

# Lecture Notes

## 1. Internet of Things (IoT) Introduction

### Definition

- IoT refers to the network of **physical devices** connected to the Internet that can **collect, exchange, and act on data**.
- Examples: smart home devices, wearable health trackers, industrial sensors, connected cars.

### Key Components

1. **Devices/Sensors:** Collect data (temperature, location, motion, etc.).
2. **Connectivity:** Devices connect to networks via Wi-Fi, Bluetooth, Zigbee, or cellular networks.
3. **Data Processing:** Collected data is processed locally or sent to the cloud for analysis.
4. **User Interface:** Apps or dashboards for users to interact with devices.

### Applications

- Smart homes: lights, thermostats, security cameras.
- Healthcare: remote patient monitoring.
- Industrial IoT (IIoT): predictive maintenance, automation.
- Transportation: fleet management, smart traffic systems.

## 2. Layers of Security in IoT

IoT security involves protecting devices, networks, and data across multiple layers:

## **1. Device Layer**

- Security of the physical device and its firmware.
- Measures:
  - Device authentication
  - Secure boot
  - Regular firmware updates

## **2. Network Layer**

- Security of communication between devices and servers.
- Measures:
  - Encryption (TLS/SSL)
  - Secure protocols (MQTT, CoAP)
  - Network segmentation

## **3. Data Layer**

- Protection of data at rest and in transit.
- Measures:
  - Encryption
  - Access control
  - Data integrity checks

## **4. Application Layer**

- Security of applications accessing IoT data.
- Measures:
  - Strong authentication and authorization

- Input validation
- Monitoring for anomalies

## 5. Cloud Layer

- Security for cloud services storing and processing IoT data.
  - Measures:
    - Identity and access management
    - Security monitoring and logging
    - Compliance with standards (ISO 27001, GDPR)
- 

## 3. Cloud Introduction

### Definition

- Cloud computing provides **on-demand access to computing resources** (storage, processing, networking) over the Internet.

### Key Features

- **Scalability:** Dynamically scale resources as needed.
- **Cost efficiency:** Pay-as-you-go model reduces infrastructure costs.
- **Accessibility:** Access resources from anywhere.
- **Security:** Cloud providers offer security measures (encryption, backups, monitoring).

### Cloud Service Models

1. **IaaS (Infrastructure as a Service):** Virtual machines, storage, networking.
2. **PaaS (Platform as a Service):** Development platforms and tools for building apps.
3. **SaaS (Software as a Service):** Ready-to-use applications delivered via the Internet.

## IoT & Cloud

- Cloud stores and processes the massive data generated by IoT devices.
- Enables remote monitoring, analytics, machine learning, and dashboards.

## 4. Case Studies

### Case Study 1: Mirai Botnet (2016)

- Mirai malware infected IoT devices using **default credentials**, creating a massive botnet for **DDoS attacks**.
- **Lessons Learned:**
  - Change default passwords immediately.
  - Implement automatic security updates.
  - Use network segmentation to limit lateral movement.

### Case Study 2: Capital One Data Breach (2019)

- Misconfigured AWS web application firewall allowed attackers to access **100 million customer records** via server-side request forgery and overly permissive IAM roles.
- **Lessons Learned:**
  - Properly configure cloud security groups.
  - Apply the principle of least privilege to IAM roles.
  - Conduct regular security audits of cloud configurations.
  - Implement automated configuration scanning.

### Case Study 3: St. Jude Medical Cardiac Devices (2017)

- Vulnerabilities in IoT medical devices allowed attackers to **modify pacing or deliver shocks**, demonstrating **life-threatening risks**.

- **Lessons Learned:**

- Critical IoT devices require rigorous security testing.
  - Use secure communication protocols.
  - Apply regular security updates for medical IoT.
  - Ensure regulatory oversight for safety-critical devices.
- 

## Key Takeaways

- IoT connects devices to the Internet, generating massive data.
- Security must be considered at **all layers**: device, network, data, application, cloud.
- Cloud computing is essential for IoT analytics and remote management.
- Real-world case studies highlight the **importance of secure defaults, monitoring, and compliance**.