QUESTION BANK   (15IT422EINTERNET OF THINGS)

UNITI : INTRODUCTION AND CONCEPTS OF IOT

MCQ’s

1. An increasing number of everyday machines and objects are now embedded with …………………………. and have the ability to communicate over the Internet. Collectively they make up the IoT.

a. Sensors or Actuators
b. Actuators
c. Common Channel
d. Network Channel

2. Potential applications and services in the IoT include:

a. Smart Devices / Cities
b. Smart Grids / Connected Cars
c. Home automation and Energy management
d. All the above

3. Smart objects produce large volumes of data. This data needs to be managed, processed, transferred and …………………...

a. Stored Securely.
b. Compiled
c. Interpreted
d. Outputted.

4. The use of standards

a. Ensure interoperable and cost-effective solutions.
b. Opens up opportunities in new areas.
c. Allows the market to reach its full potential
e. All the above

5. Smart lighting achieve ………………… by sensing the human movement and their environments and controlling the lights accordingly.

a. Energy Saving.
b. Cost Saving
c. Material Saving
d. Infrastructure saving

6. Smart Lighting system is ………………..

a. Energy Saving.
b. Solid State Lighting (LED)
c. IP enabled Lighting
d. Home Automation

4MARKS

1: What is IoT?

Answer 1: IoT stands for Internet of Things. It is basically a network using which things can communicate with each other using internet as means of communication between them. All the things should be IP protocol enabled in order to have this concept possible. Not one but multiple technologies are involved to make IoT a great success.

Refer IoT Basics.

2: Explain the basic architecture of IoT network.
Answer 2: Refer IoT architecture.

3: What are the main internal components of a IoT device?
Answer 3: Refer Answer3.

4: Explain different layers of a IoT device. In other words explain IoT protocol Stack.
Answer 4: Refer IoT protocol layers.

5: Explain various wireless technologies used in IoT.
Answer 5: Refer IoT wireless technologies.

6: What is the difference between IoT and M2M?
Answer 6: Refer Answer6.

7: Explain various types of antennas designed for IoT device application.
Answer 7: Refer Answer7.

8: Explain different types of sensors used in IoT applications.
Answer 8: Refer IoT Sensors, Domain specific IOTs.
9: Why do we need IoT?
10: Who is going to benefit from it?
11: Who decided that we need it and why?
12: Are there ways to optout?
13: What can we expect from open/DIY trends in IoT?
14: Can we reasonably translate our experiences and emotions into algorithms?
15: As technology gets smarter, will our abilities to think, feel and act be affected?
16: What decisions can or cannot be delegated to smart things?
17: More information euals more knowledge and empowerment?
18: Whose values and norms are embedded in our devices?
19: By what values will we relate to each other as we become things in the IoT?
20: Will IoT applications enhance existing or emerging social disparities and divides?
21: What do I want by design and by default?
22: Who will govern IoT?
23: Will there be sufficient powers for regulatory authorities to effectively counterbalance large corporations who wish to develop IoT?
24: How should we manage the work on smart cities, especially through the deployment of largescale IoT pilots, to help ensure that values and norms embedded in the smart connected devices will truly and fairly reflect the needs, expectations, concerns and priorities of citizens?
25: How will the IoT evolve under the combined pressure of nano and biotechnology, Big Data and Cloud?
26: Is the IoT likely to contribute to the development of a global ambient hyperconnected superintelligent system where technology and humans/communities/societies interconnect and integrate? (reference to "biot", "Singularity" and similar concepts)

12MARKS
1. Describe in detail about Architecture of Internet of Things.
2. Describe in detail about Physical and logical design of IOT.
3. Describe in detail about IOT enabling technologies.
4. Write short notes on IOT levels and deployment templates.
5. Write short notes on home automation, cities, and environment.
6. Write short notes on Domain specific IOTs, Energy, Retail, Agriculture And Industry.

]UNIT II : IOT AND M2M COMMUNICATION

MCQ’s

1. Machine to machine refers to direct communication between devices using any ………………….. , including wired and wireless.

a. communications channel
b. Link Channel
c. Common Channel
d. Physical Channel

2. M2M communication can include industrial instrumentation, enabling a sensor or meter to communicate the data it records (such as temperature, inventory level, etc.) to application …………………………..

a. software.
b. Hardware
c. System.
d. Server.

3. The Internet of Things is envisioned to be, where the physical world will merge with the ………...

a. Digital World.
b. Hardware
c. System.
d. Server.

4.

5. Individual devices are connected through …………….. interfaces.

a. Machine-to-Machine (M2M) communications.
b. Hardware to Machine Communications
c. System to Machine Communications.
d. Server to Machine Communications

6. The Network Configuration Protocol (NETCONF) provides mechanisms to install, manipulate, and delete the configuration of ………………….

a. Network Device.
b. Hardware
c. System.
d. Server.

7. YANG is a data modeling language used to model configuration and state data manipulated by the …………………………...

a. NETCONF remote procedure calls, and NETCONF notifications.
b. NETCONF remote procedure calls only,
c. NETCONF notifications only
d. YANG remote procedure calls, and YANG notifications.

4MARKS

1. Write the difference between IOT and M2M

2. What is the difference between SDN and NFV?

Network functions virtualization and software-defined networking are two closely related technologies that often exist together, but not always. NFV and SDNare both moves toward network virtualization and automation, but the two technologies have different goals

3. What is orchestration in Nfv?

Network functions virtualization (NFV) Orchestration (or NFV Orchestration) is used to coordinate the resources and networks needed to set up cloud-based services and applications. This process uses a variety of virtualization software and industry standard hardware.

4. What is orchestration in Nfv?

Network functions virtualization (NFV) Orchestration (or NFV Orchestration) is used to coordinate the resources and networks needed to set up cloud-based services and applications. This process uses a variety of virtualization software and industry standard hardware.

5. What is Nfv in networking?

Network functions virtualization (NFV) is the concept of replacing dedicated network appliances — such as routers and firewalls — with software running on commercial off-the-shelf servers. Optimizes service creation, activation, and assurance by bringing the benefits of the cloud to the metro edge.

6. What is SDN in networking?

Software defined networking (SDN) is an approach to using open protocols, such as OpenFlow, to apply globally aware software control at the edges of the network to access network switches and routers that typically would use closed and proprietary firmware.

7. What is virtual network functions?

A virtual network function (VNF) is a virtualized task formerly carried out by proprietary, dedicated hardware. VNF moves network functions out of dedicated hardware devices and into software. This allows specific functions that required hardware devices in the past to operate on standard x86 servers.

8. What is ETSI Nfv?

ETSI NFV is part of the European Telecommunication Standards Institute (ETSI) is an independent standardization organization that has been instrumental in developing standards for information and communications technologies (ICT) within Europe.

9. What do you mean by SNMP?

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an application–layer protocol defined by the Internet Architecture Board (IAB) in RFC1157 for exchanging management information between network devices. It is a part of Transmission Control Protocol⁄Internet Protocol (TCP⁄IP) protocol suite.

10. What is a SNMP trap?

SNMP traps are alert messages sent from a remote SNMP-enabled device to a central collector, the "SNMP manager". A trap might tell you that a device is overheating, for example. (As you'll recall, SNMP is one possible protocol that devices can use to communicate.)

12MARKS

1. Describe in detail about M2M.
2. Difference between IOT and M2M.
3. Describe in detail about ETSI M2M Architecture.
4. Write short notes on ETSI M2M SCL resource structure.
5. Write short notes on Security in ETSI M2M framework.
6. Write short notes on SDN and NFV for IOT.
7. Write short notes on IOT system management and need for IOT system management.
8. Write short notes on SNMP.
9. Write short notes on Network operator requirements.
10. Write short notes on NETCONF-YANG and IOT system management with NETCONF-YANG.
11. Write short notes on IoT Design methodology.
12. Write short notes on IOT system for Weather Monitoring.

UNIT III : IoT PLATFORMS

MCQ's

4MARKS

1. Give a list of IoT – Sensors.

S.No	Devices	
1.	accelerometers	temperature sensors
2.	magnetometers	proximity sensors
3.	gyroscopes	image sensors
4.	acoustic sensors	light sensors
5.	pressure sensors	gas RFID sensors
6.	humidity sensors	micro flow sensors

2. List out some wearable Electronics

Current smart wearable devices include −

- Head − Helmets, glasses
- Neck − Jewelry, collars
- Arm − Watches, wristbands, rings
- Torso − Clothing, backpacks
- Feet − Socks, shoes

3. List out some standard IoT devices.

- The desktop, tablet, and cellphone remain integral parts of IoT as the command center and remotes.
- The desktop provides the user with the highest level of control over the system and its settings.
- The tablet provides access to the key features of the system in a way resembling the desktop, and also acts as a remote.
- The cellphone allows some essential settings modification and also provides remote functionality.
- Other key connected devices include standard network devices like routers and switches.

4. What is (and isn't) a microcontroller?

A microcontroller unit (MCU) is a small, self-contained computer that is housed on a single integrated circuit, or microchip. They differ from your desktop computer in that they are typically dedicated to a single function, and are most often embedded in other devices (e.g. cellphones; household electronics).

5. What's the difference between a microcontroller and a microprocessor (MCU vs MPU)?

Microcontrollers also differ from microprocessors. Microprocessors contain only a CPU, and therefore require added peripherals to perform tasks. MCUs, on the other hand, contain RAM, ROM, and similar peripherals, which allow them to perform (simple) tasks independently. Ultimately, despite similar names and appearances, microcontrollers and microprocessors differ widely in their applications. Microprocessors are more powerful, but must be employed as single components in larger systems to function. Microcontrollers, meanwhile, are limited in power and functionality, but can perform simple functions independently. Your Apple TV, for example, requires a microprocessor to handle all the varied and demanding tasks it performs. A connected coffeemaker, on the other hand, only needs to perform simple routines and tasks, and therefore employs a microcontroller.

6. What is the difference between a microcontroller (MCU) and a system-on-a-chip (MCU vs SOC)?

The other term one hears often in this discussion is System on a Chip (SoC). The distinction between an MCU and an SoC is much less clear, and the two terms are often used interchangeably. However, in common usage, the term SoC typically refers to MCUs with a greater number of onboard peripherals and functionality. For the purposes of this outline, we won't make a distinction between MCUs and SoCs.

7. Why use an MCU for IoT?

SIMPLICITY

In most IoT use-cases, the relative simplicity of an MCU is an advantage rather than a disadvantage. MCUs don’t require operating systems to function, and are easy to interface with external devices such as sensors and motors. Their lack of external dependencies also makes them easy to set up. You can simply turn them on, upload firmware, and they work. Additionally, the coding required to program an MCU is minimal.

SECURITY

By virtue of their relative simplicity, MCUs also offer fewer avenues of attack. As a rule, each open port and available protocol is also a potential vulnerability. Code on MCUs runs “bare metal”, meaning it includes no intermediary operating system to execute instructions. This results in limited potential attack vectors and increased inherent security.

COST

In most contemporary IoT applications, an MCU can deliver all the processing power and functionality one needs. As a result, MCUs are most often the best, most economic hardware choice for IoT applications. Overall, they offer simple, secure, functionality for little cost.

8. What is the programming language for Arduino?

In fact, you already are; the Arduino language is merely a set of C/C++ functions that can be called from your code. Your sketch undergoes minor changes (e.g. automatic generation of function prototypes) and then is passed directly to a C/C++ compiler (avr-g++).

9. What is the Arduino Uno?

The Arduino Uno is a microcontroller board based on the ATmega328 (datasheet). It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz crystal oscillator, a USB connection, a power jack, an ICSP header, and a reset button. Dfg

10. What is Arduino IDE?

ARDUINO WEB EDITOR. ... The open-source Arduino Software (IDE) makes it easy to write code and upload it to the board. It runs on Windows, Mac OS X, and Linux. The environment is written in Java and based on Processing and other open-source software.

11. What is the Arduino?

Arduino is an open-source electronics platform based on easy-to-use hardware and software. Arduino boards are able to read inputs - light on a sensor, a finger on a button, or a Twitter message - and turn it into an output - activating a motor, turning on an LED, publishing something online. As

12. Is the Arduino a microcontroller?

"Arduino" is a software development environment and any of several microcontroller boards that the software environment can develop programs for. Most of the boards use Atmel AVR microcontrollers.

13. Comparison of Open Source Hardware: Intel Galileo vs. Raspberry Pi.

The Intel Galileo and the Raspberry Pi (RPi) are both do-it-yourself (DIY) electronics hardware development boards featuring embedded processors. RPi is loosely labelled as open source in this article, but it does not qualify as open source hardware per the strictest standards, since some of the chips on the board are notoriously difficult to get support for, rendering deep control impossible and cobbling creativity in the process. Realistically speaking, the highest levels of openness for hardware would include an open core, and yet many products claim to be open source hardware that go up to, but do not include, total control of the processor. Additionally, although RPi is a wonderful educational and media processing tool, RPi cannot be reproduced freely, as there is a copyright on the RPi schematics. Manufacture of the board is limited to a couple of licensees.

12MARKS

1. Describe in detail about Hardware used for IoT.
2. Describe in detail about Microcontrollers and Microprocessors for IoT.
3. Describe in detail about SoC and Sensors

4. Explain in detail about Introduction to Arduino.
5. Describe in detail about Pi, Spark and Intel Galileo.

UNIT IV: IoTTECHNICAL STANDARDS AND PROTOCOLS

MCQ's

4MARKS

12MARKS

1. Describe in detail about RF Protocols- RFID and NFC.
2. Describe in detail about IEEE 802.15.4: ZigBee, Z-WAVE, THREAD.
3. Describe in detail about Bluetooth Low Energy (BLE).
4. Describe in detail about IPv6 for Low Power and Lossy Networks (6LoWPAN) and Routing Protocol for Low power and lossy networks (RPL).
5. Describe in detail about CoAP ,XMPP.
6. Describe in detail about Web Socket.
7. Describe in detail about AMQP.
8. Describe in detail about MQTT.
9. Describe in detail about WebRTC and PuSH.
10. Write short notes on Architectural Considerations in Smart Object Networking.

UNIT V: DEVELOPING INTERNET OF THINGS

MCQ's

4MARKS

1. What do you mean by RFID?

RFID (radio frequency identification) is a technology that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency (RF) portion of the electromagnetic spectrum to uniquely identify an object, animal, or person.

2. How does the RFID work?

RFID methods utilize radio waves to accomplish this. At a simple level, RFID systems consist of three components: an RFID tag or smart label, an RFID reader, and an antenna. RFID tags contain an integrated circuit and an antenna, which are used to transmit data to the RFID reader (also called an interrogator).

3. How does an RFID chip work?

The RFID technology has two components – the reader and the tag. The reader has two parts – a transceiver and an antenna. The transceiver generates a weak radio signal that may have a range from a few feet to a few yards. The signal is necessary to wake or activate the tag and is transmitted through the antenna.

4. What is the RFID?

RFID tagging is an ID system that uses small radio frequency identification devices for identification and tracking purposes. An RFID tagging system includes the tag itself, a read/write device, and a host system application for data collection, processing, and transmission.

5. What is the use of RFID?

Radio-frequency identification (RFID) uses electromagnetic fields to automatically identify and track tags attached to objects. The tags contain electronically stored information.

6. Is RFID and NFC the same?

RFID is the process by which items are uniquely identified using radio waves, and NFC is a specialized subset within the family of RFID technology. Specifically, NFC is a branch of High-Frequency (HF) RFID, and both operate at the 13.56 MHz frequency.

7. De Image result for IEEE 802.15.4

IEEE 802.15.4 is a technical standard which defines the operation of low-rate wireless personal area networks (LR-WPANs). It specifies the physical layer and media access control for LR-WPANs, and is maintained by the IEEE 802.15 working group, which defined the standard in 2003fine IEEE 802.15.4

8. What is NFC on a phone?

NFC, or Near Field Communication, is a technology that allows devices to exchange information simply by placing them next to one another. ... Smartphones use NFC to pass photos, contacts, or any other data you specify between NFC enabled handsets.

9. How can NFC be used?

At the time of writing the NFC standard has three modes of operation: the peer-to-peer mode that lets two smartphones swap data, a read/write mode in which one active device picks up info from a passive one, and card emulation, in which an NFC device such as a smartphone can be used like a contactless credit card.

10. What is the use of NFC in Android?

Near Field Communication (NFC) is a set of short-range wireless technologies, typically requiring a distance of 4cm or less to initiate a connection. NFC allows you to share small payloads of data between an NFC tag and an Android-powered device, or between two Android-powered devices.

11. What is NFC technology?

Near Field Communication (NFC) is a short-range wireless connectivity standard (Ecma-340, ISO/IEC 18092) that uses magnetic field induction to enable communication between devices when they're touched together, or brought within a few centimeters of each other.

12. What is Zigbee

Zigbee is a low-cost, low-power, wireless mesh network standard targeted at the wide development of long battery life devices in wireless control and monitoring applications. Zigbee devices have low latency, which further reduces average current. Zigbee chips are typically integrated with radios and with microcontrollers that have between 60-256 KB of flash memory. Zigbee operates in the industrial, scientific and medical (ISM) radio bands: 2.4 GHz in most jurisdictions worldwide; 784 MHz in China, 868 MHz in Europe and 915 MHz in the USA and Australia. Data rates vary from 20 kbit/s (868 MHz band) to 250 kbit/s (2.4 GHz band).

The zigbee network layer natively supports both star and tree networks, and generic mesh networking. Every network must have one coordinator device, tasked with its creation, the control of its parameters and basic maintenance. Within star networks, the coordinator must be the central node. Both trees and meshes allow the use of zigbee routers to extend communication at the network level.

Zigbee builds on the physical layer and media access control defined in IEEE standard 802.15.4 for low-rate WPANs. The specification includes four additional key components: network layer, application layer, zigbee device objects (ZDOs) and manufacturer-defined application objects which allow for customization and favor total integration. ZDOs are responsible for some tasks, including keeping track of device roles, managing requests to join a network, as well as device discovery and security.

Zigbee is one of the global standards of communication protocol formulated by the significant task force under the IEEE 802.15 working group. The fourth in the series, WPAN Low Rate/zigbee is the newest and provides specifications for devices that have low data rates, consume very low power and are thus characterized by long battery life. Other standards like Bluetooth and IrDA address high data rate applications such as voice,[4] video and LAN communications.

Zigbee provides the ability to run for years on inexpensive batteries for a host of monitoring and control applications. The zigbee network layer ensures that networks remain operable in the conditions of a constantly changing quality between communication nodes. The zigbee advantage is the zigbee protocol which is designed to communicate data through hostile RF environment that are common in commercial and industrial application. Its protocol features include support for multiple network topologies such as; point to point and mesh network, collision avoidance and retries, and low latency. Another defining feature of zigbee is facilities for carrying out secure communications, protecting establishment and transport of cryptographic keys, cyphering frames, and controlling device. It builds on the basic security framework defined in IEEE 802.15.4.

13. What is Z-Wave?

Z-Wave is a wireless communications protocol used primarily for home automation. It is oriented to the residential control and automation market and is intended to provide a simple and reliable method to wirelessly control lighting, HVAC, security systems, home cinema, automated window treatments, swimming pool and spa controls, and garage and home access controls. Like other protocols and systems aimed at the home and office automation market, a Z-Wave automation system can be controlled via the Internet, with a Z-Wave gateway or central control device serving as both the Z-Wave hub controller and portal to the outside.[1] Z-Wave was originally developed by Danish startup Zen-Sys and later acquired by Sigma Designs in 2008.[2] Utilised by over 600 manufacturers, some 2,100 products have been certified as Z-Wave compatible since the standard's inception with an estimated 50 million devices having been shipped.

12MARKS

1. Describe in detail about IoT platforms design methodology.
2. Describe in detail about IoT Physical devices and endpoints.
3. Write short notes on IoT System Logical design using Python.
4. Describe in detail about IoT physical servers and cloud offerings (Cloud computing for IoT).