1. Arduino has how many **analogue pins**? Q1
   1. The answer is six
2. **constrained devices** are constrained in what functionalities?
   1. Low power
   2. Low memory
   3. Low process resources
   4. constrained node-networks
3. The **second wave** of IT driven transformation enabled? Q3
   1. Coordination and integration across individual activities and with outside suppliers, channels and customers
4. The **cost** .. .. of the .. of the smart connected products as compared to traditional products is towards? Q4
   1. Probably High-fixed
   2. but lower variable cost
5. **Oauth** is an open standard Q5
   1. The answer is access delegation
6. Name two **Network level** IoT vulnerabilities
   1. Inadequate authentication
   2. Improper Encryption
   3. Unnecessary open ports
7. what **bits does IPv6** uses Q8.
   1. 128 bits
8. a most Important learning from the your project

Smart plant watering and remote monitoring System

I learned Present your final design first, and present how you reach to it through the intermediaries steps.

1. Why is **cellular communication** in not suitable or suitable for IoT communication?
   1. LTE networks have not been designed keeping in view IoT devices, they can be even driven
   2. technologies and data plans are relatively expensive
   3. Technologies difficulties in handling large amount of IoT devices, and high energy consumption
   4. why suitable
   5. wide coverage
   6. relatively low deployment costs
   7. high level of security
   8. access to dedicated spectrum
   9. simplicity of management
   10. global availability and considerable reliability
2. Name 5 **components of IoT**
   1. Sensor
   2. Platform
   3. Connectivity
   4. analytics
   5. User interface
3. **Z-wave** Q11.
   1. Home automation
4. What is an **IP-address** Q12.
   1. IP address is a unique number for all machines on the Internet.
5. what are three main **services of cloud**?
   1. Software as a Service SaaS
      1. scalable cloud solutions in SaaS model for IoT
      2. SaaS is software distribution model, third party provide hosts application and makes them available to customers over the internet like office365, Canva
   2. PaaS Platform as A service
      1. For applications and development, providing cloud components to software
      2. a framework they can build upon to develop or customise applications
      3. PaaS make the development, testing , and deployment of application quick simple and cost-effective
   3. IaaS Infrastructure as A service
      1. Self-service models for accessing, monitoring, and managing remote data centre infrastructures such as compute (virtualised or bare metal), storage, networking, and networking services (e.g. firewalls)
      2. Instead of having to purchase hardware outright, IaaS can be purchased based on consumption
6. In internet **traffic HTTP** Q14. what number
   1. Port 80 for web traffic, secure shell for port 22
7. The emergence of so-called **hub devices** in home automation application is an example of Q16
   1. device-to-gateway model
8. In IoT the most common **interaction with internet** will be Q17
   1. Passive engagement
9. Name two **device level** to IoT vulnerabilities
   1. Deficient physical security
   2. insufficient energy harvesting
10. **NFC** stands for Q19
    1. Near-field communication
11. In **Australia, LoRa** frequency is?Q20
    1. North America which **915** Mhz
12. In smart connected products the fundamentally different entity is Q21
    1. What makes smart connected products fundamentally different is not the internet, but the changing nature of the “**things**.”
13. Name the **three core elements** of smart connected products
    1. connectivity
       1. ports antennae, protocols for wired and wireless connections with products, amplifies the capabilities and value of the smart components and enables some of them to exist outside the physical product itself
    2. smart components
       1. all the sensors and processors, amplify the capabilities and value of the physical component
    3. physical components
       1. mechanical and electrical parts
14. Is internet of things a very recent paradigm Q23
    1. The term was first used in 1999, but the first IP-based toaster featured at an Internet conference in 1990
15. What is **ISM band**, advantages and constraints?
    1. ISM stands for industrial, medical and scientific
    2. specific radio frequency is reserved for above purposes
    3. reserved internationally
    4. disadvantage, equipment must tolerate interference generated by ISM applications
    5. users have no regulator protection from ISM device operation
16. Name **three forms of connectivity** in smart products, and give example for each of them
    1. **One to One**
       1. Products directly connects with user or manufacturer, like when a car is hooked up to a diagnostic system
    2. **One to Many**
       1. a single central system connected many products simultaneously, like a car central manufacturer system monitors many cars and provide upgrade ad accomplishes remote service and upgrades
    3. **Many to Many**
       1. Multiple products connect with many other products, like in the farms system there is multiple machines working at the same field and connected with each other, sharing the geo-location information.
17. The **device-to-device** communication as stated in RFC 7452 consideration in smart object Q.26
    1. The device to device communication model represents two or more devices that **directly connect and communicate** between one another , rather than through an intermediary application server
18. **Twython** is a python SDK that aims to provide way to access Q.27
    1. Twitter
19. The **challenges for IoT** effective utilisation can be summarised in following domains Q28
    1. societal, technical, legal
20. Name **three key Requirements of Connectivit**y for IoT and explain them
    1. Availability
       1. should be a fairly good coverage across geographic area
    2. Reliability
       1. It should not be very error-prone
    3. Viability
       1. it should not be too complicated to use
21. Name three **software level** IoT vulnerability
    1. Insufficient Access control
    2. Improper patch management capabilities
    3. Weak programming practices
    4. Insufficient audit mechanisms
22. What is the working principle of **LDR light dependent resistor**?
    1. The changing light will change the resistance of LDR, more precisely the increase of light intensity result in lower resistance
23. Explain **the four core security objectives** of the system that are compromised through different attacks on IoT devices.
    1. Confidentiality
       1. unauthorised access to IoT resources
       2. brute force event, eavesdropping IoT physical measurements of faking device identities
       3. Dictionary attack aim at gaining access to IoT device through executing variants of brute force events, leading to illicit modification of settings or even full control of device functions
    2. Integrity
       1. The detection of unauthorised modification on data and settings
       2. Injecting false data or modification of device firmware
       3. FDI attacks fuse legitimate or corrupted input towards IoT sensors mislead the IoT devices’ data, lead to economic loss and even human life
       4. Firmware is rendered by malicious alteration of the firmware, which induces a functional disruption of the targeted device
    3. Availability
       1. guarantee timely access to resources including data application and network infrastructure
       2. DoS prevent the legitimate users’ timely access to IoT resources like data and services
       3. revoking device from the network or draining IoT resources until their full exhaustion
       4. Device capture: capture alter or destroy a device to retrieve stored sensitive information, including secret keys
       5. **Battery draining** by flooding with messages
    4. Accountability
       1. Guarantees the feasibility of tracing actions and events to the respective user or systems aiming to establish responsibility for actions, any vulnerabilities that hinder the proper logging would be related to accountablity
24. Smart connected products offer **opportunities** for Q33
    1. New functionality, Far greater reliability, Much higher product utilisation, capabilities that cut across and transcend traditional product boundaries
25. From a broad perspective, the confluence of several techs and market trends is making it possible to interconnect more and similar devices **cheaply and easily** today. Name any three of these techs and explain them
    1. **Ubiquitous connectivity**
       1. Low, cost high-speed, pervasive network connectivity
    2. **Widespread adoption of IP-based networking**
       1. a dominant global standard for networking
    3. **computing economics**
       1. greater computing powers, low price, low power requirement
    4. **Miniaturisation**
       1. small and inexpensive sensors but still powerful and good measurement precision
    5. **advances in data analytic**
       1. New algorithms, large computing power, data storage cloud services can analyse large amount of dat.
    6. **rise of cloud computing**
       1. remote, networked computing resources; process, manage and store data, small and distributed devices with powerful back-end analytic and control capabilities.
26. The **longer leg** in LED is Q.35
    1. It’s **positive** anode not negative cathode
27. In smart products some of the functionality even **exist outside** the product give one example of such smart product.
    1. The Bose’new WIFI system, a smartphone application running in the product cloud streams music to the system from the internet
28. The capabilities of smart, connected products can be grouped into **four areas** List them and explain each with an example
    1. Monitory
       1. health devices are collecting data generating from the sensors on patient’s body
    2. Control
       1. embedded software and cloud-based control, you can customise the light setting in your home
    3. Optimisation
       1. airline manufacturer based on the information generated from the engine sensor, trying to design a more fuel-efficiency engine
    4. Autonomy
       1. The combination of monitory control optimisation, many tasks can be completely autonomous, such as self-driving car and floor cleaning robot
29. Which of the below statement regarding the contribution of the IoT to **privacy** holds True? Q.38
    1. It has the potential to aggravate our privacy situation
30. The internet of Things is an **emerging topic** of significance of Q39.
    1. social, economic, technical