Week 8 – IOT and Cloud Security

Networks and System Security

Introduction to the Internet of Things (IoT)

Definition

The term **Internet of Things (IoT)** was introduced by Kevin Ashton (1999).
IoT refers to **physical devices** that:

- **Sense** the physical world (via sensors),
- **Act** on the physical world (via actuators),
- Are connected to other devices or the internet.

Examples: smart thermostats, industrial sensors, CCTV cameras, smart appliances.

IoT Devices and Components

Sensors

Devices that **collect data** (e.g., temperature, motion, humidity sensors).
IoT growth projections show billions of connected devices.

Actuators

Devices that **perform actions** (e.g., motors, relays, switches).
They convert digital commands into physical operations.

Developer Kits

Two main categories:

Microcontrollers (MCUs)

- Small computers with CPU, memory, and programmable I/O
- Ideal for simple, low-power IoT tasks (e.g., Arduino)

Single Board Computers (SBCs)

- More powerful; include RAM, storage, OS support (e.g., Raspberry Pi)
- Used for complex IoT workloads

Week 8 – IOT and Cloud Security

Sensors vs Actuators Comparison

Sensors → gather data
Actuators → execute actions
(Examples: accelerometer vs electric motor)

IoT-to-Cloud Interaction

A core concept of IoT is **Machine-to-Machine (M2M)** communication.
Billions of IoT devices connect to:

- Cloud services
- AI analytics
- Big data engines
- Gateways and edge computing

IoT enables smart homes, cities, healthcare, manufacturing, agriculture, and more.

IoT Architecture

4-Layer Architecture

1. **Perception Layer** – sensors and actuators (device layer)
2. **Network Layer** – connectivity (wired/wireless)
3. **Processing Layer** – cloud or middleware, analytics
4. **Application Layer** – user-facing IoT applications

4-Stage Pipeline Architecture

Another way to model IoT systems:

1. **Devices** – sensors/actuators produce data
2. **Internet Gateways** – ingest & pre-process data
3. **Edge Computing** – fast processing near the source

Week 8 – IOT and Cloud Security

4. **Cloud** – storage, analytics, management

IoT Security Challenges

1. Device-Level Vulnerabilities

- **Constrained resources** → weak/no encryption
- **Insecure default configurations** → reused passwords
  - Mirai botnet exploited this
- **Lack of update mechanisms** → unpatched devices
- **Physical insecurity** → tampering, theft

2. Network-Level Threats

- **Man-in-the-Middle attacks** (unencrypted traffic)
- **Protocol vulnerabilities** (Zigbee, Z-Wave, BLE)
- **Poor segmentation** → IoT devices can give attackers lateral access to critical systems

3. Data Privacy and Integrity Concerns

- IoT collects sensitive data (health, movement, behaviour)
- Data tampering → dangerous outcomes (e.g., medical devices, industrial systems)

4. Scalability and Management

- Billions of heterogeneous IoT devices
- Difficulty updating, monitoring, and securing at scale

Week 8 – IOT and Cloud Security

Wired vs Wireless Connectivity

Wired Connectivity

- Reliable, shielded from interception
- Types: twisted pair, coaxial, fibre optic, powerline
- Limitations: distance (e.g., max ~100m Ethernet), physical cable access

Wireless Connectivity

Uses RF or optical signals over air.

Common wireless technologies:

- **Wi-Fi** – common home/business connectivity
- **Cellular (4G/5G)** – remote IoT deployments
- **Bluetooth** – short-range communication
- **Zigbee** – low-power mesh networks
- **LoRaWAN** – long-range, low-power
- **Ethernet** (wired alternative)

Licensed vs Unlicensed Spectrum

Licensed Spectrum

- Less interference
- More predictable environment
- Expensive, regulated

Unlicensed Spectrum

- Free to use
- Easy deployment

- Higher interference risk

IoT Security Best Practices

1. Secure Device Design

- Security-by-design
- TPM, secure boot, hardware encryption
- Remove unnecessary services
- Force password changes & disable default accounts

2. Authentication & Access Control

- Strong/MFA where feasible
- Unique cryptographic identities
- Least privilege
- Certificate-based authentication

3. Secure Communication

- End-to-end encryption (TLS/DTLS)
- Lightweight cryptography (ECC, ChaCha20)
- Use secure protocol versions

4. Monitoring & Updates

- Continuous anomaly detection
- Secure firmware updates (signed, validated)
- Patch management
- Logging & auditing

5. Network Security

Week 8 – IOT and Cloud Security

- VLAN segmentation
- Firewalls
- IDS/IPS tuned for IoT traffic

6. OWASP IoT Top 10

Highlights the most common IoT risks (misconfigurations, insecure communications, weak auth, etc.).

Introduction to Cloud Computing

Cloud providers (AWS, Azure, GCP) deliver:

- Compute (VMs, containers)
- Storage
- Databases
- Networking
- Security services

Cloud Service Models

- **IaaS** – virtual machines, storage, networks
- **PaaS** – managed runtime platforms
- **SaaS** – applications delivered over internet
- **CaaS** – managed containers

Deployment Models

- Public cloud
- Private cloud
- Hybrid cloud
- Multi-cloud

Week 8 – IOT and Cloud Security

Cloud Security Challenges

1. Shared Responsibility Model

- CSP secures **the cloud** (infrastructure, hardware)
- Customer secures **in the cloud** (data, apps, identity)
  Misunderstanding this leads to breaches.

2. Data Security & Privacy

- Data breaches often caused by misconfigurations
- Data sovereignty/residency issues
- Multi-tenancy creates isolation risks

3. Identity & Access Management

- Stolen credentials
- Privilege escalation
- Overly permissive IAM roles

---

4. Misconfigurations (Major cause of breaches)

Examples:

- Public S3 buckets
- Open security groups
- Disabled logging
- Unencrypted storage

---

5. Insecure APIs

Week 8 – IOT and Cloud Security

APIs may be vulnerable to:

- Authentication flaws
- Injection
- DDoS
- Excessive data exposure

6. Account Hijacking

- Phishing
- Credential stuffing
- Exploiting API weaknesses

7. Insider Threats

- Malicious insiders
- Negligent staff misconfiguring resources

8. Vendor Lock-In

- Hard to migrate between cloud platforms
- Supply chain vulnerabilities

10. Cloud Security Best Practices

1. Identity & Access Management

- MFA everywhere
- Least privilege IAM policies

- Continuous role review

2. Data Protection

- Encryption at rest (AES-256)
- Encryption in transit (TLS 1.2+)
- Strong key management (AWS KMS, Azure Key Vault)
- Data classification & DLP tools
- Backup & recovery

3. Network Security

- VPC isolation
- Fine-grained firewall rules
- Network segmentation
- DDoS protection
- WAF for web apps

4. Configuration Management

- Infrastructure as Code (Terraform, CloudFormation)
- Continuous config scanning
- Hardening according to CIS benchmarks
- Compliance automation

5. Monitoring & Incident Response

- Centralized logging (SIEM)
- Real-time monitoring (CloudWatch, Azure Monitor)
- Anomaly detection

- Cloud-specific incident response plans
- Forensics readiness

6. Compliance & Governance

- Align with SOC 2, ISO 27001, HIPAA, PCI DSS
- Use CSPM tools (Prisma Cloud, Dome9)
- Regular audits

7. Container & Serverless Security

- Scan container images
- Monitor runtime activity
- Least privilege for serverless functions
- Secure credential storage

11. Cloud Security Frameworks & Tools

Examples include:

- **CSA Cloud Controls Matrix (CCM)**
- **NIST SP 800-144 / 145 / 146**
- **AWS GuardDuty / Inspector / CloudTrail**
- **Azure Sentinel / Security Center**
- **GCP Security Command Center**

12. IoT–Cloud Convergence

A. IoT–Cloud Integration Architecture

Week 8 – IOT and Cloud Security

IoT relies on cloud for:

- Data storage
- Device management
- Machine learning
- APIs & backend services

B. Combined Security Challenges

1. Extended Attack Surface

- IoT device compromise → cloud compromise
- Cloud compromise → IoT device control

2. Data Flow Security

Every hop (device → gateway → edge → cloud → app) must be secured.

3. Scale & Complexity

Requires:

- Automated security orchestration
- Zero-trust architecture
- Continuous validation

C. Integrated Security Strategies

- **Zero Trust** ("never trust, always verify")
- **Micro-segmentation**
- **Automated threat detection**
- **Security orchestration across layers**
- **Edge computing security**

13. Case Studies

Week 8 – IOT and Cloud Security

1. Mirai Botnet (2016)

Cause: default IoT device passwords
Impact: massive global DDoS attacks
Lessons:

- Change default passwords
- Enable auto-updates
- Segment IoT from critical systems

2. Capital One Breach (2019)

Cause: misconfigured AWS WAF + excessive IAM permissions
Impact: 100+ million customer records stolen
Lessons:

- Enforce least privilege
- Secure cloud configurations
- Automated misconfiguration scanning

3. St. Jude Medical Devices (2017)

Cause: vulnerabilities in cardiac implants
Impact: potential harmful shocks or pacing changes
Lessons:

- Rigorous testing for critical IoT
- Secure communication protocols
- Regulatory oversight

14. Key Takeaways

- IoT and cloud systems form the backbone of modern digital ecosystems.
- Both introduce significant security risks and require specialised controls.
- Security is a **shared responsibility** across manufacturers, cloud providers, developers, and users.

Week 8 – IOT and Cloud Security

- Defence-in-depth is essential — no single control is enough.
- Security must be built from **design → deployment → operation**, not added later.