1. With your knowledge of iot, discuss

i. Two main challenges for iot management

- Security

IoT has already turned into a serious security concern that has drawn the attention of prominent tech firms and government agencies across the world. The hacking of baby monitors, smart fridges, thermostats, drug infusion pumps, cameras and even assault rifles are signifying a security nightmare being caused by the future of IoT. So many new nodes being added to networks and the internet will provide malicious actors with innumerable attack vectors and possibilities to carry out their evil deeds, especially since a considerable number of them suffer from security holes.

- Connectivity

High heterogeneity remains the biggest challenge to IIoT networks and their connectivity capabilities. This heterogeneity applies to the historically diverse assets of an organization. These often involve old industrial machines and various types of analog equipment. This means machines belonging to different generations and equipped with widely varying capabilities.

ii. The statement "the best interface for a system is no user interface"?

1: The real problem that is mainly faced with an interface is basically it is an interface. In doing any daily task with the interface gets into the way it would be all together a very bad option. The main focus should be on the task and not on the interface which is related to the task. The main aspect that should be followed practically is that the mere job is not basically done on the job or it can be stated that the effort in doing a job is not on the interface it should be putting effort on a job. When a job is directly related to a interface the main design aspect is related to the inherent inhuman, unnatural which directly gives a diminishing return. The better aspect in such a scenario is not putting any emphasis on the interface and full emphasis should be towards the job which is to be performed.

iii. With two examples explain when might this apply

Example 1:

In refrigerators the user interface is implemented to control the overall temperature. This is mainly achieved by the use of a remote control which has a user interface attached to it. The remote can directly control or modify the temperature of the refrigerator and open or close the door. An extra benefit is the child clock system which helps it to protect from childer in accessing it (Takai et al., 2013). If we eliminate the user interface system by implementing sensor the door of the refrigerator can open automatically which would directly reduce the work load.

Example 2:

User interface in the merchant pay role by using of a remote application (Fisher, 2013) the implementation of the no user interface would directly reduce the steps involved in any process and which would be highly beneficial for the user.

2. The three common ways to obtain information from iot devices are sensors,RFID and video tracking. Compare the three technologies by addressing the following:

i. Advantages

ii. Disadvantages

iii. Key requirement for the things.

IoT Devices	Advantages	Disadvantages	Application
Sensors	* affect by calamities like atmospheric and, snow. *can be used in different environmental condition	*signals received are very much difficult to reflect which is mainly from curves or thin and soft objects.	* Alarm system is smart. *washing machine can be considered smart *Smart lightning.
RFID	* 100% code data security is assured which cannot be duplicated * Available in large number of sizes, types and materials.	*cost is more than barcode * Less reliability due to complexity in understanding. *Longer than the Barcode labels. .	* applied to baggage and apparel and pharmaceutical tracking (Gubbi et al., 2013). *It has also application in museum, school and universities.
Video Tracking	* communication with regards to devices. *Automation and control. *Collects information. *with video tracking monitoring is a added advantage (Singh, Tripathi and jara, 2014). * livelihood quality are improved.	*There is not any compatibility of international standard for the monitoring equipments. *complex system is more which can increase the risk related to failure. .	*Human-computer interaction. *Augmentation of reality. *Medical imaging. *Video communication.

3. In context of iot describe

i. Issues associated with security and privacy in the context of the iot.

4: Security Issues

The main aspect related to the security issue is the denial of service attack (DOS) , because of this they're very many websites which can be termed as popular were not able to be accessed. The list was so large that it made a huge wave in the technology the list included Amazon, Netflix and many others. The attack was launched by a malware activity which can be termed as Mirai. The result of the attack was that it launched a scour piece of activity which include the internet of thing devices and then enlisted those devices which included them to the target machine of the activity. (Suo et al., 2012).

Privacy Issues

Much important information which can be termed as personal information where hacked by the hackers in orders to get their personal benefit and it lead to a huge problem in different sphere. The technology directly implemented and it can be related to any banking sector. The banking sector can be considered as the most sensitive aspect of information where all the details of any particular personal can be received quite easily by the practice of hacking (Borgohian, Kumar and Sanyal, 2015).

ii. Two non-malicious issues that iot system could produce.

Access to sensitive data

One of the main IoT challenges is that the devices often record, have access to, and stream sensitive data. Security systems such as cameras and doorbells are increasingly a part of small business networks, and can quickly create major issues if hacked by a cybercriminal. Office equipment, such as printers, are also potential access points - a compromised printer could easily mean that the attacker can view everything that is printed or scanned in an office.

Sabotage

A hacked IoT device will allow the attacker to access its functions. While a coffee-maker might not allow an attacker to do anything more dangerous than brewing a latte, a hacked heating system or machinery can create far more disruption to a business. A bad actor could potentially hold a vehicle and its occupants hostage or demand payment to stop the sabotage of an assembly line.

iii. four security issues that iot system should guard against.

- Incorrect access control

Services offered by an IoT device should only be accessible by the owner and the people in their immediate environment whom they trust. However, this is often insufficiently enforced by the security system of a device. IoT devices may trust the local network to such level that no further authentication or authorization is required. Any other device that is connected to the same network is also trusted. This is especially a problem when the device is connected to the Internet: everyone in the world can now potentially access the functionality offered by the device. A common problem is that all devices of the same model are delivered with the same default password (e.g. “admin” or “password123”). The firmware and default settings are usually identical for all devices of the same model. Because the credentials for the device – assuming that, as is often the case, they are not changed by the user - are public knowledge, they can be used to gain access to all devices in that series. IoT devices often have a single account or privilege level, both exposed to the user and internally. This means that when this privilege is obtained, there is no further access control. This single level of protection fails to protect against several vulnerabilities.

- Outdated software

As vulnerabilities in software are discovered and resolved, it is important to distribute the updated version to protect against the vulnerability. This means that IoT devices must ship with up-to-date software without any known vulnerabilities, and that they must have update functionality to patch any vulnerabilities that become known after the deployment of the device. For example, the malware Linux.Darlloz was first discovered late 2013 and worked by exploiting a bug reported and fixed more than a year earlier.

- Lack of encryption

When a device communicates in plain text, all information being exchanged with a client device or backend service can be obtained by a ‘Man-in-the-Middle’ (MitM). Anyone who is capable of obtaining a position on the network path between a device and its endpoint can inspect the network traffic and potentially obtain sensitive data such as login credentials. A typical problem in this category is using a plain-text version of a protocol (e.g. HTTP) where an encrypted version is available (HTTPS). A Man-in-the-Middle attack where the attacker secretly accesses, and then relays communications, possibly altering this communication, without either parties being aware. Even when data is encrypted, weaknesses may be present if the encryption is not complete or configured incorrectly. For example, a device may fail to verify the authenticity of the other party. Even though the connection is encrypted, it can be intercepted by a Man-in-the-Middle attacker. Sensitive data that is stored on a device (at rest) should also be protected by encryption. Typical weaknesses are lack of encryption by storing API tokens or credentials in plain text on a device. Other problems are the usage of weak cryptographic algorithms or using cryptographic algorithms in unintended ways.

- Insufficient physical security

If attackers have physical access to a device, they can open the device and attack the hardware. For example, by reading the contents of the memory components directly, any protecting software can be bypassed. Furthermore, the device may have

debugging contacts, accessible after opening up the device, that provide an attacker with additional possibilities. Physical attacks have an impact on a single device and require physical interaction. Since it not possible to perform these attacks en-masse from the Internet, we do not recognize this as one of the biggest security problems, but it is nevertheless included. A physical attack can be impactful if it uncovers a device key that is shared amongst all devices of the same model, and thus compromises a wide range of devices. However, in that case we consider sharing the key amongst all devices to be the more important problem, not physical security.

- Lack of Trusted Execution Environment

Most IoT devices are effectively general-purpose computers that can run specific software. This makes it possible for attackers to install their own software that has functionality that is not part of the normal functioning of the device. For example, an attacker may install software that performs a DDoS attack. By limiting the functionality of the device and the software it can run, the possibilities to abuse the device are limited. For example, the device can be restricted to connect only to the vendor's cloud service. This restriction would make it ineffective in a DDoS attack since it can no longer connect to arbitrary target hosts. To limit the software a device can run, code is typically signed with a cryptographic hash. Since only the vendor has the key to sign the software, the device will only run software distributed by the vendor. This way, an attacker can no longer run arbitrary code on a device. To totally restrict the code run on the device, code signing must also be implemented in the boot process, with the help of hardware. This can be difficult to implement correctly. So called 'jailbreaks' in devices such as the Apple iPhone, Microsoft Xbox and Nintendo Switch are the result of errors in the implementation of trusted execution environments.

4. An iot data may be retrieved from various iot sources, including iot devices and network element(e.g sensors, gateway, switches), Iot subscribers and Iot applications. Iot device and network element data is assumed to be collected by collection systems or by collection agents.

i. What are the key differences between a collection system and collection agent

Answer 1 : Collection system is the collection of data. It is a system that evaluates sets of information in a consistent and efficient way. Modern data collection rely on advanced technology to take in huge amounts of data and analyze it correctly. It is used for collecting the data. It facilitates the process of data collection.

Whereas Collection agents are those agents who collect the data but it only collect the critical imaging device metrics necessary to manage a printing environment and they never collect any personal or end user information. They keeps the information secure.

ii. What is iot subscriber data and application data and how are there collected?

Answer 2 : IoT subscriber data - IoT subscriber data is one of the most critical functions in telecommunication industry.With the arrival of 5G and the evolution to cloud architecture , managing all subscriber data and services efficiently has never been so essential to ensure an operator 's business profitability.

Application data - Application data is the information That is specific to a user. It applies to any data created and managed by an application.They are a big part of where our data driven world is headed. These preferences determine the location and configure the cleanup mechanism fro switch 's application. The examples are Profile (name , account number) etc.

These can be collected through various ways -

1. Status data - Most IOT device generates status data data , which are collected are as raw data.

2. Location data - Location data enables you to track packages , pallets in real time.

3. Automation data - Many people are skeptical of device automation. whether its automated lights in an office settings on a thermostat , automation is necessary.