Q1) Five security concerns in Internet of Things:

1) Privacy concerns: 90 percent of devices collected at least one piece of personal information via the device, the cloud or the device's mobile application. Even worse is the fact that many devices transmit the information across network without encryption.

2) Insufficient Authentication/Authorization: A huge number of users and devices rely on weak & simple passwords & authorizations. Many citing users that confirmed accounts with weak passwords also used the same password in the cloud for cloud products.

3) Transport Encryption: Transport encryption is where information that is being transferred from one device to another device is encrypted from the outset of any communication.

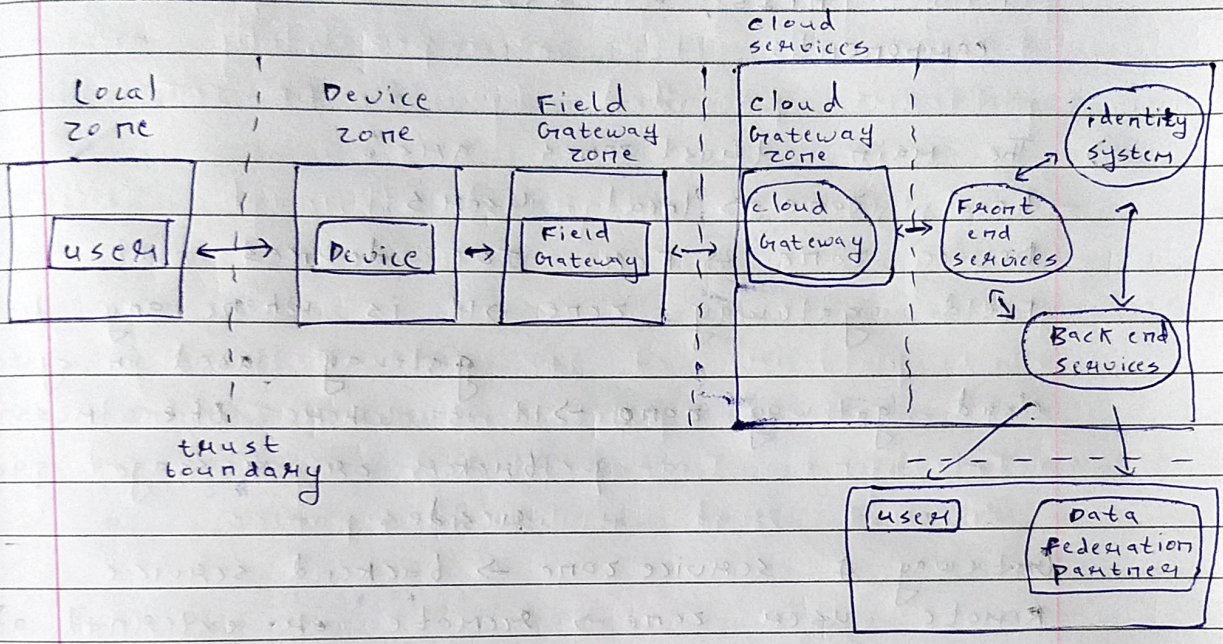
4) Web interface: 60 percent raised security concerns with their user interface. These issues included:
persistent cross-site scripting, poor session management & weak default credentials. From this, hackers were able to identify valid user accounts & take them over using things like password reset features.

Date :
Page No.

5) Insecure Software : 60 percent did not use encryption when downloading software updates. Even worse, some of the downloads that were tested could be intercepted and uploaded into a file system in Linux where the software could be seen or even modified.

Date :
Page No.

Q2) IOT security architecture :-



a) The main components are :-

- Devices : individual IOT devices that are connected to sensors, & other components.
- Field Gateway : It is a software component that serves as a connection point between cloud and one more devices or other Field gateways.
- Cloud Gateway : Instead of running on permissions or local to other devices like field gateways, they run in the cloud.

- Services : It is the bucket of other components of an IOT system backend, like REST APIs, databases or other components

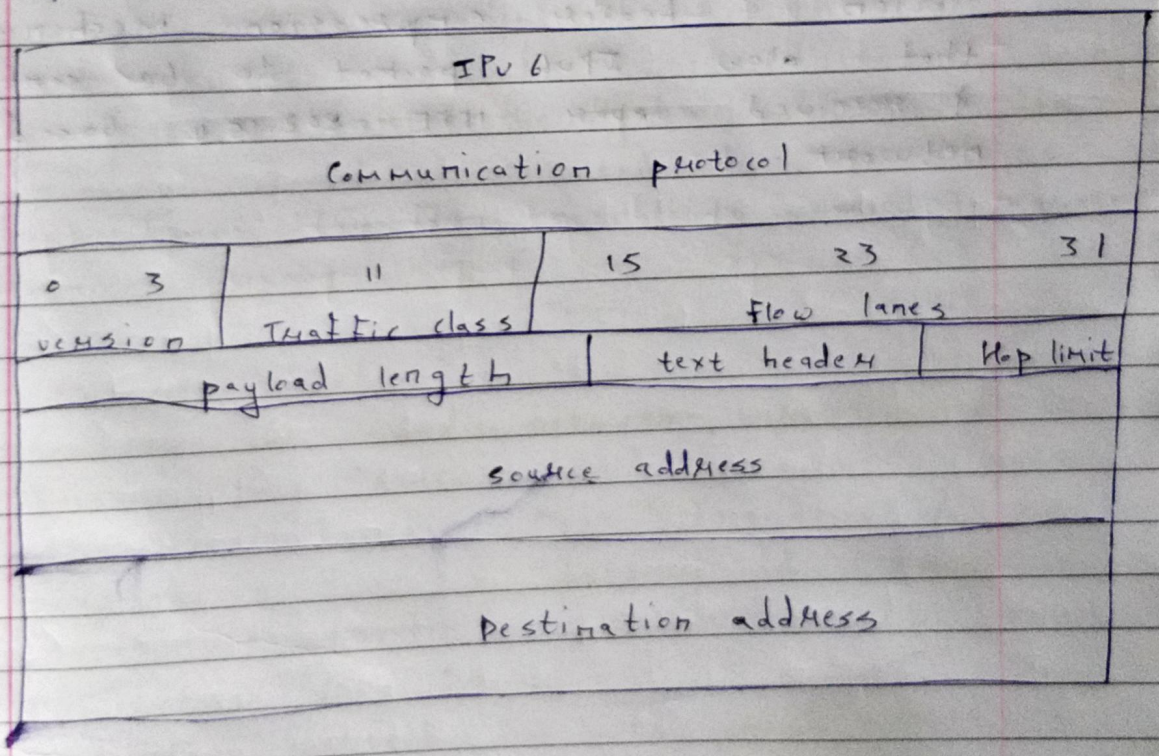
=> The main trust zones are:
Local zone → local users
Device zone → For IOT devices
Field gateway zone → It is where any field gateway used in systems
cloud gateway zone → It is where the message brokers or message queue resides
Gateway & service zone → backend service
Remote user zone → remote or external access to user.

Date :
Page No.

Q3) IPv6 :-

- Internet protocol version 6 (IPv6) is the most recent version of internet protocols, the communication protocol that provides an identification & local system for computers on network & route traffic across internet.

- IPv6 was developed by Internet-Engineering task force to deal with long-anticipated problems of IPv4 address exhaustion.



ii) 6LoWPAN :

- 6LoWPAN is an acronym of IPv6 over Low-power wireless personal Area Network.

- 6LoWPAN is the name of concluded working group in the internet area of IETF.

- The 6LoWPAN concept originated from the idea that "the internet protocol could & should be applied even to the smallest devices & that low-power devices with limited processing capabilities should be able to participate in the IoT".

- The 6LoWPAN group has defined encapsulation & header compression mechanism that allow IPv6 packet to be sent & received over IEEE 802.15.4 based network.

Date :
Page No.

Q4) During the testing of IoT devices in lab connectivity is very easy due to limited devices.

Deploying these devices in real world create different challenges such as bandwidth & Intermittent connectivity.

i) Bandwith :-

- Bandwith consumption by large number of IoT devices is challenge in IoT connectivity.

- Bandwith on cellular network is expensive especially with hundreds & thousands of IoT devices on a network sending request / response signals to your server.

- That is huge server issue and requires a large scale server from handling all this data enhances IoT devices uses less bandwith.

- And need of these band with is going to increase in upcoming time.

- So we are going to need fast connection & more & more bandwith and lightweight network that can seamlessly transfer data between devices and servers.

Date :
Page No.

ii) Intermittent Connectivity :-

- Some IoT devices such as sensors are connected via long distances wireless networks.

- So some time because of interference they are not going to be connected to the network constently.

- Because of this sometimes its difficult to make uniform data across all IoT devices.

Q5) Challenges for the adoption of latest tools & technologies in Agriculture 4.0 :-

(1) Device level :-
- Due to harsh environment like extreme hot, cold, rain, high humidity or exposure of device to wild life damages the electric circuits & disturbs its functionality.
- Also wireless devices has limited battery life
- Cost of devices & sensors are sometimes unaffordable.

(2) Data level :-
- As agriculture 4.0 heavily depends upon the quality of data collected we face issues regarding data like availability, privacy, Integretive or Interpretability.

(3) Network level :-
- Contary to wired network, wireless networks have many issues like connectivity, data transmission rate, Data transmission range, propagation issues, Latency & throughput.

(4) Application level :-

- Application itself has its own issues like real time processing capabilities, Application should be context-aware i.e. it should be aware of metadata, cyber attacks like eavesdropping, data integrity, pos attacks, risk at privacy, Also modularity & reliability.

(5) System level :-

- This includes issues related to system's scalability & flexibility.
- It should be robust, i.e realtime dynamic coping.
- It should adapt & learn new technologies through AI.
- System should get rid of complexity & find ways to keep complexity under check.

18DCE115

Date :
Page No.

Q6) INTER-IoT has a pilot, called INTER-LogP, focused on a use case of smart Transport & logistics

- INTER-IoT offers an interoperable solution in the support scenario of port management.
- Several systems will be able to identify trucks and drivers using different devices.
- This information can be shared under certain predefined rules through interoperability between the platforms involved.
- The use IoT platforms in ports can potentially enable traffic & container Monitoring, gelocation & cargo & vehicles management of storage & cargo processes and improvement of services
- This use case addresses the need of IoT platforms interoperation within port actors such as container terminals, transport companies, the port authority & customers
- Also these benefits can be multiplied through appropriate sharing of valuable information & cooperation among the different IoT platforms in port environments, creating synergies.

Date :
Page No.

- The pilot is mainly composed by an access, control system, and a health emergency system, which are possible fruit of the interoperability among platforms provided by INTER-IOT.

- The platforms integrated through INTER-IOT belong to the main actors of the port:-
  - IoT platforms of the port Authority
  - of one of the port container Terminal
  - Intelligent Transportation systems of several road haulier companies.

18DCE115

Date :
Page No.

Q)

IoT	M2M
Devices have objects that are responsible for decision making	Some degree of intelligence is observed in this
Internet protocols are used such as HTTP, FTP, and Telnet	Traditional protocols & communication Technology techniques are used
Internet connection is required for communication	Devices are not dependent on internet
Supports open API integrations	No support for open API's
Data is shared b/w other applications that are used to improve the end-user experience	Data is shared with only the communicating parties.
Example : smart wearables, big data cloud, etc.	Example : Data and information, sensors, etc.

Date :
Page No.

Q11) Communication & computing are the one of the important elements in IOT.

- Importance of communication :

- In IOT, smart devices communicate with each other via internet
- The communication happens without any human intervention.
- These devices are embedded with sensors, softwares which helps in communication.
- There are also different type of communicat
  1) Human to Machine
  2) Machine to Machine
  3) Machine to Human
- Hence communication in IOT is very important as it enables the smart devices to gather, exchange data which contributes in the success of that IOT product / project.

- Importance of Computing :

- The need of computing in IOT is to be more available & distributed
- The amount of data that is sent to the servers via various smart devices is very huge.
- Without utilizing the collected data, it is useless.

18PCE115

VISION Date: Page No.

- Hence, the need of computing is very important because of collecting, processing, analyzing and visualizing of data to be taken care of.

Date :
Page No.

Q12) Transport Framing in Advance Message Queuing protocol (AMQP) :-

- A Frame is AMQP's basic unit. They are chunks of data that are used to send information from RabbitMQ to your application & vice-versa

- Every frame will have the same basic structure :

Type	channel #	size	payload	End-byte Marker

Frame header

- These are the five parts of a Flame, the first three being its header, followed by payload & end-byte marker, to determine the end of the Frame.

- The header defines the type of Frame the channel this Frame belongs to & its size, in bytes. The payload varries accordingly with the Frame types. so each type of Frame will have a different payload format.

- There are 5 types of Frames defined in AMQP, which are :-

i) Protocol header - This the frame sent to establish a new connection between the broker and a client. It will not be used anymore after the connection.

ii) Method frame - carries a RPC request for response AMQP used a RPC pattern for nearly all kind of communication between the broker & the client.

iii) Content header - Contain specific methods carry a content & the content header frame is used to send the properties of this content.

iv) Body - This is the frame with the actual content, and can be split into multiple different frames if the message is too big. (131KB is the default frame size).

v) Heartbeat - used to confirm that a given client is still alive. If Rabbit MQ sends a heartbeat to a client & it does not respond in timely fashion, the client will be disconnected, as it's considered dead.

Date :
Page No.

Q13) Example of IoT service that uses publish-subscribe communication model :-

- With this, you can send logs to many subscribed destinations simultaneously
- You have the option of creating explicit logging channels or having message receipents log events in more than one destination.
- For example, one endpoint can subscribe to logs & send them on to a centralized system like Splunk or Elastic search.
- At the same time, other endpoints can send logs to screens or save them to a file for localised troubleshooting.
- Yet another use-case is subscribing to transactional logs for compliance purposes
- Publish-subscribe is well salled for this & can thuss add extra flexibility to one of your most important monitoring resources in a number of ways, without writing new code or building expensive redundant systems.
- A well-designed publish-subscribe system also has the ability to send ordered messages to a large number of subscribers suddenly

and simultaneously as they came & go connecting and reconnecting unpredictably and keeping their state in sync.

- In terms of design, this is best handled by outsourcing the task to a designated broker component that is designed to handle busy, haphazard network behaviour.

- offloading the responsibility of massive fanout boosts messages to a broker gives publish-subscribe model a distinct advantage in terms of scale.