Reclaiming Digital Autonomy: A Systematic Review of NDN Applications in IoT Systems

LAN WANG, TIANYUAN YU, LIXIA ZHANG

NDNCOMM 2026

The Principle of Science

The principle of science, the definition, almost, is the following: *the test of all knowledge is experiment.* Experiment is the *sole judge* of scientific "truth". But what is the source of knowledge? Where do the laws that are to be tested come from? Experiment, itself, helps to produce these laws, in the sense that it gives us hints.

But also needed is *imagination* to create from these hints *the great generalizations*—to guess at the wonderful, simple, but very strange patterns beneath them all, and then to experiment to check again whether we have made the right guess.

From Feynman Lectures on Physics

The Loss of Digital Autonomy

- The Control Point Shift
  - The control locus has moved away from users to remote cloud providers
- Three Critical Flaws
  - Proprietary Silos: Closed vendor platforms create steep engineering lock-in
  - Fragility & Latency: Every local interaction requires a remote cloud round-trip time (RTT), introducing single points of failure
  - Displaced Security: Trust anchors, key management, and policy enforcement sit entirely off-premises on third-party servers
- The Takeaway
  - Cloud addiction is an inherent, host-centric architectural constraint—not just a business model choice

The Vision: Sovereign IoT Systems

- Private by Design
  - No data leaves the local environment boundary without explicit owner consent
- Locally Autonomous
  - Core workflows and operational features remain fully functional during network partitions or WAN outages
- User-Controlled Trust
  - The device owner holds the cryptographic root of trust, completely bypassing the hardware vendor

Methodology: Tracing a Decade of Evolution

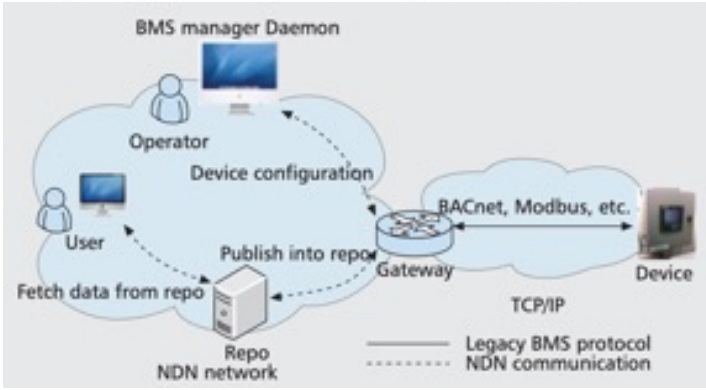
- Large research investigations into ICN/NDN-based IoT solutions
  - Gemini estimate: total number of peer-reviewed papers around 400~600+ papers
  - Across many different aspects, with performance gains as a common focus
- This talk focuses on the NDN team's work in involving *IoT system designs* from feasibility proof to enabling digital autonomy
  - 2014 Securing Building Management Systems Using Named Data Networking
  - 2016 Named Data Network of Things,
  - 2017 Breaking out of the Cloud: Local Trust Management and Rendezvous in Named Data Networking of Things
  - 2019 Publish-Subscribe Communication in Building Management Systems over Named Data Networking
  - 2021 Trust schemas and ICN: key to secure home IoT
  - 2022 Sovereign: Self-contained Smart Home with Data-centric Network and Security

2014–2016: Feasibility and Scaling Down

- 2014: Building Management System
  - Milestone: First end-to-end NDN deployment in a live physical environment
  - Contribution: Proved that hierarchical, semantically meaningful naming binds security directly to data objects rather than communication pipes

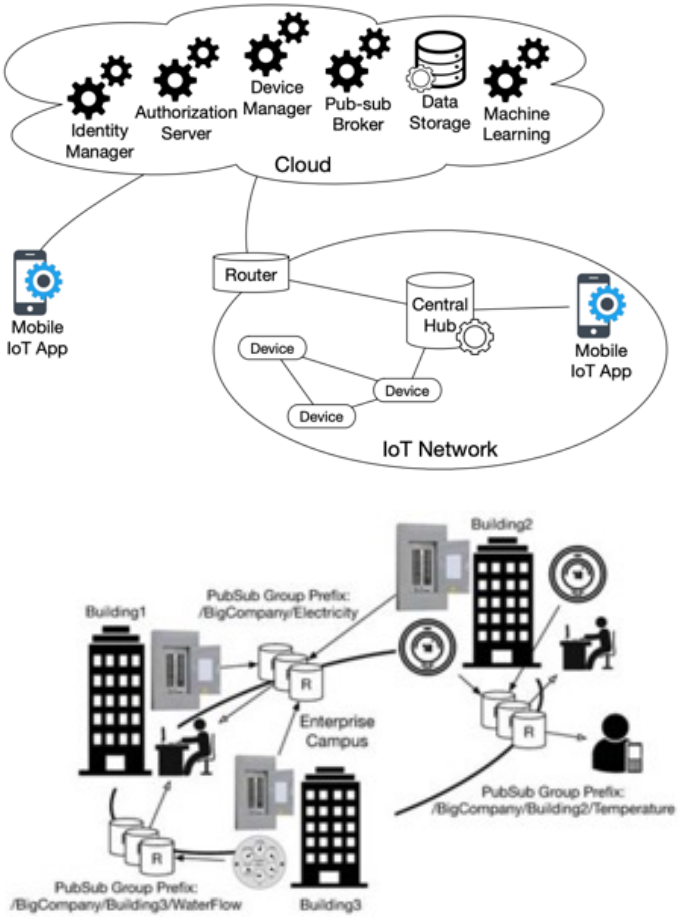
UCLA Strathmore building monitoring system deployment: a) monitored building; b) electrical demand monitor; c) chilled water flow meter.

- 2016: Named Data Networking of Things (NDNoT)
  - Milestone: Generalization of data-centric networking to highly constrained edge hardware
  - Contribution: aligning network and application semantics, enabling developers to work with “things” and their data directly and efficiently



2017–2019: The Autonomy Pivot & The Connectivity Plane

- 2017: Breaking Out of the Cloud
  - Milestone: Cloud dependence came from the architectural placement of trust and coordination.
  - Contribution: Relocate the trust anchor to the local system; rendezvous devices via shared namespace
- 2019: Pub-Sub over State Vector Sync (SVS)
  - Milestone: Eliminating centralized message brokers (e.g., cloud-managed MQTT)
  - Contribution: data-centric design combined with distributed synchronization to maintain state consistency among devices

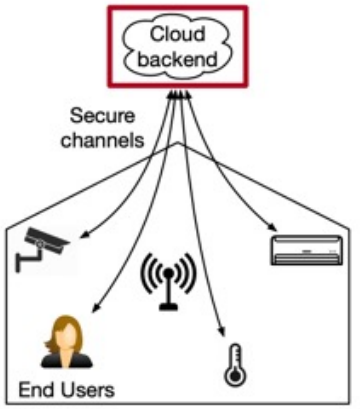


2021—Automating Usable Security via Trust Schemas

- The Usability Bottleneck:
  - In NDN, every data packet must be cryptographically signed and verified.
  - Manually managing which keys sign which data points is complex and prone to human error.
- Core Contribution: Introduced automated trust schema execution
  - For Producers: Automates the signing decision process and key creation loops without requiring manual system-administrator oversight.
  - For Consumers: Automates data packet verification by dynamically discovering the correct validation keys.
- Takeaway: Proved that strict, data-centric security enforcement can be fully automated

2022: Sovereign (The Integrated System Realization)

- System Realization
  - A fully self-contained smart home architecture that synthesizes a decade of research lessons
- Key Architectural Properties
  - Fully local trust management, hierarchical naming, and direct device-device communication
  - Eliminating dependencies on vendor PKI or external Certificate Authorities (CAs)
- The Paradigm Shift
  - Proves that moving control, trust, and rendezvous out of the cloud into user-owned environments is a deployable reality, with resource-constrained devices

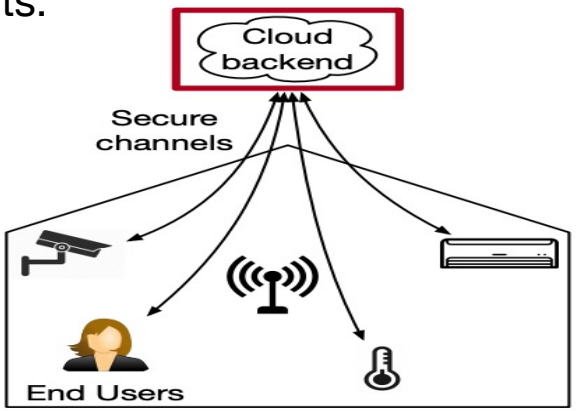


(a) Cloud-based Smart Home
Control enforced in the cloud

(b) **Sovereign**
Control enforced on devices

Conceptual Comparison: Two Competing Philosophies

- Industry Model: Cloud-Managed Aggregation
  - Data flows to cloud; control commands flow back.
  - vendor controls identity, trust anchors, and policies.
  - Security relies on channel encryption
  - Devices: merely as sensor or actuator endpoints.

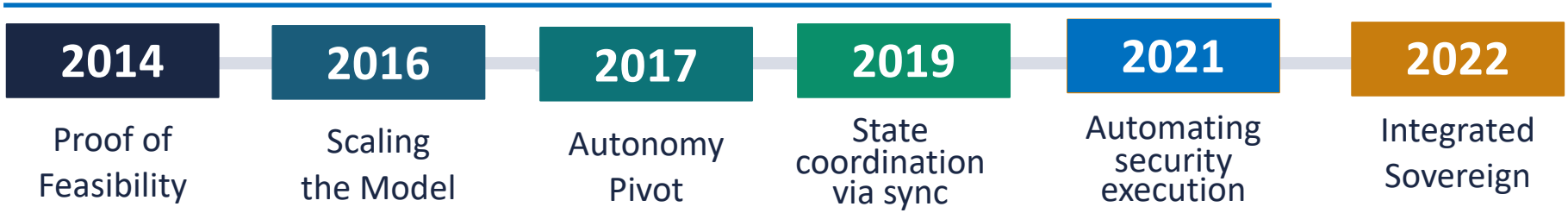


(a) Cloud-based Smart Home
Control enforced in the cloud

- NDN Model: Data-Centric Autonomy
  - Data stays local and is explicitly pulled by name.
  - The user controls the identity and the local trust anchor.
  - Security on data, utilizing name-bound signing.
  - Devices act as first-class named participants in the network.

(b) **Sovereign**
Control enforced on devices

From Experiments to Architectural Principles: Three Pillars of Sovereign Design



Experimentation revealed recurring architectural patterns: namespace ownership, localized trust, and decentralized coordination.

- Pillar 1: Namespace Design
  - Transition: From administrative naming to user-owned identity.
- Pillar 2: Security Plane
  - Transition: From transit channel signing to user-managed trust anchors.
- Pillar 3: State Coordination Plane
  - Transition: From point-to-point request-response to distributed Sync.

A decade of experiments revealed that digital sovereignty and autonomy emerge naturally when network semantics align with user ownership and local trust.

Pillar 1: Namespace is Identity

- User-Owned Identity Foundations
  - Names are structured hierarchically and carry semantic meaning (e.g., `/home/alice/thermostat`).
  - Names are designed to outlast the device hardware lifetime
- Decoupling from External Registries
  - Namespace ownership equates directly to identity ownership.
  - The local system requires zero external registries or cloud lookup to operate.
- Core Principle: Name ownership is the prerequisite for digital sovereignty.

Pillar 2: Localized Security Plane

- Data-Centric Provenance
  - Every single data packet is cryptographically signed by its producing device.
  - Consumers verify the authenticity and integrity of all received data end-to-end
- In-Band Key Distribution
  - Encryption keys are treated as standard data objects, named and distributed over the network.
  - Eliminates the need for complex out-of-band security management channels.
- The User as the Root of Trust
  - The device owner generates and securely holds the root cryptographic key locally.
  - Certificates exist as local data objects rooted entirely within the user's namespace.

Pillar 3: State Coordination Plane

- Broker-less Local Coordination
  - Utilizes State Vector Sync (SVS) to maintain state consistency across devices.
  - Devices pull missing data objects by name.
- Eliminating Centralized Intermediaries
  - Removes the need for centralized brokers, local relays, or cloud message queues.
  - Devices achieve consistency naturally through decentralized data dissemination.
  - Resilience: elimination of the global impact from a single cloud failure

Future Horizons: Integration with Agentic AI

- The Illusion of Cloud-Driven Intelligence
  - Current AI architectures assume continuous, high-bandwidth WAN access to remote data centers.
- The Demand for Local Reflexes
  - Physical systems (valves, grids, autonomous nodes) require localized decision loops.
- The Autonomy Bottleneck: Off-Grid Survival
  - In a network partition, a cloud-tethered agent is instantly paralyzed.
  - The Sovereign Requirement: The agent must maintain full operational authority and decision-making capabilities completely isolated from the internet.

Conclusion & Systemic Implications

- The Scientific Verdict
  - A decade of research demonstrated that cloud-independent IoT is viable, buildable, and resilient.
- Sovereignty as an Architectural Property
  - Systemic autonomy cannot be effectively achieved through high-level policy mandates or compliance check-boxes.
  - Sovereignty should be a structural property deliberately designed into the networking substrate.
- Securing Critical Infrastructure
  - NDN-based sovereign design offers a concrete path to isolate and secure national nervous systems (grids, healthcare, emergency services)
- The New Frontier: Systemic Adoption
  - The primary challenge has shifted from technical feasibility to overcoming legacy market inertia and industry adoption.