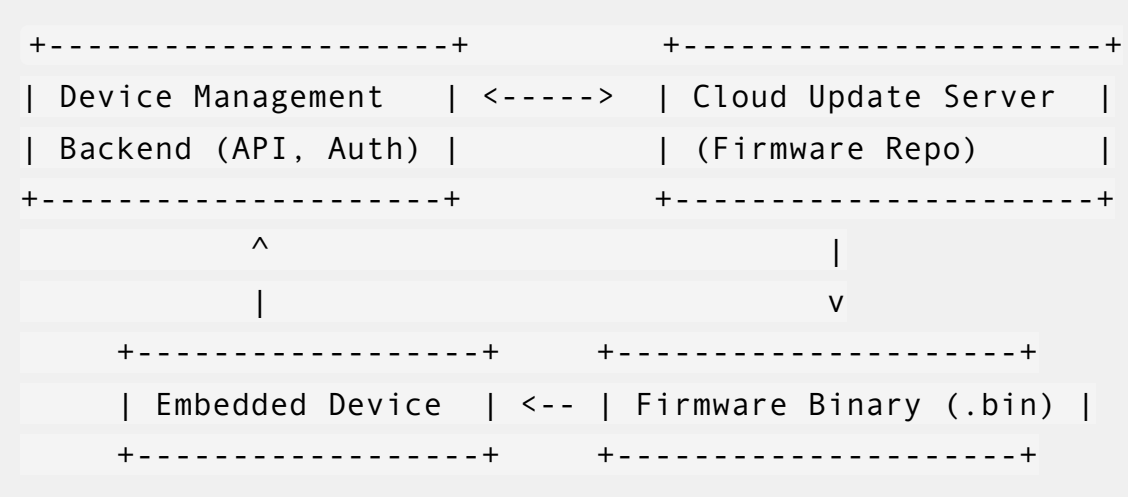
Firmware Over-The-Air (FOTA) Update Mechanism

Firmware Over-The-Air (FOTA) is a method for remotely updating the firmware of embedded devices through a wireless communication channel. Common in IoT devices, smartphones, and automotive systems, FOTA ensures devices stay secure and up-to-date without physical access.

High-Level Architecture



FOTA Process Flow

1. **Version Check** Device queries server: “Is a new firmware available?”
2. **Download Phase** If yes, device downloads the binary in chunks using:
3. HTTP(S)
4. MQTT
5. CoAP

6. LwM2M
7. **Verification**
8. Signature verification using public key cryptography (e.g., RSA/ECC).
9. CRC or SHA-based hash verification.
10. **Flashing**
11. Bootloader writes new firmware to flash.
12. Often done to a secondary slot to support rollback.
13. **Reboot and Validation**
14. Reboot to new firmware.
15. Bootloader performs post-flash health check (e.g., watchdog, diagnostics).
16. If failed, rollback to previous firmware.

Tools and Frameworks

- **Mender.io**
- **Balena**
- **RAUC (Robust Auto Update Controller)**
- **Google OTA (A/B partitions in Android)**
- **SWUpdate**

Summary

FOTA is essential for maintaining, securing, and enhancing connected devices in production. It enables cost-effective, scalable updates while minimizing physical intervention. Designing a robust and secure FOTA mechanism is crucial for modern embedded and IoT systems.