Unit 4

Interoperability

- Interoperability is a characteristic of a product or system, whose interfaces are completely understood, to work with other products or systems, present or future, in either implementation or access, without any restrictions.
  - Communicate meaningfully
  - Exchange data or services

Interoperability

- Physical objects can interact with any other physical objects and can share their information
- Any device can communicate with other devices anytime from anywhere
- Machine to Machine communication(M2M), Device to Device Communication (D2D), Device to Machine Communication (D2M)
- Seamless device integration with IoT network

Why Interoperability

- Different operating systems
  - For sensor node: TinyOS, SOS, Mantis OS, RETOS, and mostly vendor specific OS
  - For personal computer: Windows, Mac, Unix, and Ubuntu
- Different databases: DB2, MySQL, Oracle, PostgreSQL, SQLite, SQL Server, and Sybase
- Different data representations
- Different control models
- Syntactic or semantic interpretations

Types of Interoperability

- Device Interoperability
- Data Interoperability
- Semantic Interoperability
- Communication Interoperability
- Connection Interoperability

Security, Privacy & Trust

- There are a number of specific security, privacy and trust challenges in the IoT, they all share a number of transverse non-functional requirements:
  - Lightweight and symmetric solutions, Support for resource constrained devices
  - Scalable to billions of devices/transactions
- Solutions will need to address federation/ administrative co-operation
  - Heterogeneity and multiplicity of devices and platforms
  - Intuitively usable solutions, seamlessly integrated into the real world

Trust for IoT

- There is a need for a trust framework to enable the users of the system to have confidence that the information and services being exchanged can indeed be relied upon.
- The trust framework needs to be able to deal with humans and machines as users.
- The development of trust frameworks that address this requirement will require advances in areas.

- Lightweight Public Key Infrastructures (PKI) as a basis for trust management.
- Lightweight key management systems to enable trust relationships to be established and the distribution of encryption materials using minimum communications and processing resources.
- Quality of Information is a requirement for many IoT-based systems.

- Decentralized and self-configuring systems as alternatives to PKI for establishing trust.
- Novel methods for assessing trust in people, devices and data, beyond reputation systems.
- Assurance methods for trusted platforms including hardware, software, protocols, etc.
- Access Control to prevent data breaches.

Security for IoT

- As the IoT becomes a key element of the Future Internet and a critical national/international infrastructure, the need to provide adequate security for the IoT infrastructure becomes ever more important.
- Advances are required in several areas to make the IoT secure from those with malicious intent.

- DoS attacks are already well understood for the current Internet, but the IoT is also susceptible to such attacks and will require specific techniques and mechanisms.
- General attack detection and recovery/resilience to cope with IoT specific threats, such as compromised nodes, malicious code hacking attacks.
- Cyber situation awareness tools/techniques will need to be developed to enable IoT-based infrastructures to be monitored.

- The IoT requires a variety of access control and associated accounting schemes to support the various authorization and usage models that are required by users.
- The IoT needs to handle virtually all modes of operation by itself without relying on human control.

Privacy for IoT

- As much of the information in an IoT system may be personal data, there is a requirement to support anonymity and restrictive handling of personal information.
- There are a number of areas where advances are required.
- Cryptographic techniques that enable protected data to be stored processed and shared, without the information content being accessible to other parties.

- Techniques to support Privacy by Design concepts, including data minimisation, identification, authentication and anonymity.
- Fine-grain and self-configuring access control mechanism emulating the real world.
- There are a number of privacy implications arising from IoT devices where further research is required, including:

- Preserving location privacy, where location can be inferred from things associated with people.
- Prevention of personal information inference, that individuals would wish to keep private, through the observation of IoT-related exchanges.
- Keeping information as local as possible using decentralized computing and key management.
- Use of soft identities, where the real identity of the user can be used to generate various soft identities for specific applications.

IoT Related Standardizations

- Standards are needed for interoperability both within and between domains.
- Within a domain, standards can provide cost efficient realizations of solutions, and a domain here can mean even a specific organization or enterprise realizing an IoT.
- Between domains, the interoperability ensures cooperation between the engaged domains, and is more oriented towards Internet of Things applications.

- Significant attention is given to the "pre-selection" of standards through collaborative research, but focus should also be given to regulation, legislation, interoperability and certification as other activities in the same life-cycle.

- It would be beneficial to develop a wider approach to standardization and include anticipation of emerging or on-going policy making in target application areas.

- The standardisation bodies are addressing the issue of interoperable protocol stacks and open standards for the IoT.
- This includes as well expending the HTTP, TCP, IP stack to the IoT-specific protocol stack.
- This is quite challenging considering the different wireless protocols like ZigBee, RFID,Bluetooth, BACnet 802.15.4e, 6LoWPAN, RPL, and CoAP.

- Agreed standards do not necessarily mean that the objective of interoperability is achieved.
- The mobile communications industry has been successful not only because of its global standards, but also because interoperability can be assured via the certification of mobile devices and organizations.

- From the point of view of standardisation IoT is a global concept, and is based on the idea that anything can be connected at any time from any place to any network, by preserving the security, privacy and safety.
- Interoperability is a key challenge in the realms of the Internet of Things.
- This is due to the intrinsic fabric of the IoT as: (i) *high-dimensional*, (ii) *highly-heterogeneous*, (iii) *dynamic and non-linear*, (iv) *hard to describe/model*.

Current Situation

- The current M2M related standards and technologies landscape is highly fragmented.
- The fragmentation can be seen across different applied domains where there is very little or no re-use of technologies beyond basic communications or networking standards.
- Even within a particular applied sector, a number of competing standards and technologies are used and promoted.

Device Level Energy Issues

- Challenges in IoT is how to interconnect "things" in an interoperable way while taking into account the energy constraints, knowing that the communication is the most energy consuming task on devices

Low Power Communication

- **IEEE 802.15.4** has developed a low-cost, low-power consumption, low complexity, low to medium range communication standard at the link and the physical layers
- **Bluetooth lowenergy** (BLE) is the ultra-lowpower version of the Bluetooth that is up to 15 times more efficient than Bluetooth.
- **Ultra-Wide Bandwidth (UWB) Technology** is an emerging technology in the IoT domain that transmits signals across a much larger frequency range than conventional systems

- **RFID** proposes a variety of standards to offer contactless solutions.
- Cable-powered devices are not expected to be a viable option for IoT devices as they are difficult and costly to deploy.
- Battery replacements in devices are either impractical or very costly in many IoT deployment scenarios.
- As a consequence, for large scale and autonomous IoT, alternative energy sourcing using ambient energy should be considered.

Energy Harvesting

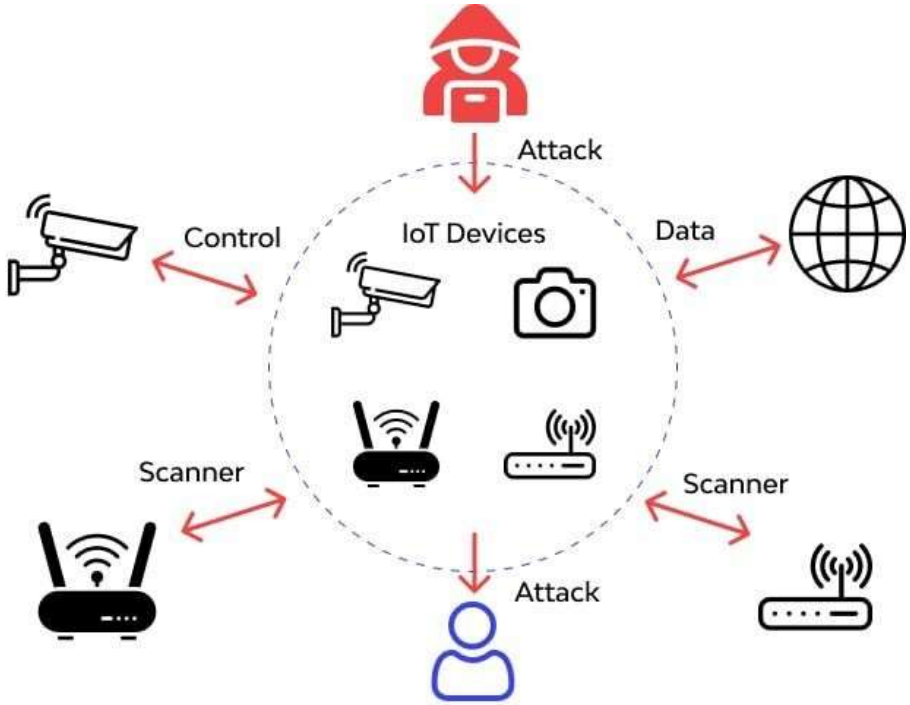
- Four main ambient energy sources are present in our environment: mechanical energy, thermal energy, radiant energy and chemical energy.
- Energy harvesting (EH) must be chosen according to the local environment.
- For outside or luminous indoor environments, solar energy harvesting is the most appropriate solution.
- In a closed environment thermal or mechanical energy may be a better alternative.

IoT Security Challenges

- Most IoT devices are not designed with security in mind, and many do not have traditional operating systems or even enough memory or processing power to incorporate security features.
- IoT devices are growing in number, with over a million new devices connecting to the internet each day.
- The result is a significant quantity of data moving freely between devices and across network environments, remote offices, mobile workers, and public clouds with minimal visibility, making it difficult to track and secure this data.
- IoT devices are vulnerable to hijacking and weaponization for use in distributed denial of service (DDoS) attacks, as well as targeted code injection, man-in-the-middle attacks, and spoofing.
- Malware is also more easily hidden in the large volume of IoT data, and IoT devices sometimes even come with malware already onboard.

IoT Attack Vector

- Botnet
- Ransomware
- AI based Attack
- IoT Device Detection & Visibility
- Convergence
- Unencrypted Data



Vulnerability Exploits

The multitude of components used in IoT devices means that they can have any number of vulnerabilities that attackers can exploit if not addressed immediately.

Malware

Malware, such as Trojans, backdoors, and ransomware, can be spread and deployed through vulnerable applications, devices, firmware, protocols, and other components of IoT systems.

Physical tampering

Deployment in poorly secured locations can expose devices to unauthorized tampering, such as changing circuitry and even replacing them with unsecured devices.

DDOS and DOS

The growing number of IoT devices and their connectivity make IoT susceptible and profitable for botnet attacks, such as those used for distributed denial of service (DDoS).

Man in the middle attack

Insecure protocols and networks can allow attackers to position themselves between communication channels.

Eavesdropping and data theft

Data transmission and storage in IoT systems can be used by intruders to gain access to important information and even to perform real-time monitoring.

IoT Attack Zones

- Devices
  - Assaults could be sent off principally through gadgets.
  - Memory, firmware, the actual connection point, the web interface, and the organization administrations are for the most part weak parts of a gadget.
  - Aggressors can exploit uncertain default settings, obsolete parts, and unstable update components.
- Channel of Communication
  - Assaults against IoT parts can get through the channels that associate them.
  - IoT conventions could have security imperfections that influence the whole framework
- Software & Application
  - Frameworks can be compromised because of imperfections in web applications and related programming for IoT gadgets.
  - Web applications can be utilized to take client qualifications or push noxious firmware refreshes

Attack Prevention Steps

- System-Wide Protections
- Add solid passwords
- Shield against actual altering
  - Ensure that the item has no uncovered ports or connectors that are effectively open to non-workers.
  - Set locks or access limitations on gadgets.
  - Keep IoT gadgets in secure spaces.
  - Try not to leave compact IoT gadgets unattended.
- Utilize a VPN
- Make network division and firewalls
- Switch off friendly sharing elements
- Safeguard PCs, tablets, and cell phones
- Complete network visibility
- Segmentation of IoT devices
- Monitoring, inspection, and policy enforcement
- The ability to take automatic and immediate action

OWASP IoT Attack Surfaces

- ❑ Attack surface ecosystem (general)
- ❑ Third-party backend APIs
- ❑ Device memory
- ❑ Update mechanism
- ❑ Device physical interfaces
- ❑ Mobile application
- ❑ Device web interface
- ❑ Vendor backend APIs
- ❑ Device firmware
- ❑ Ecosystem communication
- ❑ Device network service
- ❑ Network traffic
- ❑ Administrative

OWASP IoT Top 10

- ❑ Weak Guessable, or Hard-coded Passwords
- ❑ Insecure Network Services
- ❑ Insecure Ecosystem Interfaces
- ❑ Lack of Secure Update Mechanism
- ❑ Use of Insecure or Outdated Components
- ❑ Insufficient Privacy Protection
- ❑ Insecure Data Transfer and Storage
- ❑ Lack of Device Management
- ❑ Insecure Default Settings
- ❑ Lack of Physical Hardening

IoT Threat Model

- It is well known that IoT devices are generally lagging in terms of network and information security. This is either due to:
  - manufacturing standards
  - Devices that do not have the computational horsepower or storage space to be secured
- Even if one device is properly secured, unsecured devices can still exist in the organization's ecosystem.
- This entirely bypasses the scope and reach of IT security teams and opening up entire networks to data breaches.
- Architecturally-based IoT threat modeling can reveal these IT security bypasses.
- Without specific IoT security, an organization can easily lose control of their IoT ecosystem attack surface.
- Organizations can, for example, dictate and enforce policies that no personal smart devices are brought into the work environment.

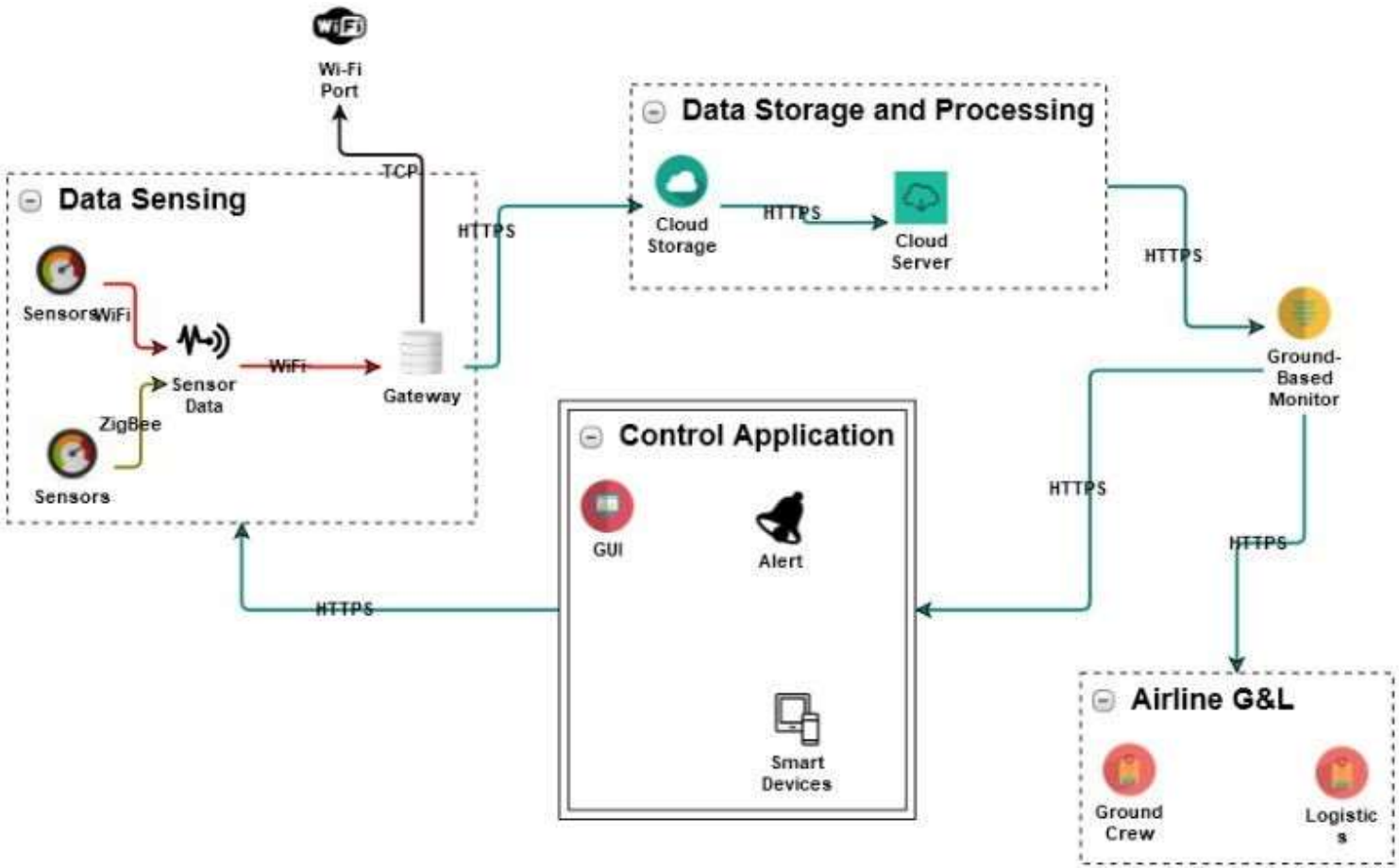
- While it is possible to prevent employees from bringing smart devices into the work environment, it would be difficult to manage visitors with IoT devices from entering the building.
- Securing the IoT ecosystem simply cannot be done by policy mandates.
- Standards and regulations are necessary and inevitable
- however, their implementation is glacial compared to the speed at which the threat landscape evolves for commercial and industrial IoT.
- A tamper-resistant security log is ideal for forensic purposes. But it has the same weaknesses as all security logs:
  - A system event needs to trigger the logging process
  - Security must then sort out the significant events from false-positive “noise.”

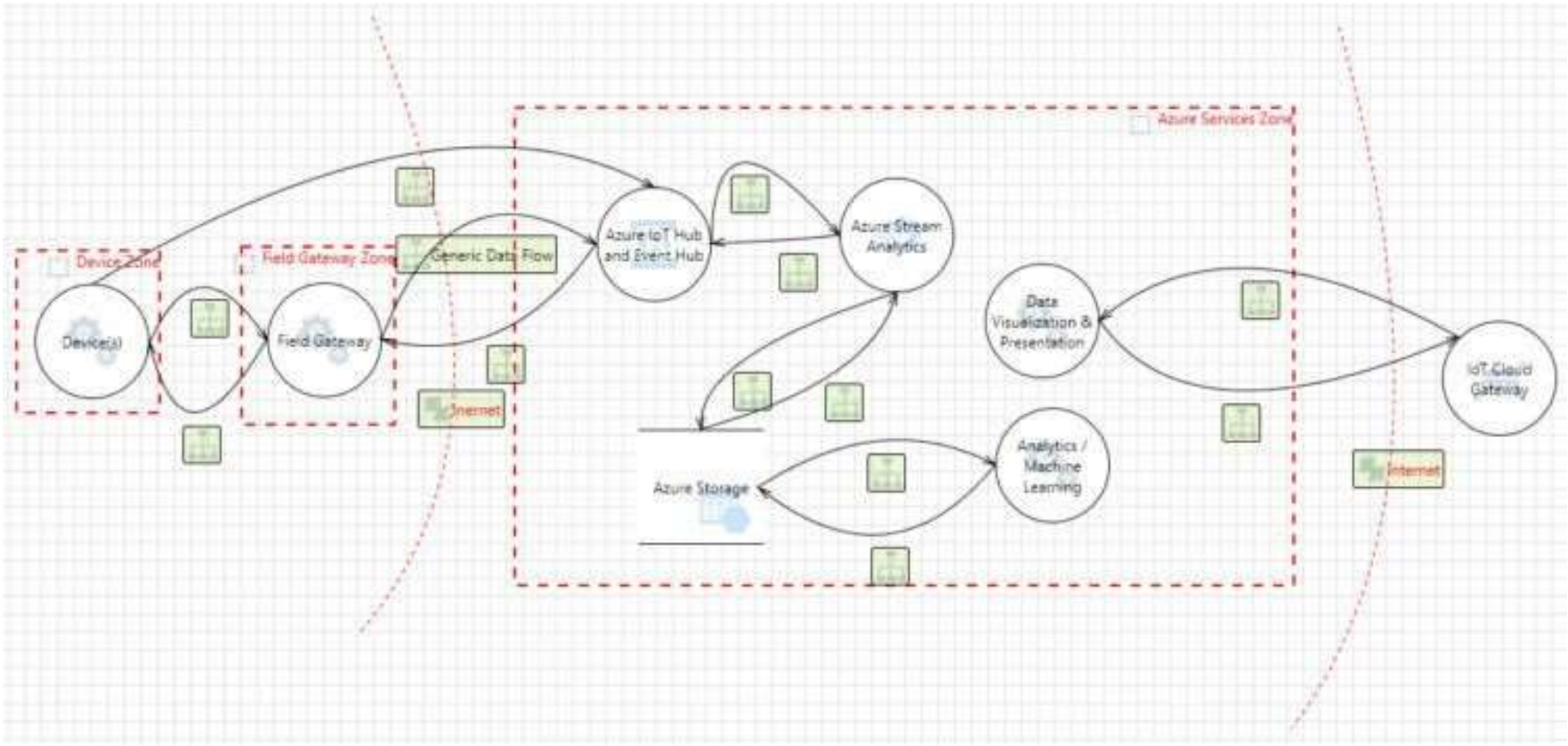
Architectural IoT Threat Modeling

- An architecturally-based IoT threat modeling example provides the answers these decision makers need.
- Threat Modeler's architecturally-based IoT threat modeling can identify specific threats throughout the IoT ecosystem and how such threats impact the larger system.
- Identified Threats:
  - Action Spoofing
  - Alteration of installed BIOS
  - Device Hijack
  - Denial of Service
  - Faking the Data Source
  - Insecure WiFi Channel
  - Manipulating Writable Configuration Files
  - Targeted Malware
  - WiFi Jamming

Steps for Threat Modeling

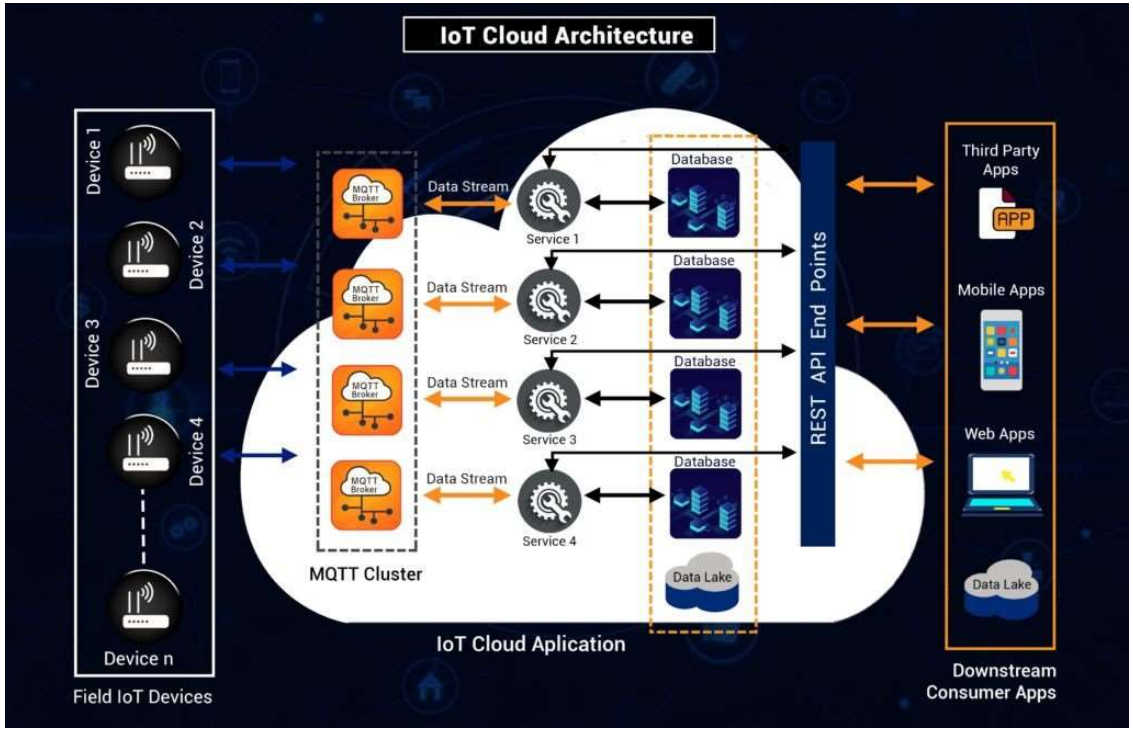
- ❑ System definition
  - ❑ Describe the lifecycle of the system
  - ❑ Describe each of the components of the system
  - ❑ Describe the fundamental operations of the system
- ❑ Identify the trust boundaries
- ❑ Identify the stakeholders
- ❑ Identify the critical assets to be protected
- ❑ Identify attack surfaces
- ❑ Create an adversary model
- ❑ Identify all potential threats
- ❑ Risk assessment of identified threats
- ❑ Define the security functional requirements to mitigate the identified threats
  - ❑ Mitigating actions
  - ❑ Residual risks may remain, and it may be necessary to go through the steps again


Wi-Fi Port
TCP
Data Sensing
Sensors
WiFi
Sensor Data
WiFi
Gateway
ZigBee
Sensors
HTTPS
Data Storage and Processing
Cloud Storage
HTTPS
Cloud Server
HTTPS
Ground-Based Monitor
HTTPS
HTTPS
Control Application
GUI
Alert
Smart Devices
HTTPS
Airline G&L
Ground Crew
Logistics


Azure Services Zone
Device Zone
Field Gateway Zone
Device(s)
Field Gateway
Generic Data Flow
Azure IoT Hub and Event Hub
Azure Stream Analytics
Data Visualization & Presentation
IoT Cloud Gateway
Internet
Azure Storage
Analytics / Machine Learning
Internet

IoT Cloud Security

- Cloud computing offers several advantages to businesses, including greater technological flexibility, reduced operational costs and easy scalability.
- When cloud computing is implemented in an IoT network, the cloud platform and connected applications become highly vulnerable to cyber threats.



IoT cloud security using holistic security principles

- Encryption of data at rest
  - an encryption algorithm is used to safeguard data that is stored on any kind of disk, including backup devices and solid-state drives.
  - Several layers of encryption can be used to protect data at rest.
- Encryption of data in transit
  - it is crucial to ensure that an end-to-end security strategy is in place. In order to protect data in transit.
  - Encrypted connections such as HTTPS, FTPS, SSL, TLS, etc. can also be used.
- Device identity
  - Each device in an IoT implementation should have a unique device identity.
  - When a device comes online, this identity is used to authenticate it and authorize secure communication with other components of the IoT ecosystem.

- Device authentication using OAuth 2.0
  - OAuth 2.0 is a powerful open standard that can be used by API developers to protect an IoT ecosystem.
  - It is a token-based authentication and authorization solution that also offers a framework for the decisions associated with authentication.
- User role and policy
  - create policies that can be attached to identities/resources to define their permissions.
  - The administrator defines the policies and specifies the access level of resources.
- Certificate based authentication
  - A certificate is essentially a signed digital document that includes attributes identifying its issuer and owner
  - The public key can establish a secure communication channel with the subject.
  - The private key is used for proving the identity of the subject once a communication session is established.
  - Certificate based authentication is more powerful than password-based authentication.

IoT Pen Testing Approaches

- penetration testing is a methodical process of scrutinising an organisation's IT system,
- Network or
- web application
- to spot potential vulnerabilities a hacker could exploit.

- Five stages of penetration testing:
- Reconnaissance, Scanning, Vulnerability Assessment, Exploitation, and Reporting.

IoT Pen Testing Approaches

Reconnaissance

- Tester embarks on an intelligence-gathering mission about the target system.
- The collection might encompass a variety of data, including information about IP addresses, domain details, network services, mail servers, and network topology.
- This proactive intelligence gathering provides invaluable insights, helping to sketch a detailed blueprint of the target's environment.
- Armed with this information, the tester can devise an informed testing strategy that can effectively probe for vulnerabilities, setting the stage for the subsequent phases of the penetration testing process.

IoT Pen Testing Approaches

Scanning

- This phase involves an in-depth technical review of the target system.
- Automated tools like vulnerability scanners, network mappers, and others are used to understand how the target system responds to various intrusions.
- Scanning enables testers to determine how the target application behaves under different conditions and to identify potential weak points that could be exploited.
- It maps out the system's digital terrain, enabling the tester to spot possible points of ingress that an attacker might use.

IoT Pen Testing Approaches

- **Vulnerability Assessment**
- Once the target system has been thoroughly scanned, the process proceeds to the Vulnerability Assessment stage.
- This phase is a careful analysis of the target system to identify potential points of exploitation.
- Using a combination of automated tools and manual methodologies, the tester scrutinises the security of the systems, identifying any potential loopholes.
- This meticulous assessment ensures a complete understanding of the system’s security posture, flagging potential vulnerabilities that could be exploited by cybercriminals.

IoT Pen Testing Approaches

Exploitation

- In this critical phase, the tester attempts to capitalise on the vulnerabilities discovered.
- The aim isn't to cause damage but to ascertain the depth of the vulnerability and assess the potential damage it could cause.
- Exploitation might involve data breaches, service disruption, or unauthorized access to sensitive information.
- This stage needs to be carefully controlled and monitored, to ensure that the system isn't accidentally damaged during the process.
- It’s a delicate balancing act between pushing the boundaries and maintaining the integrity of the system.

IoT Pen Testing Approaches

Reporting

- The final stage is Reporting, where the tester compiles a comprehensive report detailing their findings.
- This includes the vulnerabilities discovered, data exploited, and the success of the simulated breach.
- The report is not just a list of issues. It also offers recommendations for addressing the vulnerabilities, including software patches, configuration changes, and improved security policies.
- The report serves as a roadmap, guiding the organization towards a more secure IT infrastructure.

Thank you !