Q.Define the term IOT with suitable example

The Internet of Things, or IoT, is essentially an ecosystem of physical devices, vehicles, appliances, and other things that have the ability to connect, collect and exchange data over a wired and wireless network, with little or no human-to-human or human-to-computer intervention. Allowing integration and data exchange between physical devices and the computer, this new wave of technology focuses on making human life more simplified and comfortable with the right mix of efficiency and productivity.

To be more specific, taking advantage of cutting-edge technologies like Machine Learning, Machine-to-Machine (M2M) Communication and Artificial Intelligence (AI), IoT aims at extending connectivity beyond standard Internet supported physical devices (smartphones, tablets, desktops, and laptops) to a wide spectrum of non-internet-enabled physical devices and everyday objects, such as coffee makers, washing machines, door locks, etc., so you can remotely monitor and control them with the help of a mobile or tablet device

IOT Example :

1) Nest Learning Thermostat

Nest Learning Thermostat self-learning Wi-Fi-enabled smart thermostat that leverages Machine Learning to automatically optimize the heating and cooling of your home to conserve energy. You can also manually control your home's temperature with just a few taps on your smartphone or tablet

Amazon Go

Amazon Go is one of its kind retail store that facilitates customers shopping with no checkout required. All you need to sign in the Amazon Go app to enter the store, then shop as you normally would and leave the store. No lines, no checkout, just walk out!

Q.State and explain various components of IOT

1. Smart devices & sensors - Device connectivity - Sensors like Temperature sensors, Wifi Humidity sensors, Wifi Light sensor, Wifi Vibration sensor, Proximity detection, RFID tags etc. Basically these sensors are continuously collecting data from the environment and transmit the information to the next layer.

2. Gateway - IOT gateway manages the bidirectional data traffic between different networks and protocols. IOT gateway offers extreme level of security for the network and transmitted data with higher order encryption techniques.

3. Cloud - Basically cloud is an advanced high performance network of servers optimized to perform high speed data. Cloud system integrates billion of devices, sensors, gateway, protocols, data storage and provide predictive analytics.

4. Analytics - Analytics is the process of converting analog data from billions of smart devices and sensors into useful insights which can be interpreted and used for detailed analysis.

5. User interface - User interfaces are the visible, tangible part of the IoT system which can be accessible by users.

Q.Explain in brief MQTT broker

MQTT is one of the most commonly used protocols in IoT projects. It stands for Message Queuing Telemetry Transport.

In addition, it is designed as a lightweight messaging protocol that uses publish/subscribe operations to exchange data between clients and the server. Furthermore, its small size, low power usage, minimized data packets and ease of implementation make the protocol ideal of the “machine-to-machine” or “Internet of Things” world.

How MQTT works

Like any other internet protocol, MQTT is based on clients and a server. Likewise, the server is the guy who is responsible for handling the client’s requests of receiving or sending data between each other.

MQTT server is called a broker and the clients are simply the connected devices.

So: When a device (a client) wants to send data to the broker, we call this operation a “publish”.

When a device (a client) wants to receive data from the broker, we call this operation a “subscribe”.

MQTT Components:

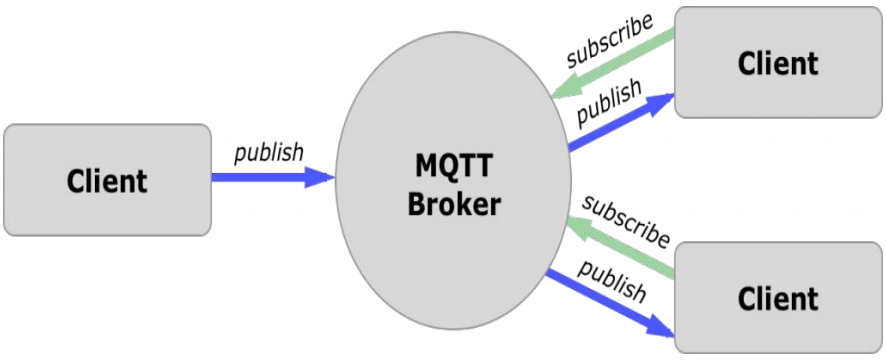
That takes us to the MQTT components, which are 5 as follows:

Broker, which is the server that handles the data transmission between the clients.

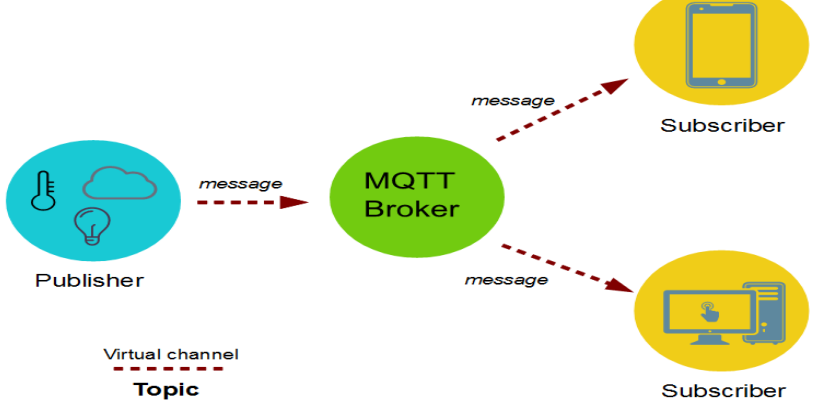
A topic, which is the place a device want to put or retrieve a message to/from.

The message, which is the data that a device receives “when subscribing” from a topic or send “when publishing” to a topic.

Publish, is the process a device does to send its message to the broker.



Subscribe, where a device does to retrieve a message from the broker.



Q Explain various aspects of trust model in arm?

Ans:1.Building trusted IoT environments is of great importance to achieve the full benefits of smart applications.

2.Trust models are proposed to tackle behaviour-related issues.

- **Trust Model Domains**: Because ICT and IoT systems may include a large number of interacting entities with different properties, maintaining trust relationships for every pair of interacting entities may be prohibitive. Therefore, groups of entities with similar trust properties can define different trust domains.
- **Trust Evaluation Mechanisms**: These are well-defined mechanisms that describe how a trust score could be computed for a specific entity. The evaluation mechanism needs to take into account the source of information used for computing the trust level/score of an entity; two related aspects are the federated trust and trust anchor. A related concept is the IoT support for evaluation of the trust level of a Device, Resource, and Service.
- **Trust Behavior Policies**: These are policies that govern the behavior between interacting entities based on the trust level of these interacting entities; for example, how a User could use sensor measurements retrieved by a Sensor Service with a low trust level.
- **Trust Anchor**: This is an entity trusted by default by all other entities belonging to the same trust model, and is typically used for the evaluation of the trust level of a third entity.
- **Federation of Trust**: A federation between two or more Trust Models includes a set of rules that specify the handling of trust relationships between entities with different Trust Models. Federation becomes important in large-scale systems.

Q. 1 State applications of IOT in real life.

Ans:

1. Smart Home

- **Smart Home has become the revolutionary ladder of success in the residential spaces and it is predicted Smart homes will become as common as smartphones.**
- **The cost of owning a house is the biggest expense in a homeowner's life. Smart Home products are promised to save time, energy and money.**

- **With Smart home companies like Nest, Ecobee, Ring and August, to name a few, will become household brands and are planning to deliver a never seen before experience.**

2. Smart Wearables
   - **Wearable devices are installed with sensors and softwares which collect data and information about the users. This data is later pre-processed to extract essential insights about user.**
   - **These devices broadly cover fitness, health and entertainment requirements.**
3. Connected Cars
   - **A connected car is a vehicle which is able to optimize it's own operation, maintenance as well as comfort of passengers using onboard sensors and internet connectivity.**
4. Smart Cities
   - **Smart city is another powerful application of IoT generating curiosity among world's population.**
   - **Smart surveillance, automated transportation, smarter energy management systems, water distribution, urban security and environmental monitoring all are examples of internet of things applications for smart cities.**
5. IoT in agriculture
   - **Smart farming is one of the fastest growing field in IoT.**
   - **Farmers are using meaningful insights from the data to yield better return on investment.**
   - **Sensing for soil moisture and nutrients, controlling water usage for plant growth and determining custom fertilizer are some simple uses of IoT.**
6. IOT in Healthcare
   - IoT in healthcare is aimed at empowering people to live healthier life by wearing connected devices.
   - The collected data will help in personalized analysis of an individual's health and provide tailor made strategies to combat illness.
7. Smart Retail
   - **IoT provides an opportunity to retailers to connect with the customers to enhance the in-store experience.**
   - **Smartphones will be the way for retailers to remain connected with their consumers even out of store.**
8. Industrial Internet
   - **Industrial Internet is the new buzz in the industrial sector, also termed as Industrial Internet of Things (IIoT).**
   - **It is empowering industrial engineering with sensors, software and big data analytics to create brilliant machines.**

Q Explain CoAP protocol used in IOT.

Ans:

- Constrained Application Protocol (CoAP) is a specialized web transfer protocol for use with constrained nodes and constrained networks in the Internet of Things.

- CoAP is designed to enable simple, constrained devices to join the IoT even through constrained networks with low bandwidth and low availability.
- It is generally used for machine-to-machine (M2M) applications such as smart energy and building automation. The protocol was designed by the Internet Engineering Task Force (IETF).
- CoAP functions as a sort of HTTP for restricted devices, enabling equipment such as sensors or actuators to communicate on the IoT.
- These sensors and actuators are controlled and contribute by passing along their data as part of a system.
- The protocol is designed for reliability in low bandwidth and high congestion through its low power consumption and low network overhead.
- CoAP relies on UDP security features to protect information.

Q Discuss various characteristics/features due to which IOT is popular in market.
Ans:
Internet of Things (IoT) is a technology of connected smart devices that has incremental use cases across industries.

1. Connectivity

- **In the case of IoT, the most important feature one can consider is connectivity.**
- **Without seamless communication among the interrelated components of the IoT ecosystems (i.e sensors, compute engines, data hubs, etc.) it is not possible to execute any proper business use case.**
- **IoT devices can be connected over Radio waves, Bluetooth, Wi-Fi, Li-Fi, etc.**

2. Sensing

- **In the case of IoT in order to get the best of it, we need to read the analog signal, convert it in such a way that we can derive meaningful insights out of it.**
- **We use Electrochemical, gyroscope, pressure, light sensors, GPS, Electrochemical, pressure, RFID, etc. to gather data based on a particular problem.**
- **For example for automotive use cases, we use Light detection sensors along with pressure, velocity and imagery sensors.**

3. Active Engagements

- **IoT device connects various products, cross-platform technologies and services work together by establishing an active engagement between them.**
- **In general, we use cloud computing in blockchain to establish active engagements among IoT components.**

4. Scale

- **IoT devices should be designed in such a way that they can be scaled up or down easily on demand.**
- **In general, IoT is being used from smart home automation to automating large factories and work stations, so the use cases vary in scale.**

5. Dynamic Nature

- **For any IoT use case, the first and foremost step is to collecting and converting data in such a way that means business decisions can be made out of it.**

- **In this whole process, various components of IoT need to change their state dynamically. For example, the input of a temperature sensor will vary continuously based on weather conditions, locations, etc.**
- **IoT devices should be designed this keeping in mind.**

6. Safety

- **One of the main features of the IoT ecosystem is security.**
- **In the whole flow of an IoT ecosystem, sensitive information is passed from endpoints to the analytics layer via connectivity components.**
- **While designing an IoT system we need to adhere to proper safety, security measures, and firewalls to keep the data away from misuse and manipulations.**

7. Integration

- **IoT integrates various cross-domain models to enrich user experience.**
- **It also ensures proper trade-off between infrastructure and operational costs.**

Q Mention advantages and disadvantages of IOT.
Ans:

Advantages:

1. Data:
The more the information, the easier it is to make the right decision. Knowing what to get from the grocery while you are out, without having to check on your own, not only saves time but is convenient as well.
2. Tracking:
The computers keep a track both on the quality and the viability of things at home. Knowing the expiration date of products before one consumes them improves safety and quality of life. Also, you will never run out of anything when you need it at the last moment.
3.
Time:
The amount of time saved in monitoring and the number of trips done otherwise would be tremendous.
4. Money:
The financial aspect is the best advantage. This technology could replace humans who are in charge of monitoring and maintaining supplies.

Disadvantages:

1. Compatibility:
As of now, there is no standard for tagging and monitoring with sensors. A uniform concept like the USB or Bluetooth is required which should not be that difficult to do.
2. Complexity:
There are several opportunities for failure with complex systems. For example, both you and your spouse may receive messages that the milk is over and both of you may end up buying the same. That leaves you with double the quantity required. Or there is a software bug causing the printer to order ink multiple times when it requires a single cartridge.
3. Privacy/Security:

Privacy is a big issue with IoT. All the data must be encrypted so that data about your financial status or how much milk you consume isn't common knowledge at the work place or with your friends.

4. Safety:

There is a chance that the software can be hacked and your personal information misused. The possibilities are endless. Your prescription being changed or your account details being hacked could put you at risk. Hence, all the safety risks become the consumer's responsibility.

Q) Discuss the working of HTTP protocol.

Ans)The Hypertext Transfer Protocol is an application protocol for distributed, collaborative, hypermedia information systems that allows users to communicate data on the World Wide Web.

HTTP was invented alongside HTML to create the first interactive, text-based web browser: the original World Wide Web. Today, the protocol remains one of the primary means of using the Internet.

As a request-response protocol, HTTP gives users a way to interact with web resources such as HTML files by transmitting hypertext messages between clients and servers. HTTP clients generally use Transmission Control Protocol (TCP) connections to communicate with servers.

HTTP utilizes specific request methods in order to perform various tasks:

GET requests a specific resource in its entirety
HEAD requests a specific resource without the body content
POST adds content, messages, or data to a new page under an existing web resource
PUT directly modifies an existing web resource or creates a new URI if need be
DELETE gets rid of a specified resource
TRACE shows users any changes or additions made to a web resource
OPTIONS shows users which HTTP methods are available for a specific URL
CONNECT converts the request connection to a transparent TCP/IP tunnel
PATCH partially modifies a web resource
All HTTP servers use the GET and HEAD methods, but not all support the rest of these request methods.

Q)How Upnp protocol is different than HTTP. Explain in brief.

Ans)

Universal Plug and Play (UPnP) is a networking protocol or a set of networking protocols which enables devices like personal computers, WiFi, Mobile devices, printers etc. to discover each other and establish connections for sharing services and data and also entertainment purposes. UPnP is intended to be used on residential networks.UPnP can be considered as an extension of Plug and Play which enables users to connect devices directly to a computer without any manual configurations to the device or to the computer.

UPnP allows direct networking between home appliances like printers, personal computers, mobile devices, and many more. It uses established standard industry protocols like TCP/IP, XML, Simple Object Access Protocol (SOAP), UDP, DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System). UPnP technology was initially promoted by UPnP forum which was an initiative by various vendors.
Advantages of UPnP:
1.It can be used for NAT traversal or Firewall punching.
2.It allows real Plug and Play compatibility.
3.It is backed by various big vendors and companies like Microsoft and Intel, which makes it an industry standard.
4.It is an ideal architecture for home devices and networks.

Q) Explain in breif how IoT can be helpful in Education and Government sector?
Ans)
Education sector:-
a. Poster boards into IoT enabled boards
It is indeed very difficult to compare the older era presentation boards with present-day multimedia poster boards. Internet gear like Glogster has changed this ease and permits us to create digital posters without problems combining with the photos, audio, video, text, and hyperlinks.
b. Interactive gaining of knowledge
Getting to know these days is not restrained to the mixture of texts and pictures but beyond that. Most of the textbooks are paired with net-primarily based websites that consist of extra substances, films, exams, animations and different substances to support the mastering.
c. Learning at any time and anywhere
IoT plays an important position in constructing a network through the use of special internet-based systems. Advanced technology enables the academics to display the development of the scholars. IoT allows students and teachers to communicate via extraordinary method, checking messages and upcoming events at the same time when away from the classroom or even replying to posts. It is by far a very effective app that provides safe network and complete privacy. It also allows a user to save your specific thoughts and class undertaking without worrying and assure you full confidentiality.
d. Superior safety features
This Application of IoT in Education is important as enforcing the superior technology answers inside the school rooms and training area may be very useful. It includes emergency indicators, audio enhancement, wi-fi clocks and hearing impaired notifications that offer the scholars and body of workers with a feeling of security.
e. Bye Bye to Chalkboards
Students in recent times make use of a very powerful platform which includes smart boards. It facilitates the lecturers to provide an explanation for the lectures more without problems with the assist of online displays and films.
Government sector:-
1. Law enforcement

The enormity of the general population and complexity of the inhabited areas like cities and towns make it hard for government agencies to provide surveillance and protection with the relatively small number of personnel they have. Even the presence of a myriad of cameras is pointless if there aren't enough eyes to constantly analyze the footage recorded by them. IoT can help government law enforcement agencies in monitoring public safety through its smart network of sensing and scanning devices. Since it is impossible for law enforcement personnel to be present at all high-risk locations simultaneously, IoT enabled surveillance systems can provide continuous, real-time intelligence. These systems, powered by machine and deep learning algorithms, can not only gather video and audio footage but also analyze it for threats. They can notify concerned personnel upon discovery of potentially harmful situations, which can be looked into and prevented in time.

IoT-enabled license plate scanning systems can help track down vehicles of criminals and traffic offenders. An intelligent, well connected IoT network can not only enable quick response to threats but can also minimize crime rates through preventive action.

2. Infrastructure management

Governments spend vast amounts of tax money on building and maintaining infrastructural facilities for the public. This includes the building of roads and bridges, power grids, water supply lines, gas supply, rail lines, airports, etc. which cost a lot more to maintain than to build. Any major damages or defects any of these systems can cause disruptions in civilian activities, which can have far-reaching ramifications. To ensure the effective functioning of these systems, governments can use IoT enabled maintenance and monitoring. For instance, IoT sensors can constantly analyze railway lines and engines for any defects or really sounds of failure and notify the authorities and the concerned staff for prompt repairs. They can also constantly monitor and regulate power supply through nation-wide power grids, and help in identifying impending break-downs.

In addition to helping governments manage infrastructure, IoT can help governments to make decisions regarding new infrastructure projects, such as laying new roads and railway lines.

3. Disaster management

Governments have the obligation of preventing man-made disasters and protecting the public from natural ones. IoT and big data enabled disaster prevention and management systems can help governments preserve human life during times of unforeseen disasters. In areas where forest fires are common, IoT sensors can be set up in forests to detect fires in their early stages to curb their spreading and the consequent devastating effects. IoT can also help in areas that are prone to flooding, by monitoring the water bodies for alerting authorities when the water levels rise at alarming rates.

IoT can also prevent man-made disasters by providing emergency response teams with continuous monitoring capability, which enables them to be prepared for contingencies.

Integrating IoT in government operations will be a long and effortful endeavor. However, the potential benefits far outweigh the initial friction. With greater penetration and propagation of IoT, governments can take a fully supervisory role, and ensure public welfare without obtrusion.

12.XMPP and clayster

*Xmpp - the Extensible Messaging and Presence Protocol (XMPP) is widely used as a communication protocol. Based on Extensible Markup Language (XML), XMPP enables fast, near-real-time exchange of data between multiple entities on a network.*In contrast to most direct messaging protocols, XMPP is described in an open standard and uses an open systems approach of development and application, by which anyone may implement an XMPP service and interoperate with other organisations' implementations.Since XMPP is an open set of rules, implementations can be developed using any software licence, and many server, client, and library XMPP implementations are distributed as free and open source software. Numerous freeware and commercial software implementations also exist.

Clayster - Internet **Clayster** Include XMPP is the core into which we normalize data from different sources and make it available in unified fabric. The Include platform abstracts and transforms any data source to coexist in a data normalized infrastructure.

13.i>thinger.io –

Thinger.io is a platform that allows connecting things to the Internet.It is Open Source, so you can take the code an build your own cloud if you want. It provides thing API discovery right out of the box, so you can code your things and interact easily from the web.

· **simple but Powerful**: Just a couple code lines to connect a device and start retrieving data or controlling it's functionalities with our web based Console, able to connect and manage thousands of devices in a simple way.

· **Hardware agnostic:** Any device from any manufacturer can be easily integrated with Thinger.io's infrastructure.

· **Open-Source**: most of the platform modules, libraries and APP source code are available in our github repository to be downloaded and modified with MIT license.

· **Customizable**: Fully white-labelable frontend allows customizing Thinger.io Platform with your brand colors, logotype and web domain.

13.ii> **Sense iot** - **Sense IoT** is a sensor data storage, visualisation and remote management platform offering leading cloud computing technologies to provide you excellent data scalability and easy visualisation. We support any web- connected third party device, sensor, or sensor network through a simple open API.

14. Red programming language-

First fullstack programming solution: combines in one tool, the ability to write high-level code (GUI apps, scripting and DSL) and fast low-level code (writing device drivers, operating systems, native interfacing, etc). Moreover, Red is also a both-sided technology (client & server).

Cross-platform native code compiler: from any platform the toolchain runs on, you can compile to about 15 other platforms, with a simple command-line option (-t Windows, -t Linux, -t Darwin, -t RPi, …).

Extremely lightweight: Red is a 1MB, single-file, no install, no setup, toolchain. It takes typically a few seconds to download and you can immediatly start writing and running code, there's *nothing* to setup (it's just terrible that this is the exception instead of being the norm…).

Batteries-included solution: it comes with a very rich runtime library, despite its tiny size, covering pretty much anything you need for common tasks.

DSL-oriented environment: Red comes with many embedded DSL addressing important needs (like GUI or system-programming). DSL are a very powerful way to reduce complexity arising from frameworks or API, while drastically increasing productivity. Red includes a DSL (called Parse) for constructing DSLs.

Red (like Rebol) is a Lisp derivative, but with a human-friendly syntax (no parenthesis hell). Red is its own data format. All code is treated as data until you evaluate it, code/data serialization comes for free. The minimal punctuation makes it easy on the eye.

Q16):features of carriots?

1.Carriots offers an end-to-end Internet of Things (IoT) platform designed

for today's industry needs and tomorrow's innovations.

2.Carriots is a smart Platform as a Service (PaaS) designed for machine to

machine (M2M) and digital twin projects.

3.Carriots accelerates your IoT application development and provides simple

scalability as your projects and devices grow.

4.Carriots lets users collect & store data from connected devices,

build powerful applications, deploy and scale

from prototypes to thousands of devices.

It's features are:

>Real-Time Interactive Visualization.

>End-to-End Security Encryption.

>User-Specified Data Engine Assignment.

>Multi-Tenant Architecture.

>Self-Service Interface.

>Analytical Data Engine.

>Multiple Data Source Reports.

>Sparse Navigation

>Embed Link Generation

Q18):various tools available for security?

We all know that data breaches are on the rise.

Which means that most people are increasing their cyber security IQ, right?

Unfortunately, that's not the case! According to a survey by Pew Research Center,

the majority of people are still unclear about some critically important cyber security

topics, terms and concepts.

Four security tools that everyone should be using:

1.Firewalls

A firewall is the first (of many) layers of defense against malware,

viruses and other threats. It scrutinizes and filters both incoming and outgoing data.

Users can also customize rules and policies based on their needs.

For example, it's often necessary to create exceptions that allow certain

apps to pass through the firewall so that they don't constantly trigger false alarms.

2.Antivirus Software

Signature-based antivirus software scans files (from any source) to make sure that

there aren't any hidden threats. And if it finds something shady or scary,

it can often remove or quarantine the affected file. While antivirus software

certainly isn't bulletproof — especially when it comes to zero-day threats

(i.e. vulnerabilities that hackers have found before software vendors have a chance to patch them and/or users have a chance to install updates) — it's still a critical piece of the cyber security puzzle. There are many options to choose from that range in price from free to hundreds of dollars a year.

3.Anti-Spyware Software

As the term implies, spyware secretly snoops on victims to see where they go online and, even more so, what they type — such as usernames and passwords, and any other confidential or personal data. That's where anti-spyware software fights back by (ideally) detecting and removing threats such as key loggers, password recorders, and so on.

4.Password Management Software

Good password management software not only saves a great deal of time, but it strengthens security and prevents major mistakes, such as saving passwords in web browsers.
If you're looking for something to fit your needs and budget, here is a review of some popular options.

5**.Also there are many more** :

>Wireshark (packet sniffer previously-known as Ethereal) ...

>Metasploit (exploit) ...

>Nessus (vulnerability scanner) ...

>Aircrack (WEP and WPA cracker) ...

>Snort (network intrusion detector) ...

>Cain and Abel (packet sniffer and password cracker) ...

>BackTrack (penetration tester) ...

>Netcat (debugger and exploration tool)

Q19):Discuss URL with respect to:

1.Structure

2.Need

3.Defination

4.Example

ans:

1.Defination of url:

What does URL stand for? URL is an abbreviation which stands for the term Uniform Resource Locator.

It contains a link to the server which is a storage of the searched resource.

In general, URL meaning is the track from the server to the final gadget

(which is a platform of the user's work) can be illustrated rather simply.

The upper element is the resource server, the lowest one – the user's device.

All the points in between the two are additional servers.

A URL is also a specific type of Uniform Resource Identifier (URI).

2.Structure of url:

URL address has a determined structure which includes:

method of access to the resource that is also named the network protocol;

access authorization;

hosts – DNS address that is inscribed as IP address;

port – one more obligatory detail included in combination with IP address;

track – determines the information about the method of gaining access;

parameter – the internal information of resource about the file.

HTTP. The first part is the name of the scheme. Then comes a colon and two slashes (//).

WWW or webreference. The second part is the name of the computer that hosts the document.

:**80**. The third part of the URL, which is optional, is the port number. Computers have a certain number of so-called ports. The meaning of the port is that through it there are interactions of a certain kind. One supports HTTP interactions, the other supports

sending mail, and so on.

something/something.html. The fourth part is also optional. This is the path to the document we want to request. The path is a set of characters separated by slashes (/).

This is very similar to the paths to folders and files on your regular computer.

There is a root folder (directory), inside it, there are other folders, which,

in turn, may contain other folders and files.

?query. The fifth part is the query string, which is also optional.

In fact, the query string is some kind of data intended for a certain program to

process it and return the necessary information. The query string consists of a question mark (?)

Followed by the transmitted information (it completely depends on which program will process it).

3.Need for url:

A URL (Uniform Resource Locator) is the reference point to your website and also

the link that people refer to the most. ... If you want your customers to be attracted

to your website and to keep returning regularly, you have to ensure your URL

is simple, short and user-friendly.

4 EXAMPLE

https://portal.svkm.ac.in/usermgmt/loginSvkm

24. Define / explain following in brief.

• Macro viruses : A macro virus is a virus that is written in a macro language i.e. a programming language that is embedded inside a software application. When a software application is infected, it causes a sequence of actions to begin

automatically when the application is opened.

• File infectors : These are file infecting viruses that usually copy their code onto executable files like .exe and .com. They replicate and spread, and might even damage host programs.

• System or boot-record infectors : These infect executable code found on certain system areas on a disk. They attach to the master boot sector and the USB thumb drives or master boot records on hard disk.

• Polymorphic viruses : It's a kind of virus that uses polymorphic engine to mutate while keeping the original algorithm intact. It changes itself everytime it runs but its function does not change.

• Stealth viruses : It is a virus that uses various mechanisms to go undetected by any kind of anti-virus software.

• Trojans : It is a type of malware that is disguised as legitimate software. Users are tricked into loading and downloading this software by hackers trying to gain the users' personal information.

• Logic bombs : It is a piece of code that is deliberately inserted into a software so that it can set off some malicious function if certain requirements are met.

• Worms : A worm is a malicious, self replicating virus that can spread rapidly throughout a network without human assistance.

• Time Bombs :It is a part of a computer program which will start or stop functioning if a predetermined date or time has been reached.

- Ransomware : A kind of malicious software where the victim's computer data is

locked and encrypted and a ransom is asked to restore access to that data.

Q27) State and Explain Various Type of Attacks

Ans)i) Many types of attacks have been around for a very long time.

ii) What's new is the scale and relative simplicity of attacks in the Internet of Things (IoT) – the millions of devices that are a potential victim to traditional style cyber attacks, but on a much larger scale and often with limited, if any protection.

iii) At its core, IoT is all about connecting and networking devices that up until now have not necessarily been connected. This means that all of those devices, whether it is your brand new connected refrigerator or your connected vehicle, are creating a new entry point to the network and therefore posing an increasing security and privacy risk.

A)Botnets: A botnet is a network of systems combined together with the purpose of remotely taking control and distributing malware. Controlled by botnet operators via Command-and-Control-Servers (C&C Server), they are used by criminals on a grand scale for many things: stealing private information, exploiting online-banking data, DDos-attacks or for spam and phishing emails. With the rise of the IoT, many objects and devices are in danger of, or are already being part of, so called thingbots – a botnet that incorporates independent connected objects.

B)Man-in-the-middle: The man-in-the-middle concept is where an attacker or hacker is looking to interrupt and breach communications between two separate systems. It can be a dangerous attack because it is one where the attacker secretly intercepts and transmits messages between two parties when they are under the belief that they are communicating directly with each other. As the attacker has the original communication, they can trick the recipient into thinking they are still getting a legitimate message. Many cases have already been reported within this threat area, cases of hacked vehicles and hacked "smart refrigerators".

C)Data and Identity Theft : While the news is full of scary and unpredictable hackers accessing data and money with all types of impressive hacks, we are often also our own biggest security enemy. Careless safekeeping of internet connected devices (e.g. mobile phone, iPad, Kindle, smartwatch, etc.) are playing into the hands of malicious thieves and opportunistic finders.

D)Denial of Service : A denial of service (DoS) attack happens when a service that would usually work is unavailable. There can be many reasons for unavailability, but it usually refers to infrastructure that cannot cope due to capacity overload. In a Distributed Denial of Service (DDoS) attack, a large number of systems maliciously attack one target. This is often done

through a botnet, where many devices are programmed (often unbeknownst to the owner) to request a service at the same time.

Q30. Smart health care

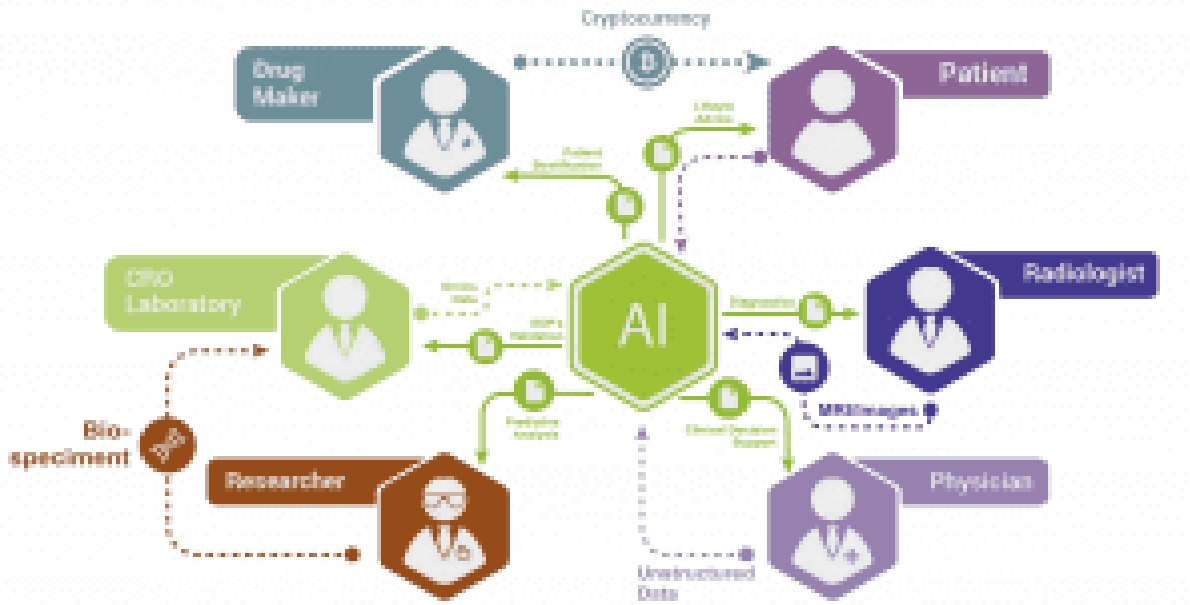
Ans.

'Smart Health Technology' combines Smart Technology and latest mobile device with health. Nowadays, numerous initiatives have been designed to encourage a broader view of health and wellbeing thus smart wearables devices like fitness tracker or fitness bands and even health assessment apps in smartphones have gained grand attention amongst fitness enthusiasts. These devices are smart in the sense as they not only just monitor health but also provide solutions if needed at the right time. Smart devices act as the base of smart healthcare.

Role of technologies in Smart Healthcare

Connectivity provides the foundation of smart city services and it acts as an enabler of smart healthcare as well. With the help of this citizens are able to communicate with authorities easily and it helps authorities as well to gather more health data of its citizens which in return can be used to inform further city and service planning that makes public healthcare a priority. Here IoT plays an important role.

IoT in healthcare allows connecting data collected from smart devices and sensors to extract valuable insights. The technology can play a foremost role in healthcare observation and help in early detection of health issues. It would also help in assimilating the data collected from tests instantly, monitor the condition of the patient, and then convey that information to the doctors and staff in real-time, thus improving the effectiveness in the overall healthcare system. In the near future personal IoT-based health checking devices will change the way, we track the health of individuals.



When the health data is collected it needs to be analyzed and managed for accurate treatment and here Artificial intelligence and automation are applied.

AI is also applied to perform tasks like analyzing laboratory tests, x-rays, CT scans, and data entry. AI-based apps can be used to access the current medical condition of patients that can provide assistance in medical consultation.

Technologies like Blockchain redefine the methods of maintaining and populating Electronic Health Records as well as they also help link them to other services like payments and insurance.

These advanced technologies are very critical in making healthcare a more determinate process, with concrete results, with a service that is more pertinent to the lifestyle of the modern citizen. Continuing innovation and improved data analysis will also help make it an area of constant enhancement that will continue to invent new ways of keeping people fitter and healthier.

Q31. Smart Farming

Ans.

Smart Farming is an emerging concept that refers to managing farms using modern Information and Communication Technologies to increase the quantity and quality of products while optimizing the human labor required.

we'll talk about two major areas of agriculture that IoT can revolutionize:

1. Precision farming
2. Farming automation/robotization

1. Precision Farming

Precision farming, or precision agriculture, is an umbrella concept for IoT-based approaches that make farming more controlled and accurate. In simple words, plants and cattle get precisely the treatment they need, determined by machines with superhuman accuracy. The biggest difference from the classical approach is that precision farming allows decisions to be made per square meter or even per plant/animal rather than for a field.
By precisely measuring variations within a field, farmers can boost the effectiveness of pesticides and fertilizers, or use them selectively.

2. Precision Livestock Farming

As in the case of precision agriculture, smart farming techniques enable farmers better to monitor the needs of individual animals and to adjust their nutrition accordingly, thereby preventing disease and enhancing herd health.
Large farm owners can use wireless IoT applications to monitor the location, well-being, and health of their cattle. With this information, they can identify sick animals, so that they can be separated from the herd to prevent the spread of disease.

Automation in Smart Greenhouses

Traditional greenhouses control the environmental parameters through manual intervention or a proportional control mechanism, which often results in production loss, energy loss, and increased labor cost.

IoT-driven smart greenhouses can intelligently monitor as well as control the climate, eliminating the need for manual intervention. Various sensors are deployed to measure the environmental parameters according to the specific requirements of the crop. That data is stored in a cloud-based platform for further processing and control with minimal manual intervention.

Agricultural Drones

Agriculture is one of the major verticals to incorporate both ground-based and aerial drones for crop health assessment, irrigation, crop monitoring, crop spraying, planting, soil and field analysis and other spheres.

Q33. Difference between IOT and M2M.

Ans.

M2M versus the IoT

M2M	IoT
M2M is about direct communication between machines.	The IoT is about sensors automation and Internet platform.
It supports point-to-point communication.	It supports cloud communication.
Devices do not necessarily rely on an Internet connection.	Devices rely on an Internet connection.
M2M is mostly hardware-based technology.	The IoT is both hardware- and software-based technology.
Machines normally communicate with a single machine at a time.	Many users can access at one time over the Internet.
A device can be connected through mobile or other network.	Data delivery depends on the Internet protocol (IP) network.