Unit-6 IoT

Illustrate challenges in securing IoT apps.
OR

Q1. Predict the possible challenges in designing secure IoT apps.

ans: Challenges for | Challenges

1. Asset management
- difficulty in maintaining an up-to-date inventory of HW & SW assets.
- IoT device may not have unique identifies : unable to participate in centralised asset management sys : not being able to connect directly to network.

2. Vulnerability management
- manufacturer may stop making patches/releases available IoT device is still in use.
- It may be too risky to install patches or upgrades or make any config changes w/o testings.

3. Access management
- IoT device may support use of one/more shared identities
- may not support use of an existing enterprise user authentication sys.
- Its use of security features may not be sufficiently manageable.

4. Incident detection
- device may not be able to log its operational & security events at all / in sufficient detail.
- It may continue operating even when logging fails.
- It may not be able to execute internal detection controls / interact with external detection controls adversely affecting device operation.

5. Data protection
- device may not provide sufficiently strong encryption for its stored data.
- device may not provide a mechanism for sanitizing sensitive data before disposing it / repurposing the device.

6. Info flow management
- device may not have capability to support configurations like "remote authentication", "preventive", limited data reporting.
- decentralised data processing functions & heterogeneous ownership of IoT devices challenge traditional data management process w.r.t. checking for accuracy of data.

7. PII processing permission management
- device may collect PII indiscriminately / analyse, share / act upon the PII based on automated processes.
- IoT devices may be complex & dynamic with sensing functionality that can collect PII being frequently added & removed.
- device may be accessed remotely allowing sharing of PII outside the control of admin.

8. Informed decision making
- device may lack interfaces that enable individuals to interact w it & read privacy notices.
- decentralised data processing functions & heterogeneous ownerships of IoT devices challenge traditional accountability processes.
- may lack interfaces to enable access to PII & as PII may be stored in unknown locations.

Q.8. Illustrate classic pillars of info assurance while securing the IoT app.

ans: 3 tenets (pillars) of information security (CIA)

1. Confidentiality (C): an act of protecting info from unauthorized disclosure to an entity
The info should be:
a. Protected at Rest: when stored on disk
b. Protected in motion: when transmitted over the network
c. Protect during use: When processing
Confidentiality is enforced using several mechanisms:
- Encryption
- Access control
- data classifica"

Ex: protect ur ATM pin
a. dont write it
b. you can say it in your mind
c. Watch if someone is looking while you type pin.

2. Integrity (I): an act of protecting info from unauth modifica" by an entity
- ensures info remains intact & no unauth entity can modify it.
- any modifica" is allowed only if the entity auth to do so.
- info requires to maintain its integrity
- integrity is enforced using:
  - Hashing
  - access control
  - Data classifica"
  - I/O sanitiza"

Ex: during criminal investigation any evidence collected is protected from touching / any modifica"s to ensure that those evidence can be used during court proceedings

3. Availability (A): an act of protecting info from unauth. destruc" by an entity
- ensures info is adequately protected to remain available when needed
- any unauth entity shouldn't be able to destroy it.
- availability principle extends to any equipment such as comps/ network devices & printers

Ex: your windows / linux sys track all activities done on sys via log files. If I do some mischiefs around your comp & then delete the log files u will have no way to prove that I did anything to your comp. Availability of log files is crucial.

availability enforced using:
1. Access control
2. Isolation
3. Backup
4. Disaster recovery
5. Business continuity processes

Q 3. Illustrate threat model in securing IoT apps.

ans: Threat modelling is a risk based approach towards designing secure sys.
It answers questions like:
1. Where am I most vulnerable to attack
2. What are most relevant threats
3. What do I need to do to safeguard against these threats.

A threat model depends on functionality that sys provides as well as skills that the attacker might have to exploit the vulnerabilities contained in sys.

Threat model for an IoT sys helps you to identify threats & helps you to build a secure IoT sys.
Some common misuse the given / threats in IoT sys are:
- Stealing / manipulating credentials
- unauth. data access.
- Denial of service (DoS)
- Man in the middle (& eavesdropping)
- Tampering identifiers

Threat model for IoT:
Components to analyse:
Devices - sensors, actuators & Edge devices
Network - communication protocols
Cloud - Backend servers storing data / running services
Users - End users interacting with IoT devices & platforms

Common threats:
Physical:
Tampering: unauth access to IoT device
Device theft: data exposure if device is stolen
Network threats:
Eavesdropping: interception of unencrypted data
Man in the Middle - malicious interception of communication
DDoS: overloading IoT networks / services.
Application threats
Unauth access: exploiting weak authentication
Injection attacks: Exploiting the vulnerabilities in app
Firmware exploits: " Outdated / insecure firmware.
Data Threats:
Data breaches: leakage of sensitive user / operational data
Data integrity attacks: unauth modification of data
Cloud threats:
API misuse: Exploiting exposed / insecure API
Credential theft: accessing cloud accounts with stolen credentials.

* Risk assessment:
Steps:
1. Identify assets: devices, networks & data
2. Identify threats: map potential threats to each asset
3. Determine impact: evaluate severity of successful attacks
4. Analyse likelihood: Assess the probability of threat occurring.

Q4. Write a short note on light weight cryptography

ans: many emerging areas in which highly constrained devices are interconnecting, typically communicating wirelessly with one another & work to accomplish some task.

∴ majority of currently cryptographic algos were designed for desktop / server, they don't fit into constrained devices.

Light weight cryptography = subfield of cryptography that aims to provide solutions tailored for resource constrained devices.

Evaluation criterias for choosing NIST approved lightweight cryptographic algos:

1. Minimum acceptability of the submission:
   Evaluⁿ will verify whether the submission meets the min acceptability req. such as cryptographic ops like encryption & decryption. This will include a security evaluation of the algo against known attack that may violate min submission requirements.
2. Side Channel & Fault Attack resistance:
   side channel resistance is the ability for an implementation to reduce the info gained by measurable phenomena about the inner workings of a cryptographic computation. Fault attack alters the normal functioning of a physical electronic device, such that it causes an error in the computation that can be leveraged to perform an attack.
3. cost: submissions will be evaluated in terms of various cost metrics as appropriate
4. Performance: submissions will be evaluated in terms of various performance metrics as appropriate
5. 3rd party analysis: submissions that have significant 3rd party analysis / leverage components of existing algs will be favoured for selecⁿ.
6. Suitability for H/W & S/W implementations:
   an algo may be well suited for both H/W & S/W or it may be specifically tailored for performance in either one.
   submissions that perform that perform well in both will likely be given greater consideration; but a submission that excels in highly constrained H/W may also be granted greater consideration for selecⁿ.

Q.5. What is activity modelling of threats? Explain access control issue w.r.t IoT security

Access control:

mechanisms of access control:

1. Identification: a way to claim an entity's presence w.r.t the process being carried out.
2. Authentication: way to ensure that entity is indeed what it claims to be
3. Authorisation: way to determine what resource an entity can access.
4. Accountability: way to record your actions
5. Non-repudiation: way to prove your actions

Access control ensures only authorized users/devices can access IoT sys. It faces unique challenges:

1. Weak authentication: many IoT devices rely on default or weak passwords, making them vulnerable to auth. access.
2. Lack of role based access: IoT sys often lack granular access control leading to over privileged users/devices.
3. Device to device communication: poorly secured communication. IoT devices can allow attackers to exploit one device to compromise other's.
4. Dynamic environments: IoT networks frequently add/remove devices, making it difficult to maintain updated access control policies.
5. Scalability issues: managing access for large scale IoT deployments is challenging, particularly for industrial IoT (IIoT)
6. Insecure APIs: exposed/unprotected APIs can allow attackers to bypass access control measures.

Mitigation:

- use strong authentication (multi factor authentication)
- Implement least privilege & role based access controls.
- Encrypt communication & secure APIs.
- regularly audit & update access policies.

List out security requirements for IoT base sys.

Q6. Use security concepts to identify diff threats & misuse (atleast 3) in following IoT appns:
i. Smart Home automn
ii. Smart parking sys.
iii. Smart irrigation sys.
iv. forest fire detection sys.

Ans: Security req. of IoT base sys

Protect device Security
- should be secured & protected
- preventing a device from being used to conduct attacks (including participating in distributed denial of service (DDoS) & eavesdropping

asset management
- maintain & current accurate inventory of all IoT devices & their relevant characteristics throughout devices lifecycle to use that info for better security & privacy risk management purposes.

Access management
- prevent unauth & improper physical & logical access to usage & administration of IoT devices
- these tasks are:
1. Identity management
2. Establishing authentication methods & processes.
3. managing roles & permissions & logging all access.

Vulnerability management
- establish a process to identify & eliminate known vulnerabilities in IoT device & firmware to reduce risk of exploitation & compromise.

Device security Incident Detection:
- establish methods & process to monitor & analyse IoT device activity for signs of incidents involving data security. These activities are:
1. security attacks, such as DoS, being carried out on devices
2. Tampering on device unit
3. malfunctioning of devices due to malicious activities.

Protect Data Security
- establish measures to protect the C I A of data collected, stored on & processed by / transmitted to or from an IoT device

Data Protection:
- establish measures to prevent access to & tampering with data at rest / in transit that might expose sensitive info or allow manipulation of IoT device
- mechanisms:
i. Data encryption at rest - provide secure storage
ii. Data encryption in transit
iii. Hashing
iv. Data access control

Data Security Incident Detection
- establish methods & process to monitor & analyse IoT device activity for signs of incidents involving data security.
activities:
1. Attempt to steal security keys
2. Trying to establish connection using obsolete insecure protocols
3. Trying to access data without permission.

Protect Individuals Privacy.
- establish measures to protect individuals privacy impacted by personal info processing beyond device managed through device & data security protection. All IoT devices process personally identifiable info (PII) directly / indirectly should establish such privacy measures.

Info flow management
- maintain accurate, accessible mapping of info & lifecycle of PII
- include the type of data or elements of PII being processed by data actions, entity doing the processing, purpose, additional relevant contextual factors about use of privacy risk management purposes.

PII Processing Permission Management
- maintain permissions of PII processing
- to prevent unpermitted PII processing
- should process their personal info only after their consent.

Informed Decision making:
- enable individual to understand effects of PII processing & interact with device & participate in decision making.
- Individual whose personal data is processed should be informed about it.

Privacy Breach Detection
- establish methods & processes to monitor & analyse IoT device activity for signs of breaches involving individuals privacy activities:
1. attempts to steal personal data of users.
2. Impersonating as legitimate users & trying to read / change personal data
3. collecting more personal data & use than what the user gave consent for.
4. Using the personal data for purposes that are not consented for by the user.

IoT applicaⁿ	Threats	Misuses	Vulnerabilities
1. Smart home automation	1. unauth access to smart devices. 2. Man in the middle attack 3. Data breaches of personal info	1. Spying via hacked camera/mic 2. Unauth control of appliances 3. device used as bot in DDoS attacks	1. default/weak passwords on devic 2. Lack of encryp" in communicaⁿ 3. Unpatched firmwa vulnerabilities
2. Smart Parking sys	1. RFID spoofing to manipulate access 2. Jamming of commun signals 3. Tampering w IoT sensors.	1. Free/unauth parking 2. Misreporting parking space availabili 3. Data misuses (ex: tracking vehicle)	1. Poor authenticaⁿ for payment sys. 2. Insecure network protocols 3. Lack of physical sensor protecⁿ
3. Smart irrigaⁿ sys.	1. Unauth control of water pumps 2. Data manipulaⁿ (ex: weather data) 3. Denial of service (DoS) attacks	1. Overwatering leading to resource waste 2. Tampering w crop specific data 3. Harming crops by decrypting irrigaⁿ	1. Insecure remote access controls 2. Lack of data integrity verificaⁿ 3. Unsecured commun channels.
4. Forest fire detecⁿ sys.	1. False alarm due to spoofed signals 2. Sensor jamming to prevent detecⁿ 3. Data intercepⁿ during transmission	1. Disabling alerts for illegal activities 2. Misuse of collected environmental data 3. Manipulaⁿ of fire detecⁿ results	1. Vulnerable wireless sensor networks 2. Lack of tamper resis H/w 3. Outdated firmwa S/w flaws.

Design an intro to IoT security highlighting unique challenges & vulnerabilities associated to IoT deployments.

Q.7. ans: What are diff vulnerabilities of IoT & how to handle em?
Software vulnerabilities: IoT devices are s/w sys. that could have security flaws & bugs. These IoT devices are often connected to network & use well established protocols for accessing them remotely. S/w vulnerabilities could potentially impact all 3 principles of security - C.I.A

layer no.	layer name	Attacks / vulnerabilities
1.	Physical	- circuits - disrupting signal - jamming RF spectrum - physical media - transmission disturbance
2	Data link	- ARP & MAC flooding - ARP & DHCP spoofing
3.	Network	- IP spoofing - source address spoofing - ICMP flood - Packet sniffing - packet drop attack - other DOS attacks
4.	Transport	- SYN flood - UDP flood - Port scanning - other DoS attacks
5.	Session	- Session hijacking - SSH downgrade - session sniffing
6.	Presentation	- malicious SSL requests - inspecting SSL encryption packets
7.	Applica°	- layer 7 DOS attacks (HTTP flood) - SQL injec° - Cross site scripting - DNS spoofing

handling em:
- Regular updates
- secure development
- Access control
- patch management

2. Hardware vulnerabilities: IoT devices are extensively built on embedded sys & constrained interfaces. These sys could have hw-specific vulnerabilities in hw components. They are also difficult to patch/update. The potentially impact CIA.
handling em:
- tamper resistance: use tamper proof designs & secure boot mechanisms
- H/w security modules (HSM's): Employ HSMs to safeguard cryptographic keys & privileges
- Supply chain security: Ensure components are sourced from trusted suppliers.
- Secure interfaces: protect h/w interfaces from unauth access

3. Cloning of things: during manufacturing, untrusted factory can easily clone physical characteristics, firmware, s/w or security configs of the thing. Deployed things might also be compromised & their s/w reverse engineered allowing for cloning/s/w modifications. Untrusted factory can also change functionality & add malicious functionality to it.
handling em:
- Unique identifiers: use unique H/w ids & secure provisioning
- Cryptographic measures: Employ secure encryp" & digital certificates for authentica"
- Device fingerprinting: use behavioural/environmental data for device valida".

4. Malicious substitution of things: during installation, genuine thing may be replaced by a similar variant w/o being detected. The substitution may also carry malicious attributes behind the scene w/o leaving traces. Which impacts CIA.
handling em:
- Secure boot: verify device integrity during startup using cryptographic sigs
- device authentica": implement mutual authentica" betn device & network
- Blockchain - use decentralised ledgers.

5. Theft of things: IoT devices small size often makes em portable & not adequately protected physically. : can be easily stolen - directly impacts availability principle. Stolen device could be performing a vital task which will further damage premises where it was installed.
handling em:
- Geo fencing: integrate geo" based restric"s to disable stolen devices.
- Remote lock/erase: enable remote capabilities to lock/erase stolen devices.
- Physical security: reenforce the physical design of IoT device against theft

6. Extrac" of private info: an attacker with physical/logical acces to IoT device may perform malicious activities & attempt to extract private info. Even with data encryp" attacker could analyze traffic to deduce meaningful info. This info extrac" is called "info disclosure"/"info leakage" Impacts Confidentiality.
handling em:
- Encryption
- Data minimiza": collect & store only necessary data
- Anonymiza": mask sensitive data to prevent personal info leakage.
- Acess logs: maintain detailed acess logs to monitor data

7. Constrained resources: IoT devices have constrained & limited resources even to carry out security operations like encryption, decryption, authentica", logging & producing traceability records. : constrained resources make IoT devices vulnerable to exploits. Impacts CIA
handling em: - use light weight protocols like CoAP & MQTT.
- use efficient algos for security & communica" - use edge computing & use energy saving modes & low power h/w components.

Q.8. Design a Case study on designing a secure IoT based intrusion detec" sys. Identify Challenges, vulnerabilities threats & considerations involved in ensuring Confidentiality, Integrity & availability of data as well as the timely detec" & response to potential security breaches.

ans: Objective: To design a secure IoT based Home Intrusion Detec" sys (HIDS) that ensures CIA of data while providing timely detec" & response to security breaches.

HIDS includes:

1. IoT sensors: door/window sensors, motion detectors & cameras.
2. Controller: central hub for data aggrega" & local proces"
3. Cloud integra": remote monitoring & control through a secure mobile app.
4. Response mechanism: alerts, alarms & automated act" like locking doors / notifying authorities.

Challenges:

1. Resource constraints: limited computing power & energy in IoT devices.
2. Data sensitivity: risk of private data leakage such as video feeds.
3. Real time processing: Ensuring timely response to potential breaches.
4. Interoperability: managing diverse devices from diff vendors
5. Evolving threats: adapting to new attack methods in IoT ecosys.

Vulnerabilities:

1. Device tampering: physical access to sensors & controllers
2. Weak authentica": default / weak passwords on IoT devices
3. Unencrypted data: data transmission over insecure channels.
4. Sfw bugs: vulnerabilities in firmware & applica"s
5. Denial of service (DoS): overloading sys to cause downtime.

Threats:

1. Eavesdropping: intercepting communica" betw devices
2. Spoofing: impersonating legitimate devices to manipulate sys.
3. Data breaches: unauth access to sensitive data stored locally / on the cloud.
4. Ransomware: locking the sys & demanding payment to restore access.
5. Advanced Persistent Threats (APTs): targeted attacks exploiting multiple vulnerabilities.

Design Considera":

* Confidentiality:
1. Encryption: - End to End encryp" for data in transit using TLS
   - AES for data stored locally / on cloud.
2. Access control: - strong strong authentica" (2FA) for users.
   - Role based access for diff sys components.
3. Data Minimiza": only collect & store necessary data.

Integrity:

1. Secure firmware updates: digitally sign updates to prevent tampering
2. Hashing: Use hashes to verify data integrity
3. Intrusion detec": anomaly based detec" for unusual patterns in sensor data.

★ Availability:

1. Redundancy: Backup power supplies & failover sys
2. DoS protection: rate limiting & traffic filtering mechanis
3. Health monitoring: regular checks on sys. components
   alerts for malfunctions.

★ Timely detection & response:

1. Edge computing: local processing for critical alerts
   reduce latency.
2. AI integration: use ML to identify unusual activity
3. Automated actions: Trigger alarms, notify users & take preventative measures upon breach detection.
4. Incident reporting: detailed logs & real time notifications for users & authorities.