

Autonomous IoT in Mobile Applications

Abstract

Most IoT devices today are "trapped" inside their own apps, making it difficult for information sharing beyond confined, proprietary applications that come bundled with the device. The proliferation of the Internet of Things (IoT) has led to a fragmented landscape of proprietary, siloed applications that hinder data sharing and cross-platform interoperability. This document introduces **DO-Mint** and **DO-Mate**, two multi-platform mobile applications developed by CNRI to integrate the **Digital Object Architecture (DOA)** with IoT environments.

By leveraging the **Digital Object Architecture** and **FDO**, these tools allow individual IoT devices to be registered and managed as **Digital Objects (DOs)**—intelligent "digital twins" that act as secure surrogates for physical hardware. **DO-Mint** facilitates the registration, handle identification, and granular access control configuration of devices, while **DO-Mate** functions as a client for service discovery and secure interaction via QR-code resolution and tokenized authorization. This architectural shift moves security and interoperability from the application layer to the object layer, eliminating "app silos" and providing a standardized, scalable framework for universal IoT discovery and collaboration.

Key Highlights of the DOA Approach:

- **Interoperability:** Replaces disparate proprietary protocols with the standardized DOIP.
- **Object-Centric Security:** Security is baked into the Digital Object itself, rather than the third-party app.
- **Discovery:** Uses unique handle identifiers to allow global discovery of devices and their service interfaces.
- **Automation:** Enables "intelligent" collaboration between devices that were previously unable to communicate.