Vidyalankar School of Information Technology

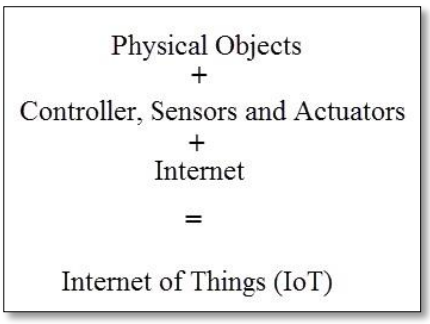
Internet of Things

University Exam Question Solution

UNIT I

1.	**Define and explain the Internet of Things. (Oct 2018) (May 2019) (Nov 2022)**

Internet of Things:



- **Physical Objects -** Thing is a word used to refer a physical object, an action or idea, a situation or activity in case when one does not wish to be precise.

- **Controller, Sensors and Actuators –** It's an embedded systems consists of different types of sensors, actuators and microcontrollers.
  - **Sensors:** The main purpose of sensors is to collect data from the surrounding environment.
  - **Actuators:** An actuator is a machine component or system that moves or controls the mechanism or the system.
  - **Controllers:** Microprocessors or Microcontrollers process the information collected by sensors and send the desired output to actuator.

- **Internet -** IoT devices will need connectivity to the controllers that will be controlling the devices. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing internet infrastructure.

- **Examples –**
  - **Smart Alarm:** The alarm can check the train times online, and if it finds train delayed, so it lets you sleep in a little longer.

  - **Smart Bus Stop:** The bus stop has large LCD display that can flash which bus is due. Every bus has GPS tracking its location, they simply connect to the bus company's online service and always give the updated information.

2	**"Any sufficiently advanced technology is indistinguishable from magic". Discuss. (Oct 2018) (May 2023)**
	• Magic like technology has evolved to meet our needs and desires. The objects in folktales and fairy tales are often wish fulfilment fantasies to fill the deepest desires. • From the point of view of a Silicon Valley entrepreneur and technologist, David Rose has talked about Enchanted Objects at TEDx Berkeley and has categorised various objects drawn from fairy tales and fantasy literature in ways that apply as much to technological objects. • For Protection, just as magical swords and helmets protected the protagonists of fairy tales from their enemies, so has much of the development of science and technology throughout history been driven by the need for military superiority, for the purpose of security or conquest. • Health has been a driver for many quests to find an ingredient for a health potion and for research into various branches of medicine, pharmacology and surgery, physiotherapy, and diet. • Humans have always desired Omniscience, from Snow White's wicked stepmother asking, "Mirror mirror on the wall, who's the fairest of them all?" to the friends settling an argument of fact by looking up articles from Wikipedia on their smartphones. • Human Connection, even when one's loved ones are far away, is an urgent, aching need: the Finnish hero's family know that he has been hurt when the enchanted comb that he left on the mantelpiece starts to bleed. Similarly, the postal service, telephones, and social networking help keep us in touch with our family and friends. • The ancient storytellers yearning for Effortless Mobility invented seven-league boots, flying carpets, and even teleportation. Through technology, we have invented cars and railways, bicycles, and aeroplanes. The need for Creative Expression is fulfilled in stories by the enchanted paintbrushes or magic flutes and harps, while we have always used technology to devise such creative outlets, from charcoal to paint to computer graphics, or from drums to violins and electronic synthesisers.
3	**Explain calm and ambient technology using example of Live wire. (Oct 2018) (May 2019) (Nov 2022) (May 2023)**
	• The IoT has its roots in the work done by **Mark Weiser** at Xerox PARC. The work he did was not assumed that there would be network connectivity but focused more on how the system would look when the objects would be integrated this term is said to be ubiquitous computing. • **Ambient** term has nothing related with foreground but is present in background.

	• **calm technology**—systems which don't vie for attention yet are ready to provide utility or useful information when we decide to give them some attention. • Major issues for designing such systems are configuration, how to provide power to all these items, how they talk to each other, and how they communicate with us • **Configuration and user interaction** are difficult problems to solve with just technical solutions. This is where good design and usability comes into Picture • A great example is **Live Wire**, one of the first Internet of Things devices. - Live Wire which is known as Dangling String. - It is a simple device: an electric motor connected to an eight-foot-long piece of plastic string. - The power for the motor is provided by the data transmissions on the Ethernet network to which it is connected, so it twitches whenever a packet of information is sent across the network. - Under normal, light network load, the string twitches occasionally. - If the network is overloaded, the string whirls madly, accompanied by a distinctive noise from the motor's activity. - Conversely, if no network activity is occurring, an unusual stillness comes over the string. - Both extremes of activity therefore alert the nearby human.
4	**What is manufactured normalcy field? Explain. (Oct 2018) (Nov 2019)**
	• Technology adoption isn't solely dependent on a device's capabilities but also on society's readiness to embrace it. Oftentimes, the difference between a technology's failure and its widespread success is the timing of its introduction, aligning with people's evolving acceptance of it. • Tech blogger Venkatesh Rao coined a term to explain this phenomenon, known as the "manufactured normalcy field." This concept suggests that we often fail to perceive the changes in our present world as they happen; significant technological advances can subtly emerge over time, essentially hidden in plain sight. • The manufactured normalcy field represents the threshold a technology must cross to be adopted by society. In other words, it needs to integrate seamlessly into the everyday routines and expectations of individuals. A successful user-experience designer should provide an experience that doesn't challenge users' existing norms significantly, even if the underlying technology is remarkably advanced. • For instance, the mobile phone's initial introduction didn't aim to redefine the very concept of communication. Instead, it was introduced as a phone without the constraints of a fixed location. Gradually, it evolved into a portable Internet terminal, capable of diverse tasks beyond mere calls. The key to this successful transformation was the use of the familiar phone metaphor. This approach leverages the fact that people tend to embrace new technology more readily when it's presented in terms of something they already understand.

	• In the context of the Internet of Things (IoT), some projects take inspiration from the world of magic and fairy tales, where everyday objects are filled with semi-hidden, enchanting capabilities. For example, the WhereDial, a project inspired by the clock in Harry Potter, uses GPS technology and location services to display family members' whereabouts, albeit without the magic, offering a real-world touch of enchantment to ordinary objects.
5	**Differentiate between static IP address and Dynamic IP address. (Oct 2018) (Nov 2022)**
	Static IP address: • A static IP address is an address that is permanently assigned to you by your ISP and does not change even if your computer reboots. • A static IP address is usually assigned to a server hosting website, and providing email, database and FTP services. • A static IP address is also assigned to a commercial leased line, or public organization requiring same IP address every time. • Since static IP address is assigned to you, you'll have to manually configure your machine (router or server) to use the static IP address assigned to you. • **Advantages:** - Address does not change good for web servers, email servers and other Internet servers. - Use DNS to map domain name to IP address and use domain name to address the static IP address. - Similar can be achieved with Dynamic DNS for dynamic IP address, but it's not as clean as the static IP address. • **Disadvantages**: - Expensive than dynamic IP address - ISPs generally charge additional fee for static IP addresses. - Need additional security - Since same IP is assigned to a machine, hackers try brute force attack on the machine over period of time. **Dynamic IP address:** • A dynamic IP address is an IP address dynamically assigned to your computer by your ISP. • Each time your computer (or router) is rebooted, your ISP dynamically assigns an IP address to your networking device using DHCP protocol. • Since your ISP dynamically assigns an IP address to a computing device on reboot, your device may not always receive the same IP address previous assigned to it. • Even if your machine is always on and permanently connected, some ISPs do change IP address on-the-fly even though this is very rare. • A sticky nature of DHCP generally reassigns same IP address to the same machine, it is not guaranteed to receive same IP address as IP pool may exhaust at times and lease time may expire. • **Advantages:** - Cheaper than static IP address. - Changing IP address gives more privacy. • **Disadvantages:**

	- Requires DHCP server to obtain an IP address. - Non-static. Each time IP address changes, you may have to find you IP address again.
6	**Define protocol. Explain the following application layer protocols: HTTP, HTTPS, SMTP, FTP,POP3, IMAP. (Oct 2018) (May 2023)**
	• **Protocol:** - A protocol is a set of rules and guidelines for communicating data. - Rules are defined for each step and process during communication between two or more computers. - Networks must follow these rules to successfully transmit data. • **HTTP:** - The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. - HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access. • **SMTP:** - Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (email) transmission. • **FTP:** - The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a client and server on a computer network. • **POP3:** - Post Office Protocol, version 3 is an email retrieval protocol used for receiving email messages from a mail server. - It's a simple and widely used method for accessing email from a remote server. • **IMAP:** - Internet Message Access Protocol is an email retrieval and synchronization protocol used for accessing and managing email messages stored on a mail server. - Unlike POP3, it allows users to manage their email messages on the server.
7	**What is MAC (Media Access Control) address? Explain. (May 2019)**
	• Every network-connected device, in addition to having an IP address, is assigned a unique MAC address. It plays a crucial role in distinguishing and addressing devices on the same physical network, enabling them to exchange data packets. This function is associated with the lowest-level "link layer" in the TCP/IP networking model. • MAC stands for Media Access Control. It serves as a hardware address that uniquely identifies a device on a network. • A MAC address is a 48-bit number, often expressed as six groups of hexadecimal digits (0-9 and A-F). Colons or hyphens separate these groups. For example: "01:23:45:67:89:ab." • MAC addresses are globally unique, meaning no two devices should have the same MAC address. This uniqueness ensures that networked devices can be accurately identified.

	• MAC addresses are primarily used within a specific Ethernet network, such as a home network, and are not typically utilized beyond the local network or your home router. • MAC addresses play a vital role in the physical routing of data packets within a network. When an IP message is transmitted across the internet, it passes through various nodes and routers. When it reaches a node that knows the location of the intended device, it uses the corresponding MAC address to deliver the message to the correct physical machine. • Most networked devices, like laptops, come with their MAC addresses hard-coded into their Ethernet chips. This ensures the uniqueness of each device. • Some chips, like the one used in the Arduino Ethernet, don't have built-in MAC addresses. Instead, a MAC address sticker may be provided. While it may seem unconventional, it serves a purpose. This MAC address is reserved and guaranteed to be unique.
8	**Discuss the issue of Privacy in Internet of Things. (May 2019)**
	• The Internet of Things devices that we own aren't the only ones that should concern us when it comes to matters of trust. • With more sensors and devices connected and reporting data to the Internet, the privacy of third parties who cross sensors' paths is an important consideration. • **Keeping Secrets** - Privacy concerns are an obvious issue, even seemingly innocuous applications can leak personal information, so one should be alert to the danger and take measures to avoid it. - Don't share more than you need to provide the service. - If you can avoid gathering and/or storing the data in the first place, you need not worry about disclosing it accidentally. • **Hashing:** - The most common use of cryptographic hashes is in password verification. - When the user wants to authenticate, the hash can be recalculated. - If it matches the password is correct. - Adding salt to the password before applying the hash would give some more features. - This adds some random, non-secret extra text to the password before the hash is computed. The salt is then stored with the hash, so the service can concatenate the two again when it needs to verify a newly presented password. - The salt prevents any attacker who ends up with a copy of the hash from easily comparing it to a dictionary of precompiled hashes to work out the password.
9	**Write the working of IP Protocol. (May 2019)**
	• The Internet Protocol (IP) is a foundational component of the broader suite of networking protocols known as TCP/IP. TCP/IP represents a stack of protocols, with each layer building upon the capabilities of the one below, creating a structured approach to data transmission. Here's how it all comes together: • **Link Layer (Low-Level Protocols):**

	- At the lowest layer, known as the link layer, the focus is on the physical transfer of bits of information across a network link. - This link can be established using various technologies, such as Ethernet cables, Wi-Fi, telephone networks, or short-range radio standards like IEEE 802.15.4 (used in Personal Area Networks, PAN). • **Internet Layer:** - Sitting on top of the link layer is the Internet layer, which abstracts away the complexities of various network links. - Its primary function is to handle the routing of data packets to their destination based on IP addresses. • **Transport Layer (TCP):** - The transport layer is where the Transmission Control Protocol (TCP) operates. TCP enhances the capabilities of IP by providing sophisticated message control. - It ensures reliable, ordered, and error-checked delivery of data between devices. TCP is essential for applications that require precise data transfer, such as web browsing and email. • **Application Layer:** - The application layer, which is at the top of the stack, houses various application-specific protocols. These protocols are responsible for handling specific tasks, such as fetching web pages, sending emails, or enabling Internet telephony. - For instance, HTTP (Hypertext Transfer Protocol) is the dominant protocol for the web and is widely used for communication between Internet of Things (IoT) devices. It defines how web browsers and web servers communicate.
10	**Write short note on DNS (Domain Name System). (May 2019) (Nov 2019) (Nov 2022)**
	• Domain Name System (DNS): Navigating the Internet with Human-Friendly Names • The Domain Name System (DNS) is an essential part of how the internet works, making it accessible and navigable for humans. While computers efficiently handle numeric IP addresses, humans find them hard to remember. DNS provides a user-friendly solution by mapping domain names to IP addresses. Here's how DNS simplifies internet navigation: • **Domain Names and TLDs:** - Domain names, like "google.com," "bbc.co.uk," "wiley.com," and "arduino.cc," are what users commonly interact with on the web. Each domain name has a top-level domain (TLD), such as ".com" or ".uk." TLDs can further subdivide into more specific domains, creating a hierarchical structure. - For instance, ".uk" branches into ".co.uk" and ".gov.uk," and ".com" knows how to find domains like "google.com" and "wiley.com." • **Resolving to Machines and Services:** - DNS records contain information about where to direct calls to individual machines or services. These records are crucial for connecting users to specific websites or services. - For example, the DNS records for ".google.com" direct users to various Google services, like "www.google.com," "mail.google.com," and "calendar.google.com." Users can access these services by entering the corresponding domain names in their web browsers. • **Beyond Websites:**

	- While most DNS examples involve websites, DNS can also point to various other internet services. For instance: - "pop3.google.com" directs you to the POP3 email server for Gmail, enabling you to receive email. - "smtp.google.com" takes care of sending email to Gmail. - "ns1.google.com" represents the address of one of Google's DNS servers, responsible for resolving domain names. • **Configuring DNS:** - To configure DNS, users typically need to modify some settings. Domain name registrars, the companies where users purchase domain names, often offer control panels for changing these settings. - Users can also run their authoritative DNS servers, which define how their domains are resolved. DNS settings may include entries specifying the association of domain names with IP addresses and the duration for which these associations remain valid.
11	**Define and Explain Ubiquitous Computing (Ubicomp) (Nov 2019) (May 2023)**
	Ubiquitous Computing: • Ubiquitous computing, this idea emerged as a predecessor to the Internet of Things (IoT), offering insights into the historical evolution of technology's role in society. • Ubiquitous computing (or "ubicomp") is a concept where computing is made to appear anytime and everywhere. • A user interacts with the computer, which can exist in many different forms, including laptop computers, tablets and terminals in everyday objects such as a refrigerator or a pair of glasses. • Ubiquitous Computing employs middleware, operating system, mobile code, sensors and other technologies to support and operate the system. • It is only differentiated from the "Internet of Things" by the fact that computing also involves an Internet connection. • Devices like mobile phones evolved from their initial purpose as portable telephones to serve as versatile Internet terminals capable of multimedia functions. This transformation occurred by embedding technology into everyday objects, reshaping them to provide additional value beyond their original design. • The integration of computing into objects and appliances has significantly reduced the cost of computing power. • This concept of ubiquitous computing has paved the way for the Internet of Things, which extends beyond ubiquitous computing by connecting devices to the Internet.
12	**List and explain the roles of people making IoT. (Nov 2019) (Nov 2022)**
	People involved in making Internet of Things (IoT) devices come from various backgrounds and possess diverse skills. IoT development is a multidisciplinary field, and individuals may have roles that span different aspects of the IoT creation process. Here are some of the key roles and their explanations: • **Hacker/Tinkerer:** - Role: Often hobbyists or amateur engineers, hackers and tinkerers experiment with building prototypes of IoT devices. They work on the initial concept and basic functionalities.

	- Responsibilities: Prototyping, experimenting, and testing IoT concepts, typically at a small scale. • **Software Developer:** - Role: Software developers focus on creating the online components and back-end systems that support IoT devices. They write code for data processing, device communication, and user interfaces. - Responsibilities: Developing the software and firmware necessary for IoT devices to function and communicate with other devices or servers. • **Designer:** - Role: Designers take on the aesthetic aspect of IoT devices. They are responsible for making the devices visually appealing, user-friendly, and cohesive with their intended environment. - Responsibilities: Crafting the physical appearance and user interface of IoT devices, ensuring they are both functional and attractive. • **Engineer:** - Role: Engineers work on the technical aspects of IoT devices. They solve complex technical challenges, address scalability issues, and ensure the devices meet performance and reliability standards. - Responsibilities: Overseeing the technical design, functionality, and production process of IoT devices, including hardware design and troubleshooting. • **Craftsperson:** - Role: Craftspersons bring their craftsmanship skills into IoT device production. They may work with various materials and techniques to create aesthetically pleasing and high-quality components. - Responsibilities: Crafting and assembling physical components of IoT devices, often focusing on the artistic and tactile aspects of the product. • **Artist:** - Role: Artists add a creative and artistic touch to IoT devices. They contribute to the unique, expressive, and creative aspects of the device's design. - Responsibilities: Incorporating artistic elements that can make IoT devices not just functional but also meaningful and inspiring. • **Builder of the Internet of Things:** - Role: The central figure in IoT development, this role is responsible for orchestrating the work of hackers, software developers, designers, engineers, craftspersons, and artists to create a complete IoT device. - Responsibilities: Overseeing the end-to-end process of IoT device development, from conceptualization to production, ensuring all components work seamlessly together.
13	**"Data available through IOT device belongs to public or company which implements the IOT device". Discuss. (Nov 2019)**
	• The ownership of data generated by IoT devices is a complex and evolving issue. The determination of who rightfully owns this data often depends on the context in which the data is collected. • In public spaces, such as the example of a camera installed in an advertising hoarding, the argument can be made that the data generated by the public (those viewing the adverts) should belong, at least in part, to the public. • Urban computing expert Adam Greenfield suggests that in such scenarios, the data generated is a result of public actions, and, therefore, the public should

	have rights to be aware of and access that data. This perspective aligns with the notion that data subjects, the individuals to whom the data pertains, should have a say in how this data is used. • On private property, the situation can be different. Property owners may assert their rights to the data generated on their premises, even if they did not install the sensors themselves. • This perspective raises questions about the rights of individuals in privately-owned public spaces like shopping malls. In such cases, determining data ownership becomes more complex, and it may be influenced by the policies of the property owner. • The Open Internet of Things Assembly in 2012 introduced the concept of data subjects, emphasizing that individuals to whom the data pertains should have a say in how that data is collected, used, and shared. • However, there is no clear consensus or established legal framework regarding the rights of data subjects in the context of IoT-generated data. As technology and IoT adoption continue to advance, the issue of data ownership and privacy is a topic that requires ongoing debate and attention. • The ultimate resolution of data ownership matters in the IoT space will likely involve legal, ethical, and societal considerations, which will evolve over time.
14	**What are TCP n UDP ports? Explain with examples. (Nov 2019)**
	TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) ports are a fundamental part of the Internet's communication system. • **TCP Ports:** • TCP ports are numbered from 0 to 65535. • When you send a TCP/IP message over the Internet, you must specify the correct port number for the recipient to understand which service or application should handle the message. • Commonly used ports are called "well-known ports," typically numbered from 0 to 1023, and are reserved for system processes or administrators. • Some examples of well-known TCP ports include: - Port 80: Used for HTTP (Hypertext Transfer Protocol), which is the protocol for the World Wide Web. When your browser requests a web page, it usually sends this request to port 80. - Port 443: Used for HTTPS (HTTP Secure), a secure and encrypted version of HTTP, commonly used for online banking, e-commerce, and other secure data transmission. - Port 22: Used for SSH (Secure Shell), a protocol for secure remote access to computers and network devices. - Port 25: Used for SMTP (Simple Mail Transfer Protocol) for sending outbound email. - Port 110: Used for POP3 (Post Office Protocol version 3) for receiving inbound email. - Port 220: Used for IMAP (Internet Message Access Protocol) for receiving inbound email.

	• Using the wrong port when sending a TCP message can result in different outcomes, such as receiving an "RST" packet, which signifies an error, or simply having the request ignored. • **UDP Ports:** • UDP ports, like TCP ports, are also numbered from 0 to 65535. • UDP is a connectionless protocol, meaning it does not establish a persistent connection before sending data. • Common UDP ports may include: - Port 53: Used for DNS (Domain Name System) to resolve domain names into IP addresses. - Port 67: Used for DHCP (Dynamic Host Configuration Protocol) for automatic IP address assignment. - Port 69: Used for TFTP (Trivial File Transfer Protocol) for transferring files. - Port 161: Used for SNMP (Simple Network Management Protocol) for network management and monitoring. • Unlike TCP, UDP doesn't establish a connection, and it simply sends data packets to the specified port without verifying the recipient's readiness.
15	**"Be conservative in what you do, be liberal in what you accept from others" Explain. (May 2023)** **Explain the following concepts with respect to IoT: (Nov 2022)** **i. Small pieces loosely joined** **ii. Graceful degradation**
	Jon Postel wrote: "Be conservative in what you do, be liberal in what you accept from others". It is good to bear this in mind when designing or building anything which must interact with other services— particularly when you aren't the one building the other components with which your system interacts. • **SMALL PIECES, LOOSELY JOINED** - In a loosely coupled design, components are independent, and changes in one will not affect the operation of others. - This approach offers optimal flexibility and reusability when components are added, replaced, or modified. • **FIRST-CLASS CITIZENS ON THE INTERNET** - Where possible, use the same protocols and conventions that the rest of the Internet uses. - Where the existing protocols don't work, work with peers to amend existing standards or create new open standards. • **GRACEFUL DEGRADATION** - Graceful degradation is the ability of a computer, machine, electronic system or network to maintain limited functionality even when a large portion of it has been destroyed or rendered inoperative.
16	**Discuss the following IOT device use at Dos Liverpool** **i) Central Heating System ii) Doorbot**
	i) Central Heating System:

	- In DoES Liverpool, the central heating system has been connected to the internet, named YAHMS. - YAHMS consists of temperature sensors for indoor and outdoor measurements, an actuator to control heating, and server software. - It has both timer-based automation for basic comfort and a web-based interface for user control. - Users can access the YAHMS website from anywhere to check temperatures and adjust heating settings. Temperature sensors remain unhoused Arduino boards and are managed by John, who oversees the project. - The cabling to the boiler is neatly installed, and electronic components are hidden from view. - The user interface is well-designed, featuring a minimal interface suitable for both desktop and smartphone access. **ii) Doorbot** - DoorBot started as a PC with a monitor showing office views, events, and welcoming messages. - It had an RFID reader for member access and speakers for personalized greetings. - Initial development was straightforward, focusing on software configuration. - To accommodate expansion, the DoorBot was switched to a cost-effective Raspberry Pi. - Using standard PCs for multiple doors is expensive; devices with integrated screens are costlier. - A Raspberry Pi, with affordability and compatibility, became a scalable solution. - Starting with a cost-effective platform simplifies scaling. - Pushing hardware limits might require a more powerful platform, affecting upgradability.