (e.g., routers, switches, access points) and their functions.
- **Explain** the concept of network protocols (e.g., TCP/IP) and their importance in communication.
- **Recognize and apply** fundamental network security concepts, including common threats (e.g., viruses, phishing) and protective solutions (e.g., firewalls, antivirus software, strong passwords)
- **Identify and classify** common problems encountered with computer hardware and networks.
- **Apply** a systematic methodology for troubleshooting (e.g., isolating the problem, checking basics, researching solutions).
- **Utilize** basic tools and techniques to resolve simple software and hardware issues.
- **Define and explain** the core concept of Artificial Intelligence and its main subfields (e.g., Machine Learning, Computer Vision, Natural Language Processing).
- **Identify** various AI applications in daily life and industrial sectors.
- **Understand** the basic principles behind simple Machine Learning systems.
- **Discuss** the potential ethical and societal implications of AI development.

عنوان المحاضرة: (security and Networking: What is a network? types of networks. Basic network components.

(First and second week) **الاسبوع الاول والثاني**

What is Network Security?

Every company or organization that handles a large amount of data, has a degree of solutions against many cyber threats. This is a broad, all-encompassing phrase that covers software and hardware solutions, as well as procedures, guidelines, and setups for network usage, accessibility, and general threat protection

The most basic example of Network Security is password protection which the user of the network

chooses. In recent times, Network Security has become the central topic of cyber security with many organizations inviting applications from people we have skills in this area. The network security solutions protect various vulnerabilities of the computer systems such as users, location, data, devices, and applications.

What is Network Security?

Any action intended to safeguard the integrity and usefulness of your data and network is known as network security. In other words, Network security is defined as the activity created to protect the integrity of your network and data.

Network security is the practice of protecting a computer network from unauthorized access, misuse, or attacks. It involves using tools, technologies, and policies to ensure that data traveling over the network is safe and secure, keeping sensitive information away from hackers and other threats.

Network Security

How Does Network Security Work :

Network security uses several layers of protection, both at the edge of the network and within it. Each layer has rules and controls that determine who can access network resources. People who are allowed access can use the network safely, but those who try to harm it with attacks or other threats are stopped from doing so

The basic principle of network security is protecting huge stored data and networks in layers that ensure

the bedding of rules and regulations that have to be acknowledged before performing any activity on the data. These levels are:

- **Physical Network Security: This is the most basic level that includes protecting the data and network through unauthorized personnel from acquiring control over the confidentiality of the network. The same can be achieved by using devices like biometric systems.**

- **Technical Network Security: It primarily focuses on protecting the data stored in the network or data involved in transitions through the network. This type serves two purposes. One is protected from**
-

- **unauthorized users, and the other is protected from malicious activities.**

- **Administrative Network Security: This level of network security protects user behavior like how the permission has been granted and how the authorization process takes place. This also ensures the level of sophistication the network might need for protecting it through**
-
- **all the attacks. This level also suggests necessary amendments that have to be done to the infrastructure.**

Types of Network Security:

There are several types of network security through which we can make our network more secure, Your network and data are shielded from breaches, invasions, and other dangers by network security

. Here below are some important types of network security:

Email Security

Email Security is defined as the process designed to protect the Email Account and its contents safe from unauthorized access. For Example, you generally see, fraud emails are automatically sent to the Spam folder. because most email service providers have built-in features to protect the content.

The most common danger vector for a security compromise is email gateways. Hackers create intricate phishing campaigns using recipients' personal information and social engineering techniques to trick them and direct them to malicious websites. To stop critical data from being lost, an email security programme restricts outgoing messages and stops incoming threats.

Network Segmentation

Network traffic is divided into several categories by software-defined segmentation, which also facilitates the enforcement of security regulations. Ideally, endpoint identity—rather than just IP addresses—is the basis for the classifications. To ensure that the appropriate amount of access is granted to the appropriate individuals and that suspicious devices are controlled and remediated, access permissions can be assigned based on role, location, and other factors.

Access Control

Your network should not be accessible to every user. You need to identify every user and every device in order to keep out any attackers. You can then put your security policies into effect. Noncompliant endpoint devices might either have their access restricted or blocked. Network access control (NAC) is this process.

Sandboxing

Sandboxing is a cybersecurity technique in which files are opened or code is performed on a host computer that simulates end-user operating environments in a secure, isolated environment. To keep threats off the network, sandboxing watches the code or files as they are opened and searches for harmful activity

Cloud Network Security

This is very vulnerable to the malpractices that few unauthorized dealers might pertain to. This data must be protected and it should be ensured that this protection is not jeopardized by anything. Many businesses embrace SaaS applications for providing some of their employees the allowance of accessing the data stored in the cloud. This type of security ensures creating gaps in the visibility of the data.

Workloads and applications are no longer solely housed in a nearby data center on-site. More adaptability and creativity are needed to protect the modern data center as application workloads move to the cloud.

Web Security

A online security solution will restrict access to harmful websites, stop web-based risks, and manage staff internet usage. Your web gateway will be safeguarded both locally and in the cloud. "Web security" also include the precautions you take to safeguard your personal website.

Intrusion Prevention System (IPS)

An intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity. The major

functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it, and attempt to block or stop it

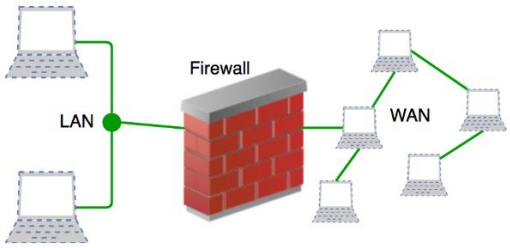
.

Antivirus and Anti-malware Software

This type of network security ensures that any malicious software does not enter the network and jeopardize the security of the data. Malicious software like Viruses, Trojans, and Worms is handled by the same. This ensures that not only the entry of the malware is protected but also that the system is well-equipped to fight once it has entered.

Firewalls Security

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules accepts, rejects, or drops that specific traffic. Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers.



Application Security

Application security denotes the security precautionary measures utilized at the application level to prevent the stealing or capturing of data or code inside the application. It also includes the security measurements made during the advancement and design of applications, as well as techniques and methods for protecting the applications whenever

Wireless Security

Wireless networks are less secure than wired ones. If not properly secured, setting up a wireless LAN can be like having Ethernet ports available everywhere, even in places like parking lots. To prevent attacks and keep your wireless network safe, you need dedicated products designed to protect it from exploits and unauthorized access.

Web Security

A web security solution manages how your staff uses the internet, blocks threats from websites, and stops access to harmful sites. It safeguards your web gateway either onsite or in the cloud. Additionally, "web security" involves measures taken to protect your own website from potential attacks and vulnerabilities

Mobile Device Security

Cybercriminals are focusing more on mobile devices and apps. In the next three years, about 90 percent of IT organizations might allow corporate applications on personal mobile devices. It's crucial to control which devices can connect to your network and set up their connections securely to protect network traffic from unauthorized access.

Industrial Network Security

As industries digitize their operations, the closer integration of IT, cloud services, and industrial networks exposes Industrial Control Systems (ICS) to cyber threats. To safeguard against these risks, it's crucial to have complete visibility into your Operational Technology (OT) security status. This involves segmenting the industrial network and providing detailed information about OT devices and their behaviors to IT security tools. This approach helps in effectively monitoring and protecting critical industrial systems from potential cyber attacks

VPN Security

A virtual private network (VPN) encrypts the connection between a device and a network, usually over the internet. A remote-access VPN commonly uses IPsec or Secure Sockets Layer (SSL) to verify and secure the communication between the device and the network. This encryption ensures that data transmitted between the device and the network remains private and secure from unauthorized access

Benefits of Network Security.

Network Security has several benefits, some of which are mentioned below:

- **Network Security helps in protecting clients' information and data which ensures reliable access and helps in protecting the data from cyber threats.**
- **Network Security protects the organization from heavy losses that may have occurred from data loss or any security incident.**
- **It overall protects the reputation of the organization as it protects the data and confidential items.**

Advantages of Network Security

- **Protection from Unauthorized Access: Network security measures such as firewalls and authentication systems prevent unauthorized users from accessing sensitive information or disrupting network operations.**

- **Data Confidentiality: Encryption technologies ensure that data transmitted over the network remains confidential and cannot be intercepted by unauthorized parties.**
- **Prevention of Malware and Viruses: Network security solutions like antivirus software and intrusion detection systems (IDS) detect and block malware, viruses, and other malicious threats before they can infect systems.**

- **Secure Remote Access: Virtual private networks (VPNs) and other secure remote access methods enable employees to work remotely without compromising the security of the organization's network .**

Disadvantages of Network Security

- **Complexity and Management Overhead: Implementing and managing network security measures such as firewalls, encryption, and intrusion detection systems (IDS) can be complex and require specialized knowledge and resources.**

- **Cost: Effective network security often requires investment in hardware, software, and skilled personnel, which can be expensive for organizations, especially smaller ones.**
- **Privacy Concerns: Some network security measures, such as deep packet inspection and monitoring, may raise privacy concerns among users and stakeholders, requiring careful balancing of security needs with individual privacy rights.**

What Is a Network Security Threat?

A network security threat is any malicious activity that compromises the confidentiality and integrity of online data and systems. It is performed by individuals or groups hoping to gain unauthorized access to systems and steal data. Additionally, perpetrators usually disrupt network operations or perform ransomware by taking

advantage of weak spots in the network. As a result, victims of network threats experience substantial financial losses, reputational damage, or legal penalties.

Read our recommendations for the best network security tools to implement and protect yourself from vicious cyberattacks.

How Does a Network Security Threat Work?

Network security threats aim to exploit system vulnerabilities or human behaviors to penetrate company networks and inflict damage to sensitive data, applications, and workloads. When a cybercriminal detects a weak spot in the system, they use it to gain unauthorized access and install

malware, spyware, or other harmful software. These weak spots are also a

gateway for social engineering attacks, where

individuals become an easier target.

A network security threat can come from the outside or the inside of an organization. Outside threats come from malicious individuals who perform phishing, distributed denial of service (DDoS) attacks, or other network security attacks. On the other hand, inside threats sometimes happen unintentionally, due to an employee's negligence, or purposefully, as a form of revenge or another malicious intent towards the company and its staff.

Network Security Threats Examples

There are many examples of network security threats organizations should watch out for. The list below provides the most common examples:

- **Malware. This threat represents installing malicious software to exploit and disrupt systems without users' knowledge.**
- **Ransomware. This attack encrypts sensitive data belonging to an individual or an organization. Ransomware makes data unreadable until the ransom is paid.**
- **Phishing. This threat works by tricking individuals into sharing sensitive information such as passwords or payment details via deceptive emails or websites.**
- **Man-in-the-middle (MitM) attacks. Man-in-the-Middle attacks intercept online communication between individuals to steal or alter confidential data.**
- **Distributed denial of service (DDoS) attacks. DDoS attacks use compromised devices to flood systems with traffic and exhaust their bandwidth and other resources.**
- **SQL injections. These attacks exploit databases to steal, alter, or delete the information in them.**
- **Zero-day exploits. These exploits are instant attacks on detected hardware or software vulnerabilities before the vendor gets the chance to remediate them.**
- **Insider threats. Insider threats are made by internal members of organizations who abuse their access to sensitive information for malicious agendas.**
- **Drive-by downloads. Drive-by downloads are performed by downloading damaging software to the users' devices without their knowledge to perform attacks.**
- **Credential stuffing. Credential stuffing is abusing previously leaked credentials on multiple platforms expecting that individuals use the same ones on each site.**
- **Social engineering. Social engineering exploits human psychology to get them to share confidential information**

or perform damaging activities to their organization and data.

How to Identify Network Security Threats?

There are many ways to identify network security threats before they happen

. Below are the most common methods:

- Intrusion detection systems (IDS). These systems monitor network traffic for suspicious activities and alerts network administrators.
- Firewall logs. Firewalls log details about traffic, including connection attempts or any anomalies.
- Security information and event management (SIEM) systems. SIEM systems collect and analyze logs from multiple network devices to detect potential attacks.
- Antivirus and antimalware software. This software scans network devices to detect malicious behavior.
- Traffic analysis. This analysis helps detect unauthorized data flows or
- communication with suspicious IP addresses.
- Vulnerability scanning. These scans identify network vulnerabilities to shed light on potential weak spots.
- Penetration testing. These tests simulate real network attacks to check the system's ability to remediate them quickly.
- Behavior analytics. Human behavior is analyzed to determine patterns and deviations from it that might seem suspicious.

How to Prevent Network Security Threats?

Here are the ways to prevent network security threats:

- Regular patching and software updates. System patching and software updates are crucial for preventing threats that become more sophisticated as time passes.
- Using firewalls. Firewalls serve as a barrier between trusted and untrusted networks, which goes a long way in threat prevention.
- Using VPNs. VPNs ensure secure.
- remote access to systems through encryption.
- Implementing multi-factor authentication (MFA). MFA requires several confirmations of identity during logins to prevent unauthorized access.
- Creating regular backups. Organizations should backup all their data for easy recovery in case of data losses.
- Training employees. Employees should take courses and seminars.
- and engage in simulated attacks to ensure they follow the current security policies.
- Defining permissions. Organizations must specify who has access to sensitive information and systems to minimize potential for attacks.
- Using segmented networks. If an attack occurs, network
- segmenting prevents it from spreading to the entire system.

Staying Cyber-Safe

Cyber attackers frequently target networks that businesses rely on in their online operations. By frequently testing security strategies and methods, organizations ensure they.

are up-to-date with the latest network safety and three

Anastazija Spasojevic

Anastazija is an experienced content writer with knowledge and passion for cloud computing, information technology, and online security. At phoenix NAP, she focuses on answering burning questions about ensuring data robustness and security for all participants in the digital landscape.

A network security threat can come from the outside or the inside of an organization. Outside threats come from malicious individuals who perform phishing, distributed denial of service (DDoS) attacks, or other network security attacks. On the other hand, inside threats sometimes happen unintentionally, due to an employee's negligence, or purposefully, as a form of revenge or another malicious intent towards the company and its staff.

Network Security Threats Examples

There are many examples of network security threats organizations should watch out for. The list below provides the most common examples:

- **Malware. This threat represents installing malicious software to exploit and disrupt systems without users' knowledge.**
- **Ransomware. This attack encrypts sensitive data belonging to an individual or an organization. Ransomware makes data unreadable until the ransom is paid.**

- **Phishing. This threat works by tricking individuals into sharing sensitive information such as passwords or payment details via deceptive emails or websites.**
- **Man-in-the-middle (MitM) attacks. Man-in-the-Middle attacks intercept online communication between individuals to steal or alter confidential data.**
- **Distributed denial of service (DDoS) attacks. DDoS attacks use compromised devices to flood systems with traffic and exhaust their bandwidth and other resources.**
- **SQL injections. These attacks exploit databases to steal, alter, or delete the information in them.**
- **Zero-day exploits. These exploits are instant attacks on detected hardware or software vulnerabilities before the vendor gets the chance to remediate them.**
- **Insider threats. Insider threats are made by internal members of organizations who abuse their access to sensitive information for malicious agendas.**
- **Drive-by downloads. Drive-by downloads are performed by downloading damaging software to the users' devices without their knowledge to perform attacks.**
- **Credential stuffing. Credential stuffing is abusing previously leaked credentials on multiple platforms expecting that individuals use the same ones on each site.**
- **Social engineering. Social engineering exploits human psychology to get them to share confidential information or perform damaging activities to their organization and data.**

How to Identify Network Security Threats?

There are many ways to identify network security threats before they happen. Below are the most common methods

- **Intrusion detection systems (IDS). These systems monitor network traffic for suspicious activities and alerts network administrators.**

- **Firewall logs. Firewalls log details about traffic, including connection attempts or any anomalies.**
- **Security information and event management (SIEM) systems. SIEM systems collect and analyze logs from multiple network devices to detect potential attacks.**
- **Antivirus and antimalware software. This software scans network devices to detect malicious behavior.**
- **Traffic analysis. This analysis helps detect unauthorized data flows or communication with suspicious IP addresses.**
- **Vulnerability scanning. These scans identify network vulnerabilities to shed light on potential weak spots.**
- **Penetration testing. These tests simulate real network attacks to check the system's ability to remediate them quickly.**
- **Behavior analytics. Human behavior is analyzed to determine patterns and deviations from it that might seem suspicious.**

How to Prevent Network Security Threats?

Here are the ways to prevent network

security threats:

- **Regular patching and software updates. System patching and software updates are crucial for preventing threats that become more sophisticated as time passes.**
- **Using firewalls. Firewalls serve as a barrier between trusted and untrusted networks, which goes a long way in threat prevention.**
- **Using VPNs. VPNs ensure secure remote access to systems through encryption.**
- **Implementing multi-factor authentication (MFA). MFA requires several confirmations of identity during logins to prevent unauthorized access.**
- **Creating regular backups. Organizations should backup all their data for easy recovery in case of data losses.**

- **Training employees. Employees should take courses and seminars and engage in simulated attacks to ensure they follow the current security policies.**
- **Defining permissions. Organizations must specify who has access to sensitive information and systems to minimize potential for attacks.**
- **Using segmented networks. If an attack occurs, network segmenting prevents it from spreading to the entire system.**
-

Staying Cyber-Safe

Cyber attackers frequently target networks that businesses rely on in their online operations. By frequently testing security strategies and methods, organizations ensure they are up-to-date with the latest network safety and threat protection standards.

(Third week) الاسبوع الثالث

Electronic Banking (E-Banking

Banking) E-banking is defined as the automated) delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels. E-banking includes the systems that enable financial institution customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the Internet or mobile phone. Customers access e-banking services using an intelligent electronic device, such as a personal computer (PC), personal digital assistant (PDA), automated teller machine (ATM), or telephone.

Electronic banking, also known as Electronic Fund Transfer (EFT), uses computer and electronic technology as a substitute for checks and other paper transactions. EFT's are initiated through devices like cards or codes that let you, or those you authorize, access your account. Many financial institutions use ATM or debit cards and Personal Identification Numbers (PIN's) for this purpose. Some use other forms of debit cards such as those that require, at the most, your signature or a scan.

Types of E-banking

The terms 'PC banking', 'online banking', 'Internet banking', 'Telephone banking' or 'mobile banking' refer to a number of ways in which customers can access their banks without having to be physically present at the bank branch. E-banking may be understood as term that covers all these ways of banking business electronically.

Tele-banking service is provided by phone. To access an account, it is required to dial a particular telephone number and there are several options of services.

These options include:

- **Checking account balance.**
- **Funds transfer between current, savings and credit card accounts.**
- **Bill payments.**
- **Stock exchange transaction.**
- **Receive statement via fax.**
- **Loan payment information.**

PC Banking

The increasing awareness of the importance of literacy of computer has resulted in increasing use of personal computers through the entire world. Furthermore, incredible plummet of cost of microprocessor has accelerated the use of computer. The term 'PC banking' is used for banking business transacted from a customer's PC. Using the PC banking or home banking now customers can use their personal computers at home or at their office to access their accounts for transactions by subscribing to and dialing into the banks' Intranet proprietary software system using password.

Internet Banking

Internet banking would free both bankers and customers of the need for proprietary software to carry on with their online banking transactions. Customer behavior is changing rapidly. Now the financial service characterized by individuality, independence of time and place and flexibility. These facts represent huge challenges for the financial service providers. So the Internet is now considered to be a 'strategic weapon' for them to satisfy the ever-changing customers' demand and innovative business needs.

Mobile Banking

Actually mobile banking is a variation of Internet banking. Mobile banking is a good example of how the lines between the various forms of e-banking are becoming gradually blurred. Due to the new transmission technologies such as WAP (Wireless Application Protocol), portable terminal like mobile phones, personal digital assistant (PDA) or small hand-held PCs are providing bank customers with access to the Internet and thus paving the way to Internet banking. It assures immense flexibility and makes the financial services independent of time and place. However, the use of mobile banking is still in a nascent state. The slower transmission speed of the WAP standard and the limited amount of information available are just two of the factors inhibiting the use of those terminals.

Electronic Banking Services

Electronic banking offers several services that consumers may find practical: Automated Teller Machines (ATM) or 24-hour tellers are electronic terminals that let your bank be on transaction almost any time. To withdraw cash, make deposits, or transfer funds between accounts, you generally insert an ATM card and enter your PIN. Some financial institutions and ATM owners charge a fee, particularly to consumers who don't have accounts with them or on transactions at remote .
locations. Generally, ATMs must tell you they charge a fee and its amount on or at the terminal screen before you complete the transaction. Check the rules of your institution and the ATMs you use to find out when or whether a fee is charged.

Direct Deposit

lets you authorize specific deposits, such as paychecks and social security checks, to your account on a regular basis. You also may pre-authorize direct withdrawals so that recurring bills, such as insurance premiums, mortgages, and utility bills, are paid automatically. Be cautious before you pre-authorize direct withdrawals to pay sellers or companies with whom you are unfamiliar; funds from your bank account could be withdrawn fraudulently.

Pay-by-Phone Systems

let you call your financial institution with instructions to pay certain bills or to transfer funds between accounts. You must have an agreement with the institution to make such transfers. Debit Card Purchase Transactions let you make purchases with a debit card, which also may be your ATM card. This could occur at a store or business, on the Internet or online, or by phone. The process is similar to using a credit card, with some important exceptions. While the process is fast and easy, a debit card purchases transfers money — fairly quickly — from your bank account to the company's account. So it is important that you have funds in your account to cover your purchase. This means

you need to keep accurate records of the dates and amounts of your debit Information Systems (card purchases and ATM withdrawals in addition to any checks you write. Also be sure you know the store or business before you provide your debit card information, to avoid the possible loss of funds through fraud. Your liability for unauthorized use, and your rights for error resolution, may differ with a debit card.

Electronic Cheque Conversion

converts a paper cheque into an electronic payment in a store or when a company receives your cheque in the mail. In a store, when you give your cheque to a cashier, the cheque is run through an electronic system that captures your banking information and the amount of the cheque. You're asked to sign a receipt and you get a copy for your records. When your cheque has been handed back to you, it should be voided or marked by the merchant so that it can't be used again. The merchant electronically sends information from the cheque (but not the cheque itself) to your bank or other financial institution, and the funds are transferred into the merchant's account. When you mail-in a cheque for payment to a merchant or other company, they may electronically send information from your cheque (but not the cheque itself) through the system, and the funds are transferred into their account. For a mailed cheque, you should still receive advance notice from a company that expects to send your cheque information through the system electronically.)

Security Considerations in E-Banking Systems

With demanding security regulations throughout the world and increasing amount of valuable services provided using the Internet and other networked media, the assurance of secure and privacy preserving identity authentication became a crucial issue. E-banking risk arises from fraud, processing errors, system disruptions, or other

unanticipated events resulting in the institution's inability to deliver products or services. This risk exists in each product and service offered. Institutions should determine the appropriate level of security controls based on their assessment of the sensitivity of the information to the customer and to the institution and on the institution's established risk tolerance level. There are three major identity authentication approaches: knowledge-based, token-based and biometrics.

Knowledge-based methods

rely on information that only a genuine user is supposed to know, such as passwords or PINs. Token-based authentication requires that the user presents a legitimate token which is provided by a recognized authority. Commonly used tokens are smart cards with built-in microchips which can store a user's personal information, access rights, etc. Biometric authentication requires that a subject possesses a body trait (such as a fingerprint or iris pattern) or is able to reproduce a particular behavioral task (such as a signature or spoken password) that matches the previously stored template, in order to be positively verified.

Electronic Fraud in E-banking systems

The key focus in minimizing electronic fraud is to enable the actual user of the account to be correctly identified. The notion of allowing a card to prove your identity is fast becoming antiquated and unreliable. With this in mind, using biometrics to develop a more accurate identification process could greatly reduce fraud. The main forms of biometrics, which are available today, are:

- **Fingerprinting**
- **Facial recognition**
- **Iris recognition**
- **Voice recognition**
- **Computer recognized hand writing analysis**

Although all of these biometric techniques are accurate ways of identifying people, voice recognition and handwriting analysis do not lend themselves to electronic payments use as easily. Hand writing

styles change over time and, depending on the state the customer (i.e. sober), could easily affect their ability to satisfy the computer of their identity. A similar problem is experienced with voice recognition. If the environment experiences high levels of background noise, the ability to identify the customer becomes more difficult.

Advantages and Potential Difficulties of (Electronic Banking Advantages)

1. For organizations who give their own time it means that they can carry out banking out of working hours in the evenings and at weekends. Customers are able to carry out transactions 24 hours a day, 7 days a week and will no longer be restricted to bank opening hours.

2. Customers can instantly see what is happening with their money rather than waiting for statements to be sent.

3. There is no time spent queuing or journey time to travel to and from the bank for clients or employees of the organization.

4. Electronic banking enables individual branches to have their own local accounts but enables the organizations to access information regarding the bank balances of each branch. This may help the customers to exercise greater control over branch finances and may enable the funds of all the branches to be added together to secure a more favorable rate of interest.

Potential Difficulties

1. Learning curve: Banking sites can be difficult to navigate at first. Plan to invest some time and/or read the tutorials in order to become comfortable in your virtual lobby.

2. Bank site changes: Even the largest banks periodically upgrade their online programs, adding new features in unfamiliar places. In some cases, you may have to re-enter account information.

3. The trust thing: For many people, the biggest hurdle to online banking is learning to trust it. Did my transaction go through? Did I push the transfer button once or twice? Best bet: always print the transaction receipt and keep it with your bank records until it shows up on your personal site and/or your bank statement.

4. For organization or clients that have more than a basic computer banking service there may be a charge for the services of the bank.

5. To use telephone banking there is the cost of the telephone calls to the bank, although these are usually charged at a local rate.

(fourth and fifth week) الاسبوع الرابع والخامس

Common PC Hardware Problems-Solved

Dealing with PC hardware problems can be frustrating, significantly when they hinder our productivity and cause inconvenience. From blank monitors to keyboard malfunctions, and display image distortions, these issues can disrupt our workflow. However, fear not, as we've got you covered! In this article, we'll explore eight common PC hardware problems and provide practical solutions to get your system back on track.

We all know that hardware failure is very common. So after polling nearly two hundred clients, it's not surprising that 99% per cent of them had experienced a hardware failure. But the problem is that during this collapse, they lose data.

Blank Monitors

One of the most unsettling issues is encountering a blank computer monitor when you power on your PC. Before panicking, check the monitor's power supply and connection to the computer. If the issue persists, try connecting the monitor to another computer to identify whether the problem lies with the monitor or the PC. Faulty cables or outdated graphics drivers could be po

tential culprits.

Keys Not Working on the Keyboard

Are some of your keyboard keys unresponsive? This problem could occur due to debris accumulation beneath the keys or a malfunctioning keyboard driver. Try cleaning the keyboard gently using compressed air and update the keyboard driver. If the issue persists, consider replacing the keyboard with a new one.

Mouse Problems

A malfunctioning mouse can significantly hinder your computing experience. If your mouse cursor is freezing or moving erratically, check the mouse's physical condition and its connection to the PC. You may also want to update the mouse driver or try using a different USB port to see if the issue resolves.

Uninstall the USB Port Driver

When multiple USB devices stop working, it might be due to a corrupted USB port driver. Uninstalling the driver and restarting your PC will prompt Microsoft Windows to reinstall the appropriate driver automatically. This simple step can often fix USB-related problems.

Laptop Touchpad Causing the Cursor to Jump Randomly

For laptop and computer users experiencing cursor jumps or erratic movements, disabling the touchpad while typing can be an effective solution. Navigate to your touchpad settings and enable the option to disable the touchpad temporarily when typing

Disable USB Selective Suspend

If your PC encounters issues with USB devices, such as external hard drives disconnecting unexpectedly, the USB Selective Suspend feature might be to blame. Disabling this feature in the Power Options can resolve such complex computer issues.

Display Screen Image Distortion

Distorted images or strange artefacts on the screen can be disconcerting. Check the graphics card connections and ensure that the drivers are up to date. If the problem persists, consider testing the monitor on another personal computer or using a different monitor to isolate the issue.

Keyboard Problems

If your keyboard is typing multiple characters with a single keystroke or repeating keys, adjusting the keyboard repeat rate and delay system hardware settings in Windows can often resolve the problem. Additionally, cleaning the keyboard and ensuring there is no physical damage may help.

Motherboard Problems

The motherboard is the heart of your PC, and when it encounters issues, the entire system can suffer. If you experience frequent crashes before the operating system loads or notice random reboots, it could indicate a problem with the motherboard. Consult a professional technician for a thorough diagnosis and possible repair.

Laptop Speaker Making Static Noises

If your laptop’s speakers produce annoying static or crackling sounds, try updating the audio drivers first. If the issue persists, the speakers may be faulty, and a technician can help with necessary repairs or replacements.

Signs You Need to Call a Professional

Certain hardware issues might require the expertise of a professional. For instance, persistent fan noises, signs of virus infection, or a failing hard disk demand immediate attention from an experienced technician. Don’t hesitate to seek professional help to prevent further damage.

Fan Noises

Noisy fans can be annoying and disruptive. Regularly clean the fans and ensure proper airflow to minimize fan noises. If the noise continues, you may need to replace the fan or consider upgrading to a quieter cooling solution.

PC Fans Not Working Properly

Overheating is a serious concern for PCs, and malfunctioning fans can worsen the problem. Regularly check your PC’s fans for proper functioning, and consider cleaning them to ensure an optimal cooling system.

Signs of Virus Infection

Virus infections can wreak havoc on your PC, causing performance issues, unexpected crashes, and data breaches. Keep your system updated with reliable antivirus software and perform regular scans to detect and remove potential threats.

Apple MacBook Dimmed Screen as a Sign of Motherboard Failure

For MacBook users, a dimmed or blacked-out screen might indicate a problem with the motherboard. Seek assistance from an authorized service center or an Apple-certified technician to diagnose and resolve the issue.

Too Much Pressure on the RAM

Physical pressure on the RAM modules can lead to connection issues, causing your PC to crash or freeze. Make sure the RAM is properly seated and not subject to unnecessary pressure or force.

Keyboard Issues

Keyboard malfunctions, such as keys not registering or sticking, can be caused by dirt or debris between the keys. Carefully clean your keyboard or consider replacing it if the problem persists.

Noisy PC

Unusual grinding or whirring sounds coming from your PC could be a sign of hardware issues. Check your hard drive and fans to identify the source of the noise, and seek professional help if needed.

Fix the Blue Screen of Death

Encountering the dreaded Blue Screen of Death can be alarming. BSD errors often indicate hardware or driver problems. Troubleshoot the issue by updating drivers or performing a system restore.

Noisy Hard Drive

If your hard drive starts making strange noises, it might be failing. Back up your data immediately and consider replacing the hard drive to avoid data loss.

Faulty Hard Disk

A faulty hard disk can lead to data loss and system crashes. If your PC shows signs of a failing hard disk, such as slow performance or frequent error messages, back up your important data immediately. Replacing the faulty hard disk with a new one and restoring your data can prevent further complications.

Blank Monitor

Encountering a blank monitor upon starting your PC can be alarming. Before panicking, ensure that all connections between the monitor and PC are secure. If the issue persists, it may indicate a problem with the graphics card or the monitor itself. Testing the monitor on another PC or trying a different monitor will help identify the source of the problem.

When The Monitor Goes Black After a Few Seconds

If your monitor loses signal and goes black after a few seconds, the issue could be related to the graphics card, monitor settings, or cable connections. Double-check all connections and ensure the monitor settings are correct. If the problem persists, consult a professional technician for further assessment.

How to Fix Mouse Left-click Malfunction in Windows

Mouse left-click malfunctions can hinder your productivity and cause frustration. To fix this issue in Windows, follow these steps:

1. Check Mouse Hardware: Ensure that there are no physical issues with the mouse, such as damaged buttons or loose connections.
2. Update Mouse Driver: Go to Device Manager, locate the mouse under “Mice and other pointing devices,” right-click, and select “Update driver.” Choose the option to search automatically for updated driver software.
3. Roll Back Driver: If the issue started after a driver update, you can roll back to the previous driver version. In Device Manager, right-click the mouse and choose “Properties.” Under the “Driver” tab, select “Roll Back Driver” if the option is available.
4. Check Mouse Settings: Access Mouse Settings in the Control Panel or Settings app and adjust the mouse click settings. Ensure that the left-click function is set to the correct action.
5. Scan for Malware: Malware can cause unexpected behaviour, including mouse issues. Run a full system scan using your antivirus software.
6. Try Another Mouse: If the problem persists, try using a different mouse to determine if the issue is with the hardware or software.

Three Things That Help You To Avoid Common Hardware Problems in Computer

Keep Inside Clean and Clear for Effective Cooling

Overheating is a common problem that can lead to hardware failures. Dust and debris can accumulate inside your PC, obstructing airflow and causing components to overheat. Regularly clean the interior of your PC and ensure that all fans are functioning correctly to maintain effective cooling.

Run Diagnostics

When faced with mysterious PC issues, running diagnostics is often the first step towards identifying the root cause. Most PCs have built-in diagnostic tools that can perform comprehensive tests on hardware components. By analyzing the results, you can pinpoint potential problems and take appropriate action.

Getting a Professional Repair

While some hardware issues are easily resolved, others require the expertise of a professional technician. Don’t hesitate to seek professional help when needed, especially for complex problems like motherboard failures or hard disk issues. A trained specialist can diagnose the problem accurately and provide reliable solutions.

Intech House Advice: How to Avoid Computer Hardware Problems

As technology continues to advance, our dependence on personal computers has grown exponentially. Whether for work, entertainment, or communication, PCs play a vital role in our daily lives. However, encountering hardware problems can disrupt our productivity and cause frustration. In this article, we will provide you with expert advice from Intech House on how to avoid common PC hardware problems and keep your computer running smoothly.

1. Invest in Quality Components:

When building or buying a PC, opt for quality components from reputable manufacturers. Quality components are more reliable, tend to have longer lifespans, and are less likely to encounter hardware failures. While they may come at a slightly higher cost, the peace of mind and reduced risk of issues are well worth it.

1. Properly Install Hardware:

Whether you're upgrading components or assembling a new PC, proper installation is crucial. Follow manufacturer guidelines, use the right tools, and avoid applying excessive force when connecting components. Incorrect installations can lead to physical damage or compatibility issues, causing potential hardware failures.

1. Keep Your PC Clean:

Dust and debris accumulation inside your PC can hinder airflow and cause overheating. Regularly clean the interior of your PC, especially around fans and heat sinks, to prevent hardware components from overheating and potentially failing. Use compressed air to blow away dust gently, and consider investing in dust filters for improved long-term maintenance.

1. Use a Surge Protector:

Power surges and electrical spikes can damage your PC's components, leading to hardware failures. Invest in a good-quality surge protector to safeguard your PC from voltage fluctuations. Surge protectors act as a buffer and can save your PC from potential damage caused by sudden power surges.

1. Keep Your PC Cool:

Overheating is a significant cause of hardware problems. Ensure your PC has proper ventilation and is placed in a well-ventilated area. Consider adding additional cooling solutions, such as case fans or liquid cooling systems, if you engage in resource-intensive tasks like gaming or video editing.

1. Install Reliable Antivirus Software:

Virus infections can wreak havoc on your PC, leading to data loss and system instability. Install reliable antivirus software and keep it up to date to detect and prevent potential threats. Regularly perform full system scans to ensure your PC remains virus-free.

1. Keep Software Updated:

Outdated software, including operating systems and drivers, can cause compatibility issues and impact hardware performance. Regularly update your operating system and hardware drivers to access bug fixes, security updates, and improved compatibility with the latest applications.

1. Properly Shut Down Your PC:

Avoid abrupt power-offs and improper shutdowns, as they can lead to file corruption and hardware damage. Always shut down your PC through the appropriate software options or use the “Shutdown” button in your operating system.

(Sith week) الاسبوع السادس

Introduction

Artificial intelligence (AI) is at the cutting edge of technological development and has the potential to profoundly and incomparably influence humankind's future]. Understanding the consequences of AI is increasingly important as it develops and permeates more facets of society. The goal of this paper is to provide a comprehensive exploration of AI's transformative potential, applications, ethical considerations, challenges, and opportunities.

AI has rapidly advanced, and this progress has deep historical roots. AI has experienced **important turning points and discoveries that have fueled its development from its early beginnings in the 1950s to the present [2]. These developments have sped up the process of developing artificial intelligence on par with that of humans, opening up new avenues for exploration.**

AI comprises a wide range of techniques and technologies, including computer vision, deep **learning, machine learning, and symbolic AI These technologies provide machines the ability to think like humans do by enabling them to perceive, analyze, learn, and make decisions. Understanding the intricacies of these AI systems and their underlying algorithms is essential to appreciate the immense potential they hold.**

AI has a wide range of transformational applications that affect practically every aspect of our life. In healthcare, AI is revolutionizing medical diagnostics, enabling personalized treatments, and assisting in complex surgical]. procedures The transportation sector is witnessing the emergence of autonomous vehicles and intelligent traffic management systems, promising safer and more efficient mobility In finance and economics, AI is reshaping algorithmic trading, fraud detection, and economic forecasting, altering the dynamics of global markets. Moreover, AI is transforming education by offering personalized learning experiences and intelligent tutoring systems, fostering individual growth and enhancing educational outcomes

However, as AI proliferates, it brings with it ethical and societal implications that warrant careful examination. Concerns about job displacement and the future of work arise as automation and AI technologies increasingly replace human labor. Privacy and data security become paramount as AI relies on vast amounts of personal information. Issues of bias and fairness emerge as AI decision-making algorithms can inadvertently perpetuate discriminatory practices. Moreover, the impact of AI on human autonomy raises profound questions about the boundaries between human agency and technological influence

Historical overview of Artificial Intelligence

Artificial intelligence can be traced back to the early dreams of researchers and scientists who wanted to understand and duplicate human intellect in computers. The core concepts of AI were laid during the Dartmouth Conference in 1956, when John McCarthy, Marvin Minsky, Nathaniel Rochester, and Claude Shannon coined the name "Artificial Intelligence" and outlined the goal of building machines that could simulate human intelligence The early development of AI was focused on symbolic AI, which involves employing logical principles and symbolic representations to mimic human reasoning and problem-solving. Early AI systems, such as the Logic Theorist and the General Problem Solver, demonstrated the ability of machines to solve mathematical and logical issues. However, advancement in AI was hampered by the time's low computer capacity and the difficulties of encoding comprehensive human knowledge.

Key milestones in AI research and technological advancements

Over the decades, the field of AI has seen significant milestones and technological achievements. AI researchers made significant advances in natural language processing and knowledge representation in the 1960s and 1970s, establishing the framework for language-based AI systems. These improvements resulted in the 1980s development of expert systems, which used rule-based algorithms to make choices in specific domains. Expert systems have found use in medical diagnosis, financial analysis, and industrial process control. IBM's Deep Blue defeated world chess champion Garry Kasparov in 1997, marking a watershed point in AI's ability to outperform human professionals in strategic thinking. This accomplishment demonstrated the effectiveness of brute-force computing and advanced algorithms in handling challenging tasks.

With the advent of machine learning and neural networks in the twenty-first century, AI research saw a paradigm change. The availability of large datasets and computer resources facilitated neural network training, resulting in advancements in domains such as speech recognition, image classification, and natural language understanding. Deep learning, a subtype of machine learning, transformed AI by allowing systems to create hierarchical representations from data, replicating human brain functions. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) have sped up advances in computer vision and natural language processing. These advancements fueled the development of intelligent virtual assistants like Siri and Alexa, and enabled AI systems to outperform humans in picture recognition and language translation tasks

Definition and scope of AI

AI is a multidisciplinary field that tries to develop intelligent agents capable of executing activities that would normally require human intelligence. Reasoning, problem-solving, learning, perception, and language comprehension are examples of these tasks. AI aims to mimic human cognitive abilities by allowing robots to interpret data, make decisions, and adapt to new settings. AI has a wide range of applications, ranging from simple rule-based systems to powerful deep learning algorithms. While AI has made significant strides in various domains, achieving human-level intelligence, often referred to as Artificial General Intelligence (AGI), remains a formidable challenge.

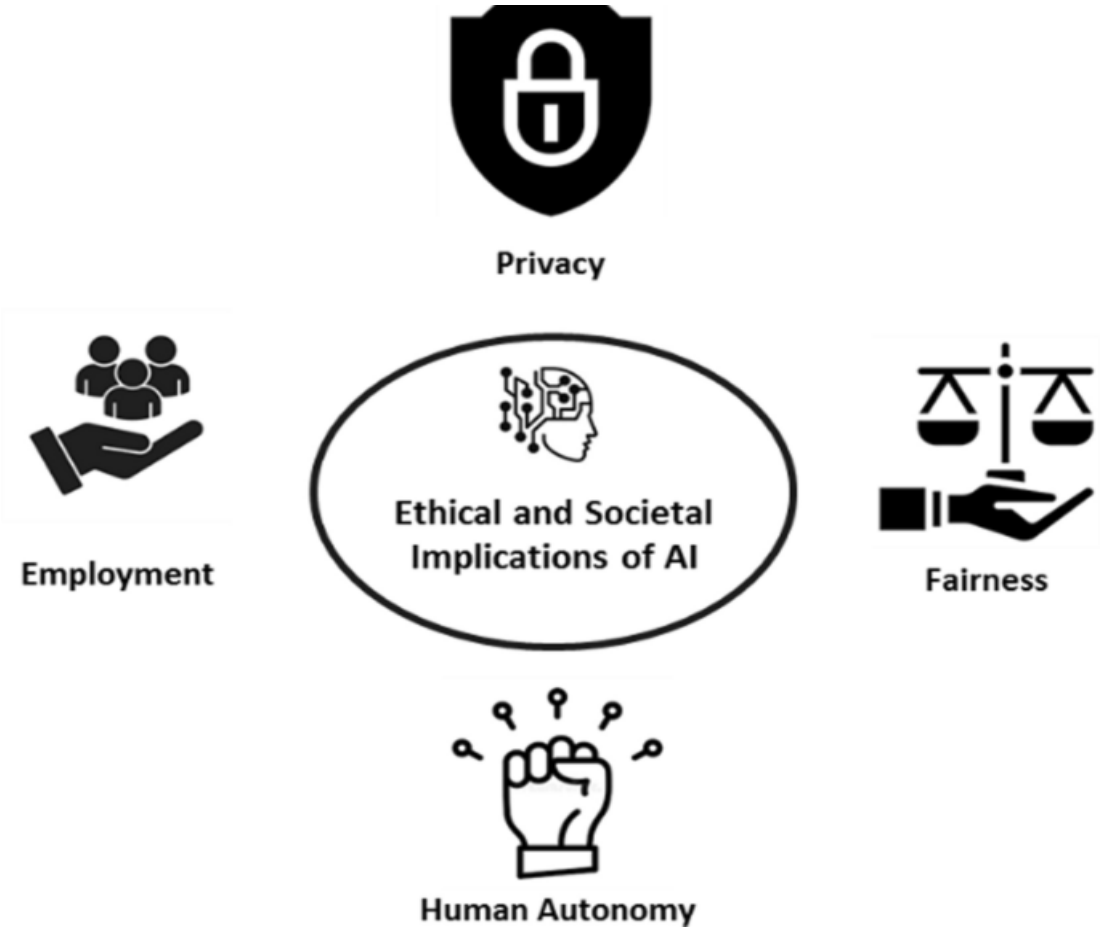
Ethical considerations in AI development and deployment

The rapid advancement of AI raises ethical challenges that require careful consideration. One prominent concern is bias in AI algorithms which can lead to unfair or discriminatory outcomes, especially in domains like hiring and criminal justice. Ensuring transparency and explainability in AI decision-making is essential to build trust and accountability. Privacy and data security are paramount, as AI systems often require large amounts of data to function effectively.

Safeguarding personal information and preventing data breaches are critical aspects of responsible AI deployment. Additionally, the potential impact of AI on employment and societal dynamics necessitates thoughtful planning and policies to ensure a smooth transition and address potential workforce displacement.

Ethical and societal implications of AI

This section investigates the ethical and societal consequences of artificial intelligence. depicts an in-depth examination of the ethical and societal ramifications of AI. This graphic depicts the primary areas of influence, which include employment, privacy, fairness, and human autonomy. Understanding these ramifications is critical for navigating the appropriate development and deployment of AI technology, assuring an ethical and societally beneficial future.



Ethical and societal implications of AI

1 Impact on employment and workforce

Concerns have been raised concerning the influence of AI technologies on jobs and the workforce as they have become more widely adopted. Certain work roles may be vulnerable to displacement as AI-driven automation becomes more ubiquitous, potentially leading to unemployment and economic instability. Routine and repetitive tasks are especially prone to automation, potentially harming industries including manufacturing, customer service, and data input.

2 Privacy, security, and data ethics

The increasing reliance on AI systems, particularly those that utilize vast amounts of personal data, raises critical ethical considerations related to privacy and data ethics []. The responsible and ethical use of data becomes paramount, requiring organizations to ensure informed consent, data anonymization, and stringent data protection measures. The misuse or unauthorized access to personal data by AI systems poses significant risks to individuals' privacy and can lead to various forms of exploitation, such as identity theft and targeted advertising. Furthermore, if AI technologies are not adequately regulated, they may intensify surveillance issues, potentially resulting in infringement of civil liberties and private rights [].

3 Bias, fairness, and transparency in AI systems

AI systems are only as unbiased as the data on which they are trained, and inherent biases in the data might result in biased AI decision-making []. Algorithmic bias can lead to unequal treatment and discrimination, sustaining societal imbalances and strengthening preexisting prejudices.

To address algorithmic prejudice, thorough data curation is required, as is diversity in data representation, as well as constant monitoring and evaluation of AI systems for any biases. Furthermore, guaranteeing justice and openness in AI decision-making is critical for increasing public trust in AI systems..

4 AI and human autonomy

As AI technologies advance, they have the potential to influence human autonomy and decision-making []. AI-powered recommendation systems, personalized marketing, and social media algorithms may impact human behavior, preferences, and views, creating ethical concerns about individual manipulation and persuasion. In the design and deployment of AI systems, striking a balance between improving user experiences and protecting human agency becomes crucial []. Policymakers and technologists must consider the ethical implications of AI-driven persuasion and manipulation and implement safeguards to protect individuals from undue influence. Additionally, AI developers should adopt ethical guidelines that prioritize human autonomy and empower users to make informed choices and maintain control over their digital experiences.

How AI Devices in Daily Life are Transforming Our World

The integration of AI devices in daily life is revolutionizing the way we live, work, and interact with the world around us. From smart home assistants like Amazon Alexa and Google Home to autonomous vehicles and predictive analytics tools, AI technology has become increasingly prevalent in our everyday routines.

The impact of *artificial intelligence devices on our lives* is undeniable, with advancements in machine learning and natural language processing enabling these devices to understand and respond to human interactions in more sophisticated ways than ever before. These AI devices are not only making our lives more convenient and efficient, but they are also helping us to make more informed decisions and improve our overall quality of life.

In this article, we will explore the ways in which AI devices are transforming our world and discuss the implications of their increasing presence in our daily lives. From healthcare to transportation to entertainment, AI technology is reshaping the way we live and interact with technology, and the possibilities for future innovation are endless. If you want to explore the world of AI take a look at the courses at AI Jobs Academy

Understanding Artificial Intelligence in Daily Life

The use of AI has become an integral part of our daily lives, with examples of artificial intelligence being found in various applications. From AI image generators to AI algorithms that power recommendation engines on streaming platforms, there is a wide range of applications of artificial intelligence in everyday life.

One of the best **examples of AI in daily life** is the use of artificial intelligence to help with tasks such as virtual assistants like Siri and Alexa. These virtual assistants use a combination of artificial intelligence and machine learning to provide personalized responses to user queries.

Additionally, popular social media platforms use AI to tailor user feeds based on their preferences, demonstrating the widespread use of **AI in everyday life.** Another example of artificial intelligence in daily life is the use of AI-powered chatbots for customer service interactions. These chatbots are part of the growing trend of using AI to automate tasks and improve efficiency.

Exploring AI in Smart Home Devices

Exploring **AI in smart home devices** has opened up a world of possibilities for homeowners looking to streamline their daily routines. With the integration of artificial intelligence, devices such as smart thermostats, lighting systems, and security cameras can learn and adapt to the habits and preferences of the occupants.

This not only enhances convenience but also leads to increased energy efficiency and overall cost savings. Imagine coming home to a house that has adjusted the lighting and temperature to your liking before you even walk through the door.

These advancements in AI technology in smart home devices are making homes smarter, more efficient, and ultimately more comfortable for those who dwell within. As the technology continues to evolve, the potential for even greater levels of customization and automation in our homes is truly exciting.

.

Enhancing Daily Living with Smart Home AI

Living with smart home technology powered by AI has enabled individuals to enhance their everyday life through the convenience and efficiency it provides. Thanks to AI, tasks such as adjusting temperature settings, turning on lights, and even ordering groceries can now be automated, saving time and energy for homeowners.

The importance of artificial intelligence in smart homes is apparent in the way it learns and adapts to users' preferences, ultimately making their living environment more personalized and comfortable. From controlling appliances to enhancing security measures, everyday life includes a seamless **integration of AI devices in daily life** in various aspects of our daily routines.

With the continuous advancements in AI, the possibilities for improving daily living in smart homes are endless, making it an invaluable tool for modern living.

everyday scenarios. From virtual assistants like Siri and Alexa of AI in to smart devices that use artificial intelligence to predict user preferences, AI is increasingly becoming a staple in our daily routines. These **AI devices in daily life have features** that range from smart home technology to personalized shopping recommendations based on past behaviors.

One of the key future prospects of AI and ML integration in daily life is the ability to personalize and optimize daily tasks. For instance, smart thermostats can adjust temperatures based on user behavior, saving energy and enhancing comfort. AI-powered healthcare devices can monitor vital signs and provide timely alerts for potential health issues, improving overall well-being.

In addition, AI and ML integration in daily life can also enhance productivity and efficiency. Smart cars that use artificial intelligence can optimize routes and driving patterns, reducing commute times and fuel consumption. Virtual assistants can automate routine tasks, freeing up time for more important endeavors.

The future of AI and ML integration in daily life is indeed promising, with endless possibilities for innovative and practical applications that will continue to shape how we live and interact with technology. receive it.

AI applications in various fields

AI's transformative impact extends across healthcare, transportation, finance, and education. This section explores these applications and addresses ethical considerations for responsible AI development and deployment. Figure 1 presents an overview of the wide-ranging applications of AI across

1 Healthcare

The use of AI in healthcare has heralded a new age of revolutionary advances, altering medical procedures and having a profound impact on patient care [2]. Machine learning algorithms are used in AI-powered medical diagnosis and treatment systems to assess massive volumes of patient data, such as medical records, imaging investigations, and genetic information]. These AI technologies can help healthcare personnel make more precise and fast diagnoses by comparing patient data with huge databases and patterns, resulting in earlier disease identification and more effective treatment strategies. Furthermore, AI's ability to process and interpret complex medical pictures, such as MRI and CT scans, has shown outstanding accuracy in detecting anomalies and assisting radiologists in .spotting probable problems that the human eye may ignre

Precision medicine, powered by AI, takes personalization to a new level by tailoring therapies to individual patients' genetic makeup, lifestyle, and medical history. AI algorithms can offer individualized healthcare regimens that maximize treatment efficacy while minimizing adverse effects, resulting in improved patient outcomes and a higher quality of life.

AI-assisted robotic surgeries represent another milestone in healthcare AI applications. Advanced robotic systems, guided by AI algorithms, assist surgeons during surgical procedures by providing real-time insights, enhanced dexterity, and precision These AI-driven robotic assistants can make surgery less invasive, reducing trauma to patients, shortening recovery times, and minimizing the risk of complications. The integration

of AI into surgical workflows has significantly raised the bar for surgical precision, resulting in superior patient care and expanded surgical capabilities.

2 Finance and economics

The impact of AI on the financial and economics sectors has been tremendous, with significant changes in established processes and the introduction of creative solutions Algorithmic trading powered by AI has transformed financial markets, enabling faster and more data-driven decision-making. Machine learning algorithms automatically evaluate market data, discover patterns, and execute trades, resulting in better investing strategies and more efficient capital allocation. AI-powered trading systems can react to market movements and quickly adjust trading positions, improving trading results and portfolio performance.

AI's contribution to risk assessment and fraud detection in the financial sector has been critical in guaranteeing the security and integrity of financial transactions In real-time, machine learning algorithms may evaluate historical transaction data, find aberrant trends, and flag potentially fraudulent actions. By continuously learning from new data, these AI systems can react to evolving fraud tendencies and increase the resilience of financial institutions against fraudulent threats.

With the incorporation of AI technology, economic forecasting and predictive analytics have also seen considerable breakthroughs []. To provide more accurate forecasts and insights, AI-powered models may process large and diverse datasets such as economic indicators, consumer behavior, and macroeconomic factors. AI-driven economic projections can help policymakers and businesses make educated decisions, plan resource allocation, and adapt proactively to changing economic situations, resulting in more stable and resilient economies.

3 Education

AI is altering the educational landscape by bringing creative solutions to improve student learning experiences and outcomes [7, 9]. Artificial intelligence-based adaptive learning systems use data analytics and machine learning algorithms to assess individual students' strengths and weaknesses in real time. Adaptive learning platforms generate tailored learning pathways by adapting instructional content to each student's unique learning pace and preferences, increasing engagement and information retention. Targeted interventions, interactive courses, and timely feedback can help students improve their academic performance and gain a deeper grasp of subjects.

Intelligent teaching systems are yet another advancement in educational AI [25]. These systems use natural language processing and machine learning to provide students with tailored teaching and support. Intelligent tutoring systems, which can recognize and respond to students' inquiries and learning demands, provide personalized advice, promote self-directed learning, and reinforce concepts through interactive exercises. This individualized learning experience not only improves students' academic performance, but it also instills confidence and motivation to pursue interests further.

AI is also important in measuring learning outcomes and educational analytics [26]. AI algorithms can provide significant insights into learning patterns, instructional efficacy, and curriculum design by evaluating massive amounts of educational data, including student performance indicators and assessment results. These data-driven insights can be used by educational institutions and policymakers to optimize educational

programs, identify areas for development, and create evidence-based policies that encourage improved educational results.

Transportation

The transportation sector is undergoing a revolutionary transformation driven by AI applications. One of the most anticipated breakthroughs is the development of autonomous vehicles and self-driving technologies []. AI algorithms, together with advanced sensors and cameras, enable vehicles to navigate complex traffic environments autonomously. By continuously processing real-time data, AI-equipped self-driving cars can detect and respond to obstacles, traffic signals, and pedestrian movements, significantly reducing the likelihood of accidents caused by human errors. The potential impact of autonomous vehicles extends beyond enhancing road safety; it holds the promise of alleviating traffic congestion, optimizing energy consumption, and enabling seamless transportation for the elderly and disabled populations.

Intelligent traffic management systems powered by AI offer promising solutions to tackle traffic congestion and enhance overall transportation efficiency These AI systems can optimize traffic flow, identify congestion hotspots, and dynamically alter traffic signal timings to cut wait times by collecting data from numerous sources such as traffic cameras, GPS devices, and weather conditions. Smart traffic management has the potential to improve urban mobility while also lowering carbon emissions and promoting sustainable transportation.

AI is also important in optimizing logistics and transportation networks []. AI algorithms can optimize supply chain operations, cut transportation costs, and enhance delivery times by evaluating massive volumes of data on shipping routes, cargo loads, and transportation timetables. Furthermore, AI's predictive capabilities allow organizations to more efficiently forecast demand variations and plan inventory management, decreasing waste and improving overall operational efficiency.

marketing

.

The current study aimed to identify the impact of the use of artificial intelligence means on the development of digital marketing, due to the recent development in information and communication technology, and the need to reach a high degree of quality digital marketing, and with the development of artificial intelligence methods that have been used and spread in many applications. The most important of which are social networking applications, and just as artificial intelligence can identify the customer through speech, chat, logical analysis of big data, and providing advice, it can be useful in e-marketing through (e-mail, search engines and chatbots), and therefore the researcher saw It can be useful in the quality of digital marketing for dairy products, and the study sample consisted of (350) who work in companies (Juhayna - Almarai - Lamar). Selling, where, through artificial intelligence, the features of automatic response are available that allow communication at any time and from anywhere, which achieves interactivity, and artificial intelligence means provide an advantage for e-mail. Which confirmed the importance of using it in digital marketing, as it provides the feature of automatic response, notifications and interests, and the study recommended that dairy companies expand the use of artificial intelligence applications in electronic marketing, which contributes to increasing sales and .achieving competitive advantage

•

Key Benefits of AI and Robotics in Finance

1. **Enhanced Efficiency and Productivity**: AI and robotics streamline operations by automating repetitive tasks, reducing manual errors, and increasing overall productivity. For example, robotic process automation (RPA) can handle high-volume, routine tasks such as data entry, reconciliations, and compliance reporting, freeing up human employees to focus on more strategic activities.

2. **Improved Decision-Making**: AI algorithms analyze vast amounts of data to identify patterns and trends that human analysts might overlook. This capability enables more informed decision-making in areas such as investment management, fraud detection, and credit scoring. Machine learning models can continuously learn and adapt, enhancing their predictive accuracy over time.

3. **Personalized Customer Experiences**: AI-driven chatbots and virtual assistants provide customers with personalized financial advice, 24/7 support, and seamless service experiences. By leveraging natural language processing (NLP) and sentiment analysis, these tools can understand and respond to customer inquiries more effectively.

4. **Risk Management and Fraud Detection**: AI and robotics enhance risk management by identifying potential risks and anomalies in real-time. Machine learning models can detect unusual patterns indicative of fraud or cyber threats, enabling proactive measures to mitigate risks. Additionally,

AI can assist in stress testing and scenario analysis to ensure financial stability.

Use Cases of AI and Robotics in Finance

1. **Algorithmic Trading**: AI-powered algorithms are revolutionizing trading by executing trades at high speeds and volumes, leveraging real-time market data and sophisticated strategies. Algorithmic trading minimizes human intervention, reduces latency, and increases trading efficiency. In 2020, algorithmic trading accounted for approximately 60-73% of overall U.S. equity trading volume.

2. **Robo-Advisors**: Robo-advisors use AI algorithms to provide automated, personalized investment advice to clients. These platforms consider individual risk profiles, financial goals, and market conditions to create and manage investment portfolios. By 2025, the global robo-advisory market is projected to reach $1.2 trillion in assets under management.

3. **Credit Scoring and Lending**: AI models analyze a wide range of data points, including credit history, social media activity, and transaction behavior, to assess creditworthiness more accurately. This approach allows financial institutions to extend credit to a broader range of customers while minimizing default risks.

4. **Regulatory Compliance**: Regulatory technology (RegTech) leverages AI and robotics to automate compliance processes, monitor transactions for suspicious activities, and ensure adherence to regulatory requirements. AI can scan and analyze vast amounts of regulatory texts, flagging potential compliance issues and reducing the burden on compliance teams.

Future Trends in AI and Robotics in Finance

1. **Explainable AI**: As AI becomes more integral to financial decision-making, there is a growing need for explainable AI (XAI) that provides transparent and interpretable insights. XAI helps build trust and ensures regulatory compliance by explaining the reasoning behind AI-driven decisions.

2. **AI-Powered Predictive Analytics**: Predictive analytics will play a crucial role in forecasting market trends, identifying investment opportunities, and optimizing financial strategies. AI models will continue to evolve, incorporating more diverse data sources and delivering increasingly accurate predictions.

3. **Advanced Robotics in Customer Service**: The future of customer service in finance will see the integration of advanced robotics capable of understanding and responding to complex customer queries. These robots will leverage AI, NLP, and computer vision to provide human-like interactions and support.

4. **AI-Driven Risk Management**: AI will enhance risk management practices by providing real-time risk assessments, stress testing, and scenario analysis. Financial institutions will rely on AI to anticipate and mitigate emerging risks, ensuring financial stability and resilience.

الأسبوع الثالث عشر

(Thirteen-week)

International Relations

Introduction

Technological development has always been one of the most important enabling tools that rearrange the shape of international relations, as it affects the development of states' capabilities to coerce others, and gives states the advantage of leadership in rearranging the hierarchy of international power and reorganizing the procedures, regulations and laws that govern the relationship between international environmental actors.

Challenges, risks, and regulation of Artificial Intelligence

The challenges, risks, and regulation of AI. It explores an overview concern related to superintelligence, transparency, unemployment, and ethical considerations. Understanding these complexities is vital for guiding responsible AI development and governance.

1 Superintelligence and existential risks

As AI technologies advance, the prospect of creating Artificial General Intelligence (AGI) or superintelligent systems raises existential risks [. Superintelligence refers to AI systems that surpass human intelligence across all domains, potentially leading to unforeseen and uncontrollable consequences. To avoid disastrous outcomes, it is vital that AGI is developed with rigorous safety mechanisms and is linked with human values. The fear is that AGI will outpace human comprehension and control, resulting in unanticipated acts or decisions with far-reaching and irreversible repercussions. To solve this, researchers and governments must engage in AGI safety research and form worldwide partnerships to construct governance structures that prioritize the safe and responsible development of AGI.

2 Lack of transparency and accountability in AI systems

One of the major issues in AI is the lack of transparency and accountability in the decision-making processes of AI systems [30]. Complex AI systems, such as deep neural networks, can be difficult to analyze and explain, giving rise to the "black box" AI problem [16]. This lack of transparency raises worries about possible biases, errors, or discriminatory effects from AI judgments. Researchers and developers must focus on constructing interpretable AI models that can provide explicit explanations for their actions in order to establish confidence and ensure the responsible usage of AI. Furthermore, building accountability frameworks that hold businesses and developers accountable for AI system outcomes is critical in addressing potential legal and ethical repercussions.

3 Unemployment, socioeconomic disparities, and the future of work

The rapid deployment of AI-driven automation has ramifications for employment and social inequities. As AI replaces certain job roles and tasks, there is a possibility of job displacement, leading to unemployment and income inequality [28]. Low-skilled workers in industries highly susceptible to automation may face the most significant challenges in transitioning to new job opportunities. Addressing these challenges requires a multi-faceted approach, including retraining and upskilling programs, social safety nets, and policies that promote job creation in emerging AI-related sectors. Additionally, measures such as universal basic income and shorter workweeks have been proposed to alleviate the potential socioeconomic impact of AI-driven automation on the workforce.

4 Ethical, legal, and regulatory considerations for AI development and deployment

The rapid advancement of AI technologies has outpaced the development of comprehensive ethical, legal, and regulatory frameworks [33]. Ensuring that AI is developed and deployed responsibly and ethically is crucial to avoid potential harm to individuals and society at large. Ethical considerations include addressing algorithmic bias, ensuring fairness, and safeguarding privacy and data rights. Legal and regulatory considerations encompass liability issues, data protection laws, and intellectual property rights related to AI systems. The need for international cooperation in

formulating AI governance frameworks is paramount, as AI's impact transcends national boundaries. Policymakers, industry stakeholders, and experts must work collaboratively to establish guidelines and standards that promote the ethical development and use of AI technologies while striking a balance between innovation and protecting the common good.

In conclusion, while AI technologies hold immense promise, they also present significant challenges and risks that must be addressed proactively and responsibly. Superintelligence and existential risks demand focused research and governance to ensure AGI development is aligned with human values. The lack of transparency and accountability in AI systems necessitates efforts to create interpretable and accountable AI models. The potential impact of AI-driven automation on employment and socioeconomic disparities requires comprehensive policies and safety nets to support workforce transitions. Ethical, legal, and regulatory considerations are vital in fostering the responsible development and deployment of AI while balancing innovation with societal well-being. By addressing these challenges and risks collectively, we can harness the transformative potential of AI while safeguarding the welfare of humani

The Ethical Considerations of Artificial Intelligence

Artificial intelligence is progressing at an astonishing pace, raising profound ethical concerns regarding its use, ownership, accountability, and long-term implications for humanity. As technologists, ethicists, and policymakers look at the future of AI, ongoing debates about the control, power dynamics, and potential for AI to surpass human capabilities highlight the need to address these ethical challenges in the present. With the White House recently investing $140 million in funding and providing additional policy guidance, significant steps are being taken to understand and mitigate these challenges to harness AI's immense potential.

. _____

Bias and Discrimination

AI systems are trained on massive amounts of data, and embedded in that data are societal biases. Consequently, these biases can become ingrained in AI algorithms, perpetuating and amplifying unfair or discriminatory outcomes in crucial areas such as hiring, lending, criminal justice, and resource allocation. For example, if a company uses an AI system to screen job applicants by analyzing their resumes, that AI system was likely trained on historical data of

successful hires within the company. However, if the historical data is biased, such as containing gender or racial biases, the AI system may learn and perpetuate those biases, thus discriminating against candidates who don't match the historical hirings of the company. Several U.S. agencies recently issued warnings about how they intend to push back against bias in AI models and hold organizations accountable for perpetuating discrimination through their platforms.

Transparency and Accountability

AI systems often operate in a "black box," where these systems offer limited interpretability of how they work and how they arrived at certain decisions. In critical domains like health care or autonomous vehicles, transparency is vital to ascertain how decisions are made and who bears responsibility for them. Clarifying accountability is particularly important when AI systems make errors or cause harm, ensuring appropriate corrective actions can be taken. To combat the black box challenges, researchers are working to better develop explainable AI, which helps characterize the model's fairness, accuracy, and potential bias.

Creativity and Ownership

When a painter completes a painting, they own it. But when a human creator generates a piece of digital art by entering a text prompt into an AI system that was programmed by a separate individual or organization, it's not so clear. Who owns the AI-generated art? Who can commercialize it? Who is at risk for

infringement? This emerging issue is still evolving as AI advances faster than regulators can keep up. As human creators generate digital art through AI systems developed by others, it remains critical that lawmakers clarify ownership rights and provide guidelines to navigate potential infringements.

Privacy, Security, and Surveillance

The effectiveness of AI often hinges on the availability of large volumes of personal data. As AI usage expands, concerns arise regarding how this information is collected, stored, and utilized. For example, China is using tools like facial recognition technology to support their extensive surveillance network, which critics argue is leading to discrimination and repression of certain ethnic groups. In AI, preserving individuals' privacy and human rights becomes paramount, necessitating robust safeguards against data breaches, unauthorized access to sensitive information, and protections from extensive surveillance.

and inclusivity in development, and fostering ongoing discussions are integral to responsible AI deployment. By proactively engaging with these concerns, we can harness the incredible potential of AI while upholding ethical principles to shape a future where socially responsible AI is the norm.

Future technology trends

Technological change is set to have profound impacts over the next 10-15 years, widely disrupting economies and societies. As the world faces multiple challenges, including ageing, climate change, and natural resource depletion, technology will be called upon to contribute new or better solutions to emerging problems. These socioecological demands will shape the future dynamics of technological change, as will developments in science and technology.

This chapter discusses ten key or emerging technologies that are among the most promising and potentially most disruptive and that carry significant risks. The choice of technologies is based on the findings of a few major foresight exercises carried out in recent years. The ten technologies are as follows: the Internet of Things; big data analytics; artificial intelligence; neurotechnology's; nano/microsatellites; nanomaterials; additive manufacturing; advanced energy storage technologies; synthetic biology; and blockchain. The chapter describes each technology in turn, highlighting some of its possible socioeconomic impacts and exploring related policy issues. A final section highlights some common themes across the ten technologies.

Introduction

Technological change is a significant megatrend in its own right, constantly reshaping economies and societies, often in radical ways. The scope of technology – in terms of its form, knowledge bases and application areas – is extremely broad and varied, and the ways it interacts with economies and societies are complex and co-evolutionary. These conditions create significant uncertainty about the future directions and impacts of technological change, but also offer opportunities for firms, industries, governments and citizens to shape

technology development and adoption. Various types of technology assessments, including trend analyses, evaluations, forecasts and foresight exercises, can provide helpful inputs in this regard. Technological forecasting has been widely practiced in the worlds of business, public policy, and R&D management since the 1950s. Its goal is to predict with the greatest accuracy possible technological trajectories and their impacts.

The Internet of Things

The Internet of Things (IoT) promises a hyper-connected, digitally responsive society that will have a profound impact on all sectors of the economy and society. While it has great potential to support human, societal and environmental development, several safeguards need to be put in place to ensure data protection and security.

The Internet of everything

IoT comprises devices and objects whose state can be altered via the Internet, with or without the active involvement of individuals (OECD, 2015a). The term goes beyond devices traditionally connected to the Internet, like laptops and smartphones, by including all kinds of objects and sensors that permeate the public space, the workplace and homes and that gather data and exchange these with one another and with humans..

Further development of the IoT is challenged by high ICT-related costs and emerging skills needs

How fast and how effectively the IoT will evolve over the next 15 years depends to a large extent on the roll-out of fixed and mobile broadband and the decreasing cost of devices (OECD, 2015a). In addition, in order to optimize the potential of the IoT, business and government will have to build capacity to process the large amounts and variety of data that are produced. The large volume of data generated by the IoT is of little value if information cannot be extracted and analyzed.

In particular, research systems and the healthcare sector are set to benefit

Increasing access to public science has the potential to make the entire research system more effective and productive by reducing duplication and the costs of creating, transferring and re-using data; by allowing the same data to generate

more research, including in the business sector; and by multiplying opportunities for domestic and global participation in the research process (OECD, 2014a). The rise of open data and open access policies and infrastructures is already making isolated scientific datasets and results part of big data. The number of stakeholders involved in research practices and policy design will continue to increase, making science a citizen endeavour, reinforcing a more entrepreneurial approach to research and encouraging more responsible research policies.

Big data analytics offers the potential of bringing substantive improvement to different dimensions of healthcare, including patient care, health systems management, health research and the monitoring of public health (OECD, 2015b). Sharing health data through electronic health record systems can increase efficient access to healthcare and provide novel insights into innovative health products and services (OECD, 2013a). The diagnosis, treatment and monitoring of patients may become a joint venture between analytical software and physicians. Clinical care may become more preventive in nature, as monitoring and predictive analytics help discover pathologies early on. On top of open research data, the IoT will enable a plethora of health-related data on both sick and healthy people that could serve as valuable research input and bring advances to medicine. Broad data on healthcare utilization could be put together with deep clinical and biological data, opening new avenues to advance common knowledge, such as on ageing-related diseases, or to support interdisciplinary research, for instance, on the combined effects of cure and care (Anderson and Oderkirk, 2015).

Part 1: Computer Networks

1. What is the main difference between the Internet and an Intranet? Provide an example for each.
2. Briefly explain the function of each of the following devices in a network:
    - Switch
    - Router
    - Wireless Access Point
3. What is an IP Address, and what is its purpose in computer networks?
4. Compare Ethernet (wired) and Wi-Fi (wireless) cables in terms of their advantages and disadvantages for a home or office network environment.

Part 2: Artificial Intelligence (AI)

1. What is the general definition of Artificial Intelligence (AI)? Name two fields where AI is currently applied.
2. Briefly explain the concept of Machine Learning as a subfield of Artificial Intelligence.
3. Give an example of an AI application you use in your daily life, and explain how it relies on AI.
4. What is a Robot, and how is it related to Artificial Intelligence?
5. What ethical or societal challenges might arise from the rapid development of Artificial Intelligence? Name one challenge.
6. What is the difference between Narrow AI (Weak AI) and General AI (Strong AI)?

Part 3: Computer Troubleshooting

1. Your computer is not turning on at all after pressing the power button. Name two basic steps you would check as part of the troubleshooting process.
2. If a computer is running very slowly, name three possible causes for this issue and three potential solutions.
3. Persistent "Low Memory" error messages appear on the computer. What can you do to resolve this problem?

Suggested Books

l. Graham Brown, David Watson, "Cambridge IGCSE Information and Communication
Technology", 3rd Edition (2020)

2. Alan Evans, Kendall Martin, Mary Anne Patsy, "Technology In Action Complete" , 16th Edition (2020).
3. Ahmed Banafa, "Introduction to Artificial Intelligence (Al)", 1st Edition (2024)

ومن الله التوفيق