Large-Scale IoT Infrastructure – Security, Management and Deployment Practices

Across Europe, public and private organizations are rolling out dense IoT sensor networks for example to monitor air quality, groundwater levels, micro-climate, and infrastructure health. Field constraints (spotty connectivity, harsh environments, limited power) collide with enterprise requirements (privacy, security, auditability, repeatable operations). The result is a software-intensive challenge: how do we securely provision thousands of devices, update them without bricking, and prove that our IoT fleet is observable, compliant, and resilient?

The focus of this individual specialization is on **secure fleet management and operations at scale**: over-the-air (OTA) updates, device identity and provisioning, CI/CD for firmware and edge apps, cloud device management, and measuring resilience against realistic failure and attack modes. Students will study current standards and platform capabilities, then validate best practices in a prototype environment that mirrors real-world constraints.

1.1 Assignment scope

Students learn how to secure and operate large-scale IoT fleets end-to-end. That includes: (a) critically applying IoT security frameworks (e.g., NIST/ETSI) to real designs; (b) designing and testing secure OTA update strategies (A/B, staged rollout, rollback safety); (c) comparing and using cloud IoT device-management capabilities (identity/provisioning, device twin/shadow, policy enforcement) on major platforms; and (d) doing rigorous engineering research, literature review, benchmarking, and empirical testing, to justify architectural choices. The emphasis is on practices that hold up under real constraints (lossy links, low power) and on demonstrable operational readiness.

1.2 Example study materials (indicative, not exhaustive)

Standards & guidance

- NISTIR 8259 (Foundational Cybersecurity Activities for IoT Device Manufacturers)
- ETSI EN 303 645 (Cyber Security for Consumer IoT)

MOOCs / docs

- Coursera: IoT Security (University of Colorado)
- edX: Cybersecurity for IoT (University of Washington)
- Platform docs: Azure IoT Hub; AWS IoT Core (identity, provisioning/DPS/JIT, device twin/shadow, OTA)

Books

- Practical Internet of Things Security , Russell & Van Duren
- Designing Connected Products , Rowland et al.

1.3 Capstone project proposal – apply theory to practice

Brief: Build a reproducible testbed with 200+ simulated devices representing mixed field sensors (e.g., air-quality and groundwater level). Integrate with a chosen cloud IoT platform for device identity, provisioning, and policy control. Implement a signed OTA pipeline that supports canary → phased rollout → fleet, with health checks and automatic rollback. Instrument the system for observability (update success rate, latency, failure causes) and evaluate resilience under realistic faults: packet loss, corrupted images, expired certs, and gateway outages. Deliver a short report with results and operator runbooks (emergency patch, device quarantine, key rotation) plus a live demo of a staged rollout with an induced failure cohort and successful recovery.

1.4 Prerequisite knowledge

- Networking: TCP/IP and TLS/SSL basics sufficient to reason about mutual auth and secure channels.
- Software engineering & DevOps: Git, CI/CD pipelines, artifact signing, automated testing.
- Cloud fundamentals: IAM, messaging, storage, and basic service integration (Azure/AWS/GCP).
- Containerization: Docker / Kubernetes fundamentals for building the simulated fleet and tooling.

1.5 Contact information

Ambient Intelligence Research Group, Saxion University of Applied Sciences, Saxion

Website: http://www.saxion.nl/ami

Contact: Javier Ferreira Gonzalez, j.ferreiragonzalez@saxion.nl