Question Bank IA_2 EIOT

Unit IV: Identity Lifecycle, Authentication & Access Control

1. Define authentication credentials in the context of IoT. (2 Marks)
2. Differentiate between password-based authentication and biometric authentication in IoT. (2 Marks)
3. Explain how 802.1X is used in IoT Identity and Access Management (IAM). (5 Marks)
4. Compare PKI for IoT and symmetric key-based authentication, highlighting scalability challenges. (5 Marks)
5. What is the purpose of OAuth 2.0 in IoT authorization? (2 Marks)
6. Explain IAM identities ?(2 marks)
7. Explain IAM technologies & tools & Benefits? 5 marks?
8. Explain IAM Identity lifecycle with the diagram? 5 marks

Unit V: Mitigating IoT Privacy Concerns & Compliance

1. List any two privacy challenges introduced by IoT. (2 Marks)
2. What is an IoT Privacy Impact Assessment (PIA)? (2 Marks)
3. Describe the Privacy by Design (PbD) principles with respect to IoT devices. (5Marks)
4. Identify two IoT compliance challenges faced by organizations. (2 Marks)
5. Examine how existing compliance standards (e.g., GDPR, HIPAA) support or fail to support IoT. (5 Marks)
6. What is Key Dimensions of IoT Compliance? 2Marks

Unit VI: Enterprise IoT Case Studies

1. Mention one-way IoT is transforming the cleaning service industry. (2 Marks)
2. Explain the role of IoT in Global Cold Chain Management to ensure food safety. (5 Marks)
3. What is Intelligent Lot Tracking in enterprise IoT? (2 Marks)
4. Discuss the Industrial Internet Consortium (IIC) testbeds and their importance in IoT deployment. (5 Marks)
5. Assess the impact of IoT on supply chain transparency using a real-life case study. (5 Marks)

Done, but not read

Remaining to add

READ

What is the purpose of OAuth 2.0 in IoT authorization? (2 Marks)

Definition:

- **OAuth 2.0 is an industry-standard authorization framework that allows a user to grant a third-party application limited access to their protected resources (like data or services) without sharing their login credentials**
- It provides a **secure and standardized way** for IoT devices and applications to get **limited access** to other network services.

Purpose of OAuth 2.0 in IoT Authorization:

Point	Explanation
1. Secure Proxy Access	Enables IoT devices or applications to access resources **on behalf of a user** without using the user's password directly.
2. Token-Based Authorization	Uses **access tokens** instead of usernames and passwords — reducing the risk of credential theft.
3. Fine-Grained Permissions	Devices receive only **specific permissions (scopes)**, ensuring **least-privilege access** (e.g., a smart light can control brightness but not view camera feeds).
4. Supports Multi-Device Communication	Allows different IoT devices (like sensors, hubs, and apps) to securely communicate and share data with each other.
5. Integration with Cloud Services	Commonly used when IoT devices need to access **cloud APIs** (e.g., Google Cloud IoT, AWS IoT).
6. Centralized Authorization Server	OAuth 2.0 uses an **authorization server** that issues and validates access tokens for all IoT devices.
7. No Password Exposure	Users never share their actual credentials with IoT devices — they only authorize access through tokens.
8. Revocable and Time-Limited Access	Tokens can **expire** or be **cancelled**, ensuring better control and security over device access.
9. Interoperability	Works across multiple platforms and IoT systems, enabling secure **cross-platform integration**.
10. Lightweight and Scalable	Suitable for **large-scale IoT networks**, where many devices need controlled access to APIs and cloud services.

Example:

- A **smart home thermostat** uses **OAuth 2.0** to connect to a **cloud weather API**.
- The user grants permission once, and the thermostat gets an **access token** to fetch weather data — without ever knowing the user's login credentials.

Explain IAM identities? (2 marks)

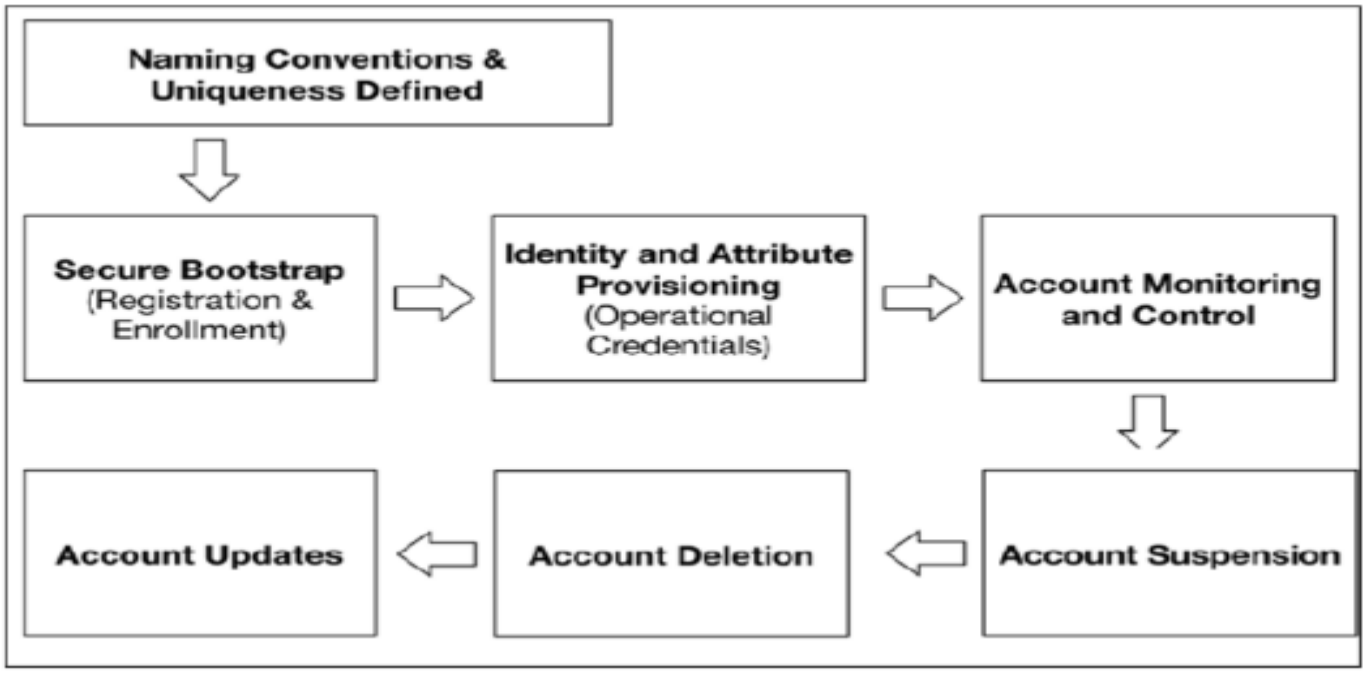
IAM Identities (Identity and Access Management Identities):

- **Definition:**
  IAM identities are **digital representations of users, devices, or applications** that interact with an IoT system.
- **Purpose:**
  They define **who or what** can access resources and **what actions** they can perform.
- **Types:**
  1. **User Identities** – for human users (e.g., admin).
  2. **Device Identities** – for IoT devices (e.g., smart sensor).
  3. **Service Identities** – for apps or cloud services.
  4. **Group/Roles** – for multiple users/devices with same permissions.
- **Functions:**
  Provide **authentication**, **authorization**, and **access control** in IoT systems.
- **Example:**
  A smart home system uses IAM identities so that only the registered user and trusted devices can access or control the home network.

In short:

IAM identities help IoT systems securely identify, authenticate, and authorize users, devices, and services.

Explain IAM Identity lifecycle with the diagram? 5 marks



IAM Identity Lifecycle — Explanation (step-by-step)

---

1. Naming Conventions & Uniqueness Defined

- **What it is:** choose standard names/IDs and rules so every identity is unique and discoverable.f
- **Why:** prevents collisions, simplifies policies and auditing.
- **Example (IoT):** device IDs must follow ORG-ZONE-TYPE-XXXX (e.g., ACME-Z1-TEMP-0101).
- **Best practice:** include device type, location, and serial in the name; record metadata in an inventory.

---

2. Secure Bootstrap (Registration & Enrolment)

- **What it is:** the first-time secure on-boarding process where the device proves itself and receives credentials.
- **How it works:** device authenticates (factory token / one-time password / pre-shared secret) → generates key pair or receives key from authority → CA signs certificate / server issues initial token.
- **Example:** TS-101 (temperature sensor) shipped with a one-time activation code. At install it connects to the company provisioning endpoint, presents activation code, and performs a CSR (certificate signing request); the internal CA signs and returns an X.509 certificate.
- **Controls / Techs:** PKI (ACME / SCEP / EST), TPM / secure element, manufacturer-provisioned tokens, mutual TLS.

3. Identity & Attribute Provisioning (Operational Credentials)

- **What it is:** assign the identity (certificate/keys) and attach attributes/roles/policies needed to operate.
- **Attributes:** device type, owner, allowed network zones, roles, scopes, firmware version, lifecycle state.
- **Example:** TS-101 receives: certificate, role temperature-sensor, allowed topic factory/zone1/temperature, owner ops-team.
- **Best practice:** use automated provisioning (APIs), store metadata in inventory/CMDB, apply least-privilege IAM policies.

---

4. Account Monitoring and Control

- **What it is:** continuous monitoring of identity usage, authentication events, telemetry, and policy enforcement.
- **Why:** detect misuse, anomalous behavior, credential theft, or compromised firmware.
- **Example:** monitor TS-101 for abnormal message frequency, unexpected destinations, failed auth attempts, or firmware drift. Alerts feed into SIEM.
- **Controls / Techs:** logs, SIEM, device health telemetry, behavioral analytics, 802.1X network access control, token expiry checks.

---

5. Account Suspension (temporary block)

- **What it is:** temporarily disable identity access when suspicious behavior or compromise is suspected.
- **How:** revoke certificate or push network/ACL block, rotate tokens, quarantine device.
- **Example:** If TS-101 sends unusual traffic, the IAM/admin suspends it: CA revokes cert and the network blocks it with 802.1X and firewall rules.
- **Outcome:** device cannot access resources until investigated.

---

6. Account Deletion (deprovision / retire)

- **What it is:** permanent removal of identity and credentials when device is decommissioned or determined irrecoverable.
- **Steps:** revoke certs, delete keys from KMS, remove entries from inventory, wipe device credentials (factory reset), update audit records.
- **Example:** TS-101 is retired — CA revokes certificate, device record moved to archive, and any cloud tokens are revoked.
- **Best practice:** keep an audit trail of deletion; sanitize keys and backups.

7. Account Updates (attribute & credential changes)

- **What it is:** modify identity attributes or rotate/update credentials during lifecycle (firmware upgrade, role change, key rotation).
- **Examples:** reassign device to new zone (ZONE1 → ZONE2), renew certificate before expiry, upgrade firmware requiring new capabilities (and updated scopes).
- **When used:** after maintenance, policy change, or when suspension is cleared.
- **Controls:** automated certificate renewal, key rotation policies, update approval workflows.

How the Decision Flow Works (tie to diagram arrows)

- **Naming conventions → Secure bootstrap:** unique naming used during registration so the IAM can identify the device correctly.
- **Bootstrap → Provisioning:** once identity is verified, credentials & policies are provisioned.
- **Provisioning → Monitoring:** device operates and is continuously monitored.
- **Monitoring → Suspension:** anomalies trigger suspension to stop damage.
- **Suspension → Deletion or Updates:** if issue resolved, update/reactivate; if not, delete and retire identity.
- **Account Updates → Monitoring:** updates go back into normal operation and monitored again (closed loop).

Concrete IoT Example — Full Walkthrough (short)

1. **Naming:** ACME-Z1-TEMP-0101 assigned.
2. **Bootstrap:** Technician scans device QR → device sends CSR → CA signs certificate.
3. **Provisioning:** IAM attaches role temp-sensor, allowed MQTT topics, and operator group ops-team.
4. **Monitoring:** SIEM alerts after TS-101 sends 10× normal messages/min.
5. **Suspension:** IAM revokes cert and pushes a network block via 802.1X and firewall.
6. **Investigation:** Firmware was compromised. Decision: delete.
7. **Deletion:** revoke keys, wipe device, update inventory. New device ordered and lifecycle restarts.

Unit V: Mitigating IoT Privacy Concerns & Compliance

Q. What is an IoT Privacy Impact Assessment (PIA)?

Definition:

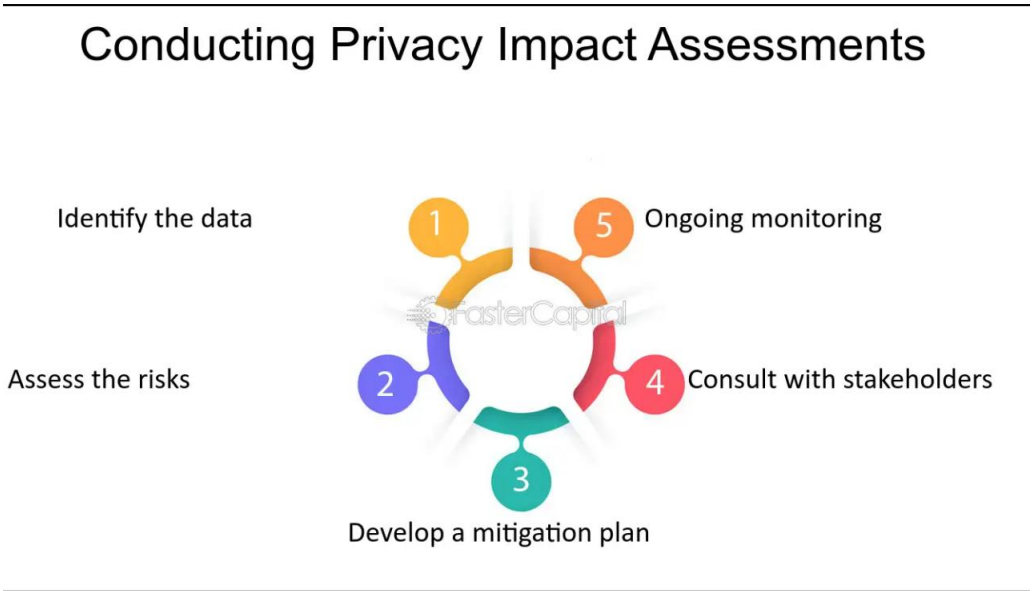
- An **IoT Privacy Impact Assessment (PIA)** is a **systematic process** used to **identify, evaluate, and minimize privacy risks**
- that may arise when collecting, storing, or sharing personal data through IoT devices and systems.

Explanation:

- It ensures that **privacy principles** (like consent, transparency, and data minimization) are followed throughout the IoT system's lifecycle — from device design to data sharing.
- A PIA helps organizations understand **how personal data flows** between IoT components and what measures are needed to **protect user information**.

Key Steps in a PIA:

1. **Identify Data Types:** What personal data the IoT system collects.
2. **Analyse Data Flow:** How data moves between devices, cloud, and third parties.
3. **Assess Risks:** Detect possible privacy breaches or misuse.
4. **Implement Safeguards:** Use encryption, access control, and consent management.
5. **Review and Monitor:** Update the assessment as the system evolves.



Example: Before launching a **smart home system**, a company conducts a PIA to check:

- If voice data is stored securely,
- Who can access it, and
- How long it will be retained.
  The company then adds **data encryption** and **user permission settings** to protect privacy.

Conclusion:

A **Privacy Impact Assessment** helps organizations design **privacy-aware IoT solutions**, reduce legal risks, and maintain **user trust** by proactively managing personal data.

Q. Describe the Privacy by Design (PbD) Principles with Respect to IoT Devices 5M

Definition:

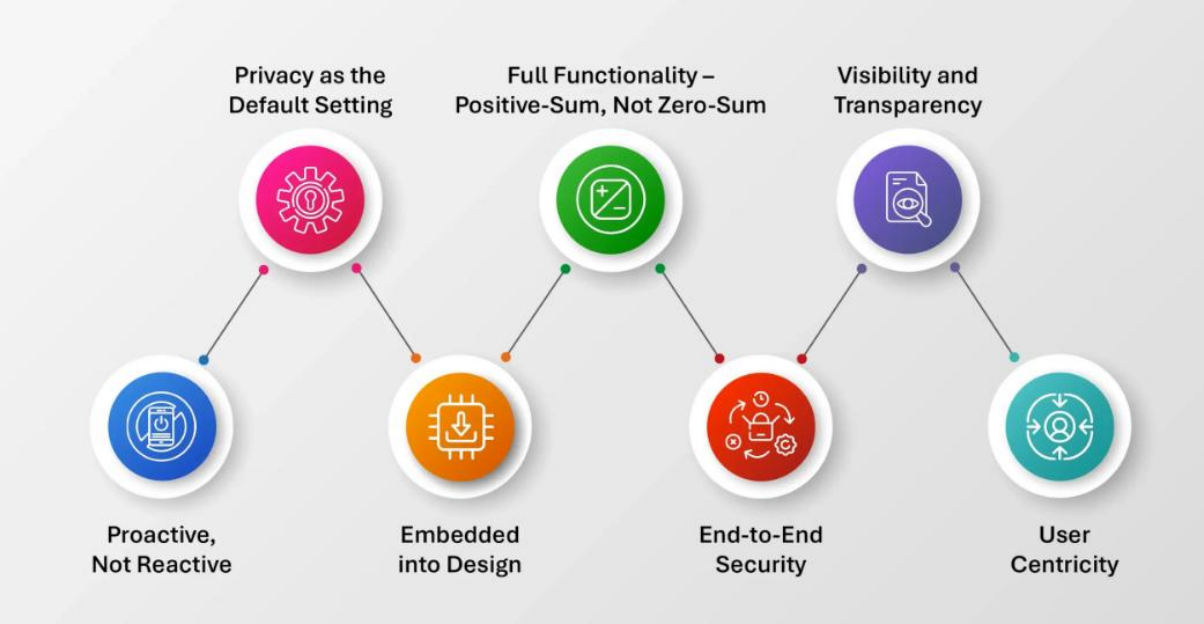
- **Privacy by Design (PbD)** means embedding privacy and data protection measures **directly into the design and architecture of IoT systems and devices**, rather than adding them later.
- It ensures that **data privacy is as important as functionality**, making privacy the **default mode** of operation.

Seven Foundational Principles of PbD in IoT

Principle	Explanation (IoT Context)	Example
1. Proactive, not Reactive; Preventive, not Remedial	IoT manufacturers should **anticipate privacy risks** and design systems to **prevent** them rather than reacting later.	A smart camera company encrypts stored video data by default to prevent misuse, instead of adding encryption after a breach.
2. Privacy as the Default Setting	IoT devices should automatically provide the **highest level of privacy** without requiring user action.	A smart home assistant only collects voice data when the "wake word" is spoken and deletes recordings automatically after processing.
3. Privacy Embedded into Design	Privacy must be **built into every stage** of IoT system design—hardware, software, and network.	A fitness tracker anonymizes user health data before sending it to the cloud, ensuring privacy from the start.
4. Full Functionality – Positive-Sum, not Zero-Sum	Privacy and functionality can **coexist**; protecting privacy should not reduce system performance.	A connected car uses local processing (edge computing) for driver data, maintaining privacy **and** performance.
5. End-to-End Security – Lifecycle Protection	Protect IoT data **throughout its entire lifecycle**—from collection to deletion.	A smart meter encrypts user energy data in transmission, stores it securely, and deletes it once billing is complete.
6. Visibility and Transparency – Keep it Open	IoT organizations must be **open about data practices**, allowing users to understand and verify privacy measures.	A smart home company publishes clear privacy policies explaining how sensor data is collected, used, and shared.
7. Respect for User Privacy – Keep it User-Centric	IoT systems should empower users to **control their data**, respecting their privacy choices.	A smartwatch allows users to manage, download, or delete their personal health data anytime via the mobile app.

Summary:

Privacy by Design in IoT ensures that every connected device — from **smart thermostats** to **industrial sensors** — is developed with **built-in privacy, transparency, and user control**. It builds **trust** between users and IoT providers while ensuring **legal and ethical compliance**.



What are Key Dimensions of IoT Compliance?

Answer:

Key Dimensions of IoT Compliance (Detailed – 10 Points):

1. **Data Privacy:** Ensures that personal information collected by IoT devices is used lawfully and with user consent, following privacy-by-design principles.
2. **Data Security:** Involves implementing encryption, authentication, and access control to protect IoT data during storage and transmission.
3. **Transparency:** Organizations must clearly disclose how, why, and where IoT data is collected, processed, and shared with third parties.
4. **Accountability:** Defines roles and responsibilities for data handling and requires maintaining logs and audit trails for compliance verification.
5. **Regulatory Adherence:** IoT systems must comply with standards like **GDPR**, **HIPAA**, and **ISO 27001** to ensure global legal alignment.
6. **Interoperability:** Promotes the use of standardized communication protocols so IoT devices can securely exchange information across platforms.
7. **Data Integrity:** Focuses on maintaining accuracy, completeness, and reliability of IoT data throughout its lifecycle.
8. **Risk Management:** Involves identifying potential threats and applying mitigation strategies to reduce privacy and security risks.
9. **User Control:** Empowers users to access, correct, or delete their data and manage permissions for data sharing.
10. **Ethical Use:** Encourages fair and responsible use of IoT data, preventing misuse, profiling, or unethical surveillance practices.

Unit VI: Enterprise IoT Case Studies

Mention one-way IoT is transforming the cleaning service industry. (2 Marks)

1. Focus on Health and Cleanliness

After the **COVID-19 pandemic**, there has been a huge rise in awareness about hygiene and safety.
IoT-enabled cleaning devices like **UV disinfection robots** and **touchless sanitization systems** ensure that cleaning happens efficiently without direct human contact, reducing the spread of germs and viruses.

- **Example:** IoT-connected **UV robots** can automatically disinfect rooms in hospitals, offices, or airports and send real-time cleaning reports to supervisors.
- These devices can be remotely monitored and controlled using IoT dashboards to maintain cleanliness levels consistently.

Impact:
IoT ensures **real-time hygiene tracking**, alerts staff when disinfection is due, and provides proof of cleaning completion — boosting **trust and health safety**.

---

2. Robotic Cleaning

The rise of **robotic cleaning systems** is another major IoT-driven change.
These robots are equipped with **sensors, cameras, and AI algorithms** to navigate and clean spaces autonomously.

- **Example:** IoT-powered robots like autonomous vacuum cleaners or mopping robots can map a room, detect dirt levels, and clean efficiently without human intervention.
- They send cleaning data (like completion time and battery status) to a cloud platform for supervisors to review.

Impact:
This allows **human workers** to focus on high-priority tasks like deep cleaning or customer interaction while robots handle routine work — improving **productivity and service quality**.

What is Intelligent Lot Tracking in enterprise IoT? (2 Marks)

Intelligent Lot Tracking in Enterprise IoT

Definition:

- Intelligent Lot Tracking is an **advanced version of traditional lot tracking** that uses **IoT technologies, sensors, cloud computing,**
- **and real-time analytics** to monitor, trace, and manage product batches automatically across the entire supply chain.

Explanation:

- In Enterprise IoT systems, **intelligent lot tracking** integrates **smart sensors**, **RFID tags**, and **IoT-enabled devices** that continuously collect and transmit real-time data (like temperature, humidity, location, or movement) about each lot.
- This data is then analyzed using **AI and cloud platforms** to ensure **transparency, traceability, and quality control** at every stage — from production to delivery.

Example:

In a **pharmaceutical company**, every batch of vaccines is equipped with an **IoT sensor** that records:

- Manufacturing date and batch ID
- Temperature and humidity during storage and transport
- Location data via GPS

If a batch's temperature exceeds safe limits, the IoT system automatically sends an alert to the quality control team, allowing immediate corrective action before the products reach customers.

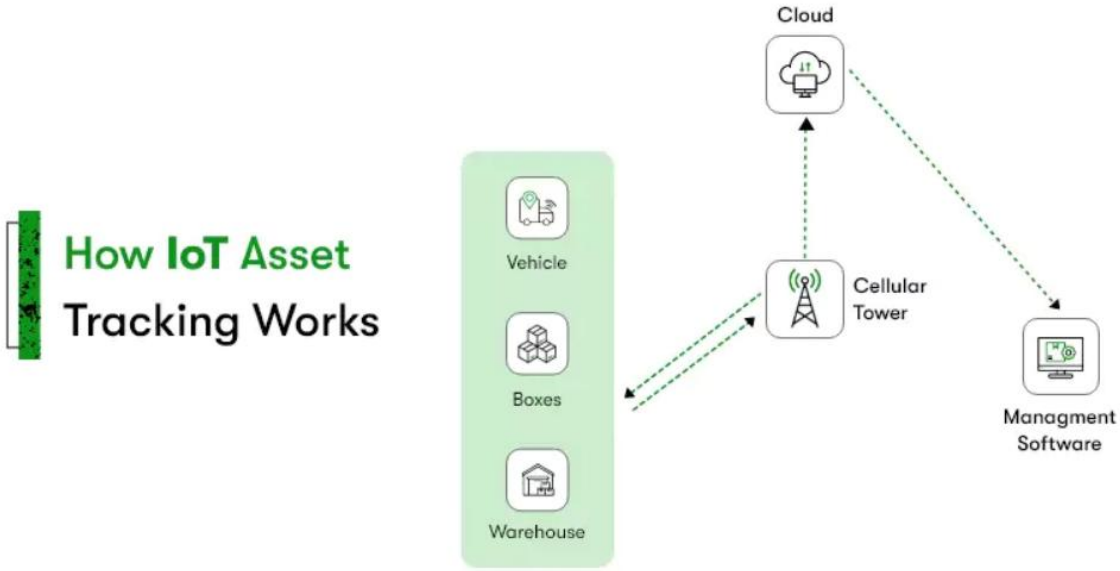
Key Benefits:

Benefit	**Description**
Real-time Monitoring	Tracks product conditions and location continuously.
Automated Alerts	Detects anomalies like temperature rise or delays instantly.

Improved Recall Management	Quickly identifies affected batches in case of defects.
Enhanced Compliance	Meets industry regulations (e.g., FDA, FSSAI, ISO).
Operational Efficiency	Reduces manual tracking and errors using automation.

Conclusion:

Intelligent Lot Tracking in Enterprise IoT ensures **end-to-end product visibility, safety, and regulatory compliance**, making it crucial for industries like **food, pharmaceuticals, and manufacturing** where product integrity is essential.



Impact of IoT on Supply Chain Transparency (with Real-Life Case Study)

---

1. Definition of IoT (Internet of Things)

- The **Internet of Things (IoT)** refers to a network of **interconnected physical devices** (like sensors, RFID tags, GPS trackers, etc.)
- that collect and exchange data over the internet **without human intervention**.

In simple terms: IoT connects machines, goods, and systems to share real-time information for better decision-making.

---

2. Definition of Supply Chain Transparency

Supply Chain Transparency means the ability to **track and trace** every step of a product's journey — from raw materials to the end consumer — providing **visibility into processes, sources, and status**.

It ensures **accountability, ethical sourcing**, and **efficient management**.

---

3. Role of IoT in Supply Chain Transparency

IoT enhances supply chain transparency by:

- Tracking goods in **real time**.
- Monitoring **environmental conditions** (temperature, humidity, etc.).
- Detecting **delays or disruptions**.
- Providing **data for analytics and compliance**.
- Allowing **automated alerts and reports** for decision-makers.

---

4. Real-Life Case Study: Maersk and IBM's TradeLens Platform

Company: *Maersk* (World's largest shipping company)
Technology: *IoT + Blockchain (TradeLens Platform)*

Overview:

Maersk, in collaboration with IBM, implemented **IoT-enabled sensors** and **blockchain-based data sharing** to monitor containers during international shipping.

Implementation:

- Containers were equipped with **IoT sensors** (GPS, temperature, humidity, shock sensors).

- Data collected was shared on the **TradeLens blockchain platform**, accessible by all supply chain participants (ports, customs, shippers, etc.).

Results:

- Real-time tracking of over **18 million containers**.
- Reduction in **paper documentation** and **customs delays**.
- Increased **trust and collaboration** among partners.
- Improved **traceability**, reducing fraud and loss.

---

5. Advantages of IoT in Supply Chain Transparency

Aspect	**Advantages**
Visibility	Real-time monitoring of goods, assets, and vehicles.
Efficiency	Automated inventory tracking reduces manual work.
Risk Reduction	Early detection of issues like theft, spoilage, or damage.
Data Accuracy	Sensor-based data eliminates human errors.
Customer Trust	Transparency improves brand credibility and consumer confidence.
Sustainability	Enables tracking of carbon emissions and eco-friendly sourcing.

---

6. Disadvantages / Challenges

Aspect	**Disadvantages / Challenges**
Cost	High setup and maintenance costs for IoT devices and platforms.
Data Security	Risk of hacking or data misuse.
Interoperability	Integration issues among devices from different vendors.
Complexity	Requires skilled workforce and training.
Data Overload	Managing and analyzing massive real-time data can be difficult.

7. Future Scope of IoT in Supply Chain Transparency

1. **AI & Predictive Analytics Integration** – Predicting delays, demand, and equipment failures.
2. **Blockchain Enhancement** – Immutable, secure data sharing for all stakeholders.
3. **5G Connectivity** – Faster, more reliable data transmission for real-time tracking.
4. **Smart Contracts** – Automated compliance and payments.
5. **Sustainability Monitoring** – Tracking carbon footprint and ethical sourcing in real time.

---

8. Other Real-World Examples

Company	Application of IoT	Outcome
Walmart	RFID tags to track products from supplier to shelf.	Reduced stockouts and improved inventory accuracy.
FedEx	IoT-based SenseAware for parcel tracking.	Real-time visibility and improved customer experience.
Coca-Cola	IoT sensors in vending machines.	Efficient restocking and predictive maintenance.

---

9. Summary

Parameter	Before IoT	After IoT Implementation
Visibility	Limited, manual tracking	Real-time, automated visibility
Transparency	Low, fragmented data	High, shared data ecosystem
Efficiency	Delays and errors	Optimized and accurate
Trust	Lack of accountability	Increased through shared visibility

---

✅ Conclusion

- The **Internet of Things (IoT)** has revolutionized supply chain transparency by enabling **real-time visibility, accountability, and efficiency**.
- The **Maersk–IBM TradeLens** case proves that IoT integration can lead to **smarter, more transparent, and sustainable supply chains**.
- Despite challenges like high costs and data security, the **future of supply chain management is IoT-driven**, supporting **global connectivity, trust, and resilience**.


Warehouse
Distributor
Manufacturer
Retailer
Supplier
Customer
IoT in Supply Chain Management