# SecureIoT-Core: A Programmable Data Plane Framework for Protecting Critical Infrastructures

# Introduction

The rapid expansion of **IoT deployments** in **finance, telecommunications, and the power grid** has created new opportunities for automation, monitoring, and digital service delivery. At the same time, it has introduced severe **cybersecurity risks**. Devices such as **smart meters, POS terminals, and CCTVs** are often deployed at massive scale, run on resource-constrained hardware, and lack robust built-in defenses. Once compromised, they can be weaponized to:

- Form **botnets** that launch DDoS attacks against financial services and citizen platforms.
- Conduct **data exfiltration** or **false data injection** into energy control systems.
- Serve as **stealthy entry points** for deeper penetration into critical infrastructures.

These threats are especially acute in the Indian context, where **digital payments, e-governance services, and the energy grid** underpin daily operations and national resilience.

---

## Why Existing Approaches Fall Short

Traditional defenses such as firewalls, ACLs, and intrusion detection systems are ill-suited to this environment:

- **Too late in the path**: centralized cloud/firewall solutions detect anomalies only after malicious traffic has already entered the network.
- **Not scalable**: ACLs and flow rules in TCAM consume large memory and power, and cannot handle tens of thousands of IoT devices at line rate.

- **Weak at device-level identity**: they authenticate flows, not devices, making it easy for adversaries to spoof or compromise authorized devices.
- **Reactive rather than proactive**: anomaly detection often occurs after service disruption.

---

## Why Programmable Data Planes Help — and Their Limitations

**P4-enabled programmable switches** offer a path forward by allowing custom packet parsing, stateful counters, and match-action rules inside the data plane. They can, in principle, enforce **per-device admission policies** and perform **in-network anomaly detection at line rate**.

However, if used *as is*, programmable data planes face important challenges:

- **Memory constraints**: per-device ACLs stored in TCAM do not scale to 10k–100k IoT devices.
- **State limitations**: switches cannot hold detailed per-device profiles without exhausting SRAM/register space.
- **Crypto limitations**: P4 cannot generate strong cryptographic tokens, leaving identity proofs weak.
- **Policy churn**: frequent device joins/leaves make maintaining flow rules unstable at scale.

---

## Proposed Two-Phase Mechanism

To address these challenges, we propose a **two-layered security framework** based on lightweight, cryptographically assured trust enforcement:

1. **Phase 1: Device Admission (DAT at ingress)**

    - At bootstrap, the **controller generates a cryptographic token** bound to `{device_id, service_profile}`.
    - The ingress P4 switch maintains a **Device Admission Table (DAT)** mapping device IDs to tokens and profiles.
    - On valid admission, the ingress switch attaches the token to the packet and enforces service-profile checks with anomaly detection counters.
    - Unauthorized or unregistered devices are dropped immediately.
2. **Phase 2: Token Validation (TVT in core/egress)**
    - Downstream switches maintain only a **Token Validation Table (TVT)** for fast exact-match checks on tokens.
    - If a token is missing, invalid, or revoked, packets are dropped/quarantined.
    - At the network egress, the token is stripped before the packet leaves the domain, preserving transparency and interoperability.

---

# Objectives

This project aims to design, prototype, and evaluate an indigenous security framework for IoT-driven critical infrastructures with the following objectives:

1. **Develop P4-based Device Admission (DAT) and Token Validation (TVT) mechanisms** to enforce device-level trust at line rate.
2. **Integrate controller-driven cryptographic token generation, distribution, and revocation** for scalable and secure identity management.
3. **Implement lightweight anomaly detection in the data plane** using per-device registers and profile-based thresholds.
4. **Demonstrate scalability and efficiency** by comparing SRAM-based token validation against TCAM-based flow rules, highlighting memory and speed benefits.

5. **Validate the framework in finance and energy IoT testbeds**, targeting TRL 5–6, to show its applicability to India's critical infrastructure needs.

---

# Expected Benefit

By combining **programmable data planes** with **controller-orchestrated cryptographic tokens**, our approach offers:

- **Scalable trust enforcement**: one device → one profile → one token; validated via compact SRAM tables.
- **Line-rate anomaly detection**: real-time counters and profile validation at ingress.
- **Defense-in-depth**: unauthorized devices blocked at admission; compromised insiders contained mid-operation.
- **Practical deployment**: no changes to existing IoT devices; tokens are injected in-network and stripped at egress.
- **Indigenous innovation**: leverages P4 programmability for India-specific finance and energy infrastructure security.