I Didn’t Peek:
And I Can Prove it

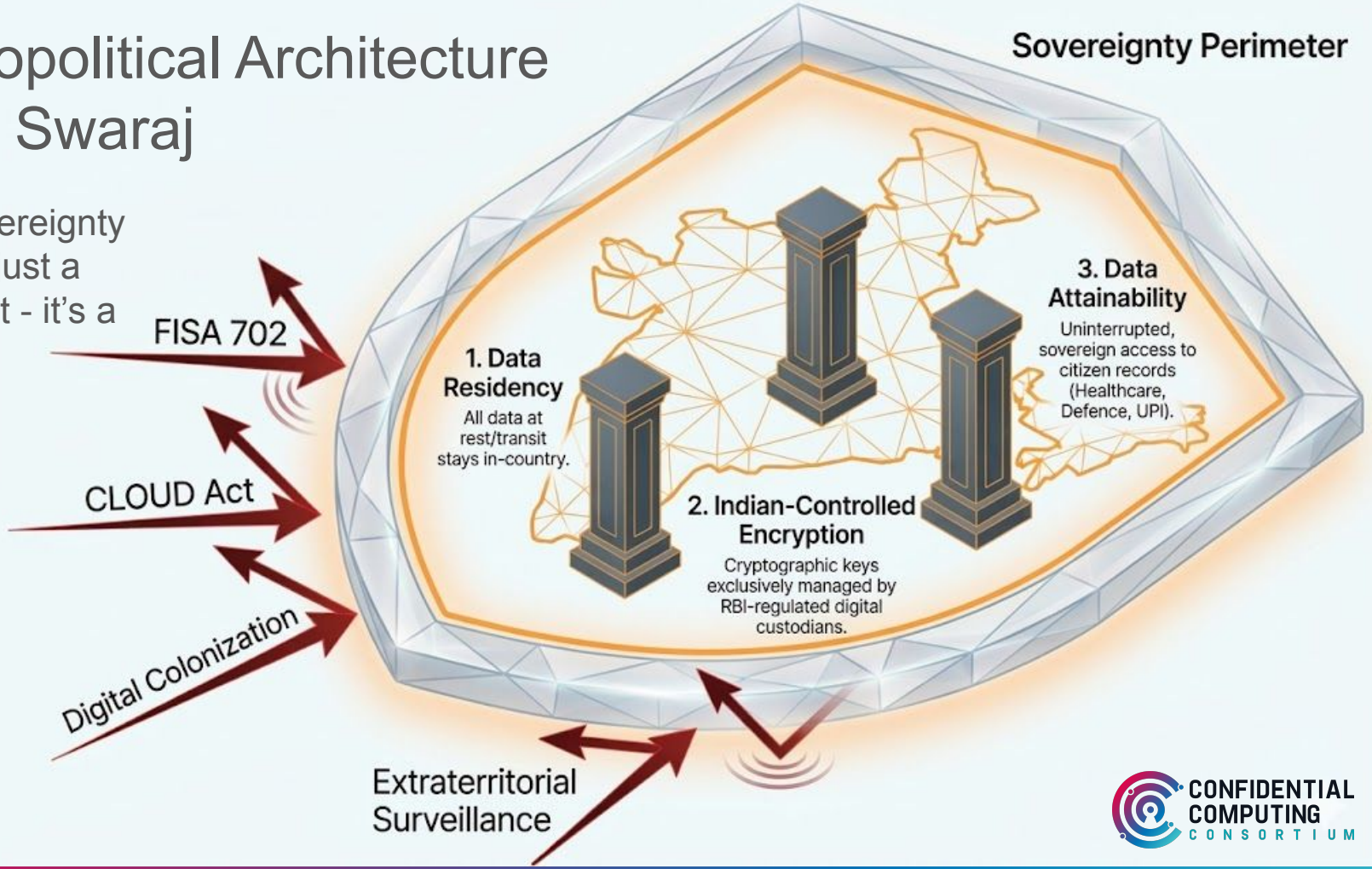
Confidential Computing for Audits and Regulators

Mike Bursell, Executive Director, CCC
Open Source Summit India 2026

CONFIDENTIAL COMPUTING CONSORTIUM

The Geopolitical Architecture Of Data Swaraj

National sovereignty is no longer just a legal concept - it's a perimeter

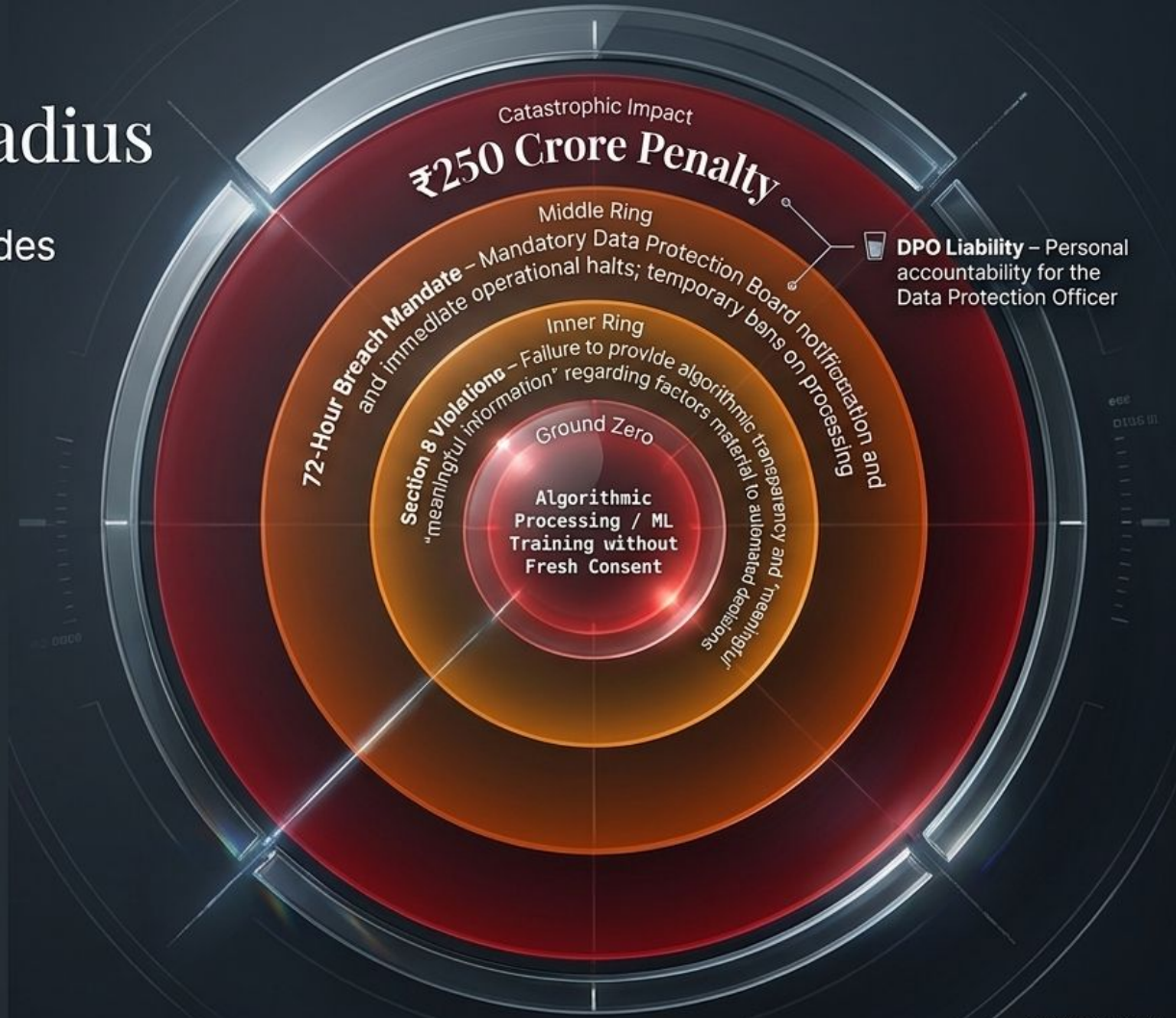


CONFIDENTIAL COMPUTING CONSORTIUM

The DPDPA Blast Radius

A single algorithmic misstep cascades into systemic business failure.

> Using personal data for AI training without separate, explicit consent is a direct violation, even if originally collected legally.



What does this mean?

Regulatory Regimes: Risk Tiers vs Data Protection

Regulatory Dimension	EU AI Act (2024)	India DPDPA (2023/2026)	The Engineering Implication
Core Philosophy			
Transparency			
Consent Model			
Human Oversight			

Regulatory Regimes: Risk Tiers vs Data Protection

Regulatory Dimension	EU AI Act (2024)	India DPDPA (2023/2026)	The Engineering Implication
Core Philosophy	Prescriptive risk classification (Prohibited, High-Risk, Minimal).		
Transparency	System docs & broad user notification.		
Consent Model	Broad processing frameworks.		
Human Oversight	Required for High-risk AI.		

Regulatory Regimes: Risk Tiers vs Data Protection

Regulatory Dimension	EU AI Act (2024)	India DPDPA (2023/2026)	The Engineering Implication
Core Philosophy	Prescriptive risk classification (Prohibited, High-Risk, Minimal).	Data-protection focused. No AI is inherently prohibited, but all data is guarded.	
Transparency	System docs & broad user notification.	Mandates clear explanation of “decision logic” (Section 8).	
Consent Model	Broad processing frameworks.	Requires fresh, distinct consent for algorithmic processing.	
Human Oversight	Required for High-risk AI.	Required for automated decisions with “significant effects”.	

Regulatory Regimes: Risk Tiers vs Data Protection

Regulatory Dimension	EU AI Act (2024)	India DPDPA (2023/2026)	The Engineering Implication
Core Philosophy	Prescriptive risk classification (Prohibited, High-Risk, Minimal).	Data-protection focused. No AI is inherently prohibited, but all data is guarded.	Engineers must track data lineage rather than just classifying the model.
Transparency	System docs & broad user notification.	Mandates clear explanation of “decision logic” (Section 8).	AI models cannot be black boxes; factors must be explainable.
Consent Model	Broad processing frameworks.	Requires fresh, distinct consent for algorithmic processing.	“Opt-in” architectures must be built into ML data pipeline
Human Oversight	Required for High-risk AI.	Required for automated decisions with “significant effects”.	Systems require “circuit breaker” for manual review.

The business impact

CONFIDENTIAL COMPUTING CONSORTIUM

The CISO’s Dilemma: Proof over Promise

The Illusion

Security

The Reality

CONFIDENTIAL COMPUTING CONSORTIUM

The CISO's Dilemma: Proof over Promise

The Illusion

~~Security~~

CISOs care about the Board and the Auditors

The Board and Auditors care about RISK

The Reality

CONFIDENTIAL COMPUTING CONSORTIUM

The CISO's Dilemma: Proof over Promise

The Illusion

~~Security~~

CISOs care about the Board and the Auditors

The Board and Auditors care about RISK

The Reality

Compliance = Policy + Audit

CONFIDENTIAL COMPUTING CONSORTIUM

The CISO's Dilemma: Proof over Promise

Auditors do not evaluate intentions. They evaluate evidence.

The Illusion

~~Security~~

CISOs care about the Board and the Auditors

The Board and Auditors care about RISK

The Reality

Compliance = Policy + Audit

CONFIDENTIAL COMPUTING CONSORTIUM

The CISO's Dilemma: Proof over Promise

Auditors do not evaluate intentions. They evaluate evidence.

The Illusion

~~Security~~

CISOs care about the Board and the Auditors

The Board and Auditors care about RISK

The Reality

Compliance = Policy + Audit

Traditional security policies are *promises*. We need technical solutions to **prove** risk mitigation to regulators.

CONFIDENTIAL COMPUTING CONSORTIUM

Introducing Confidential Computing

The Vulnerability Gap in the Cloud Estate

Data at Rest

Encrypted on storage media. Safe from physical theft.

Data in Transit

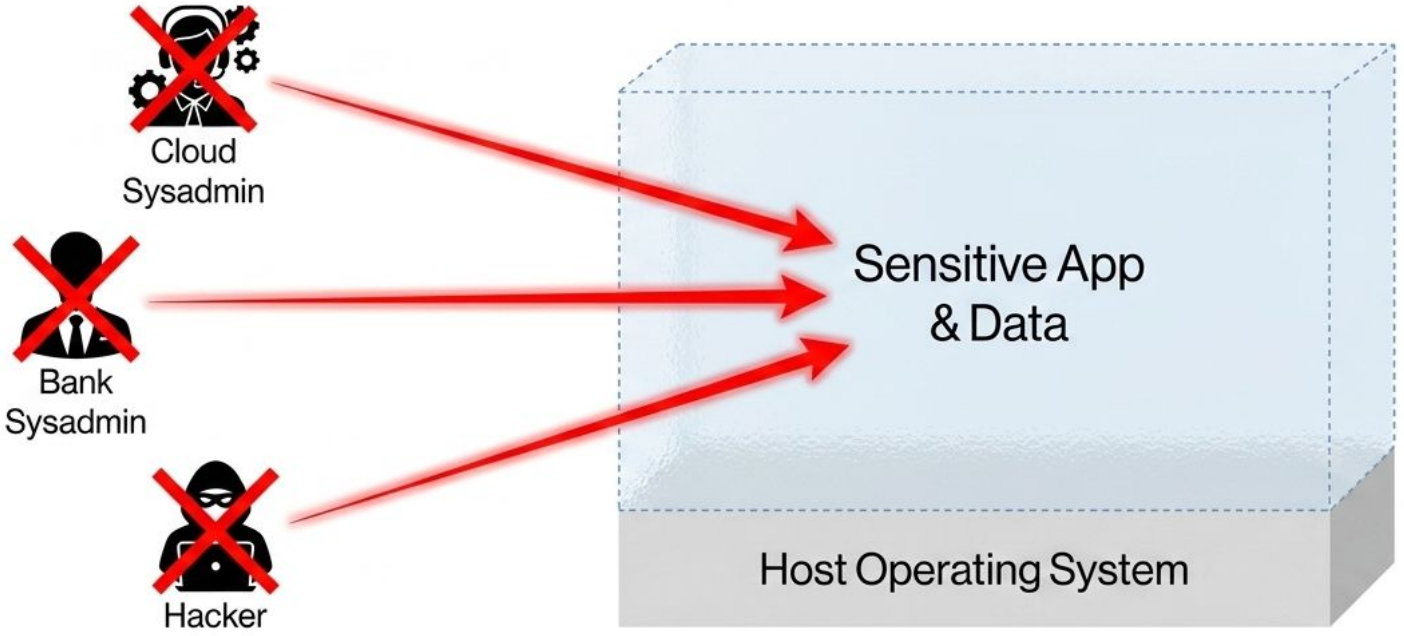
Encrypted moving across the network. Safe from packet sniffing.

Data in Use

Exposed in cleartext in memory during processing.

When your AI model trains on citizen data, or when the algorithm makes a credit decision, the data is entirely exposed in memory.

The Blind Spot: Who Can Look Inside?

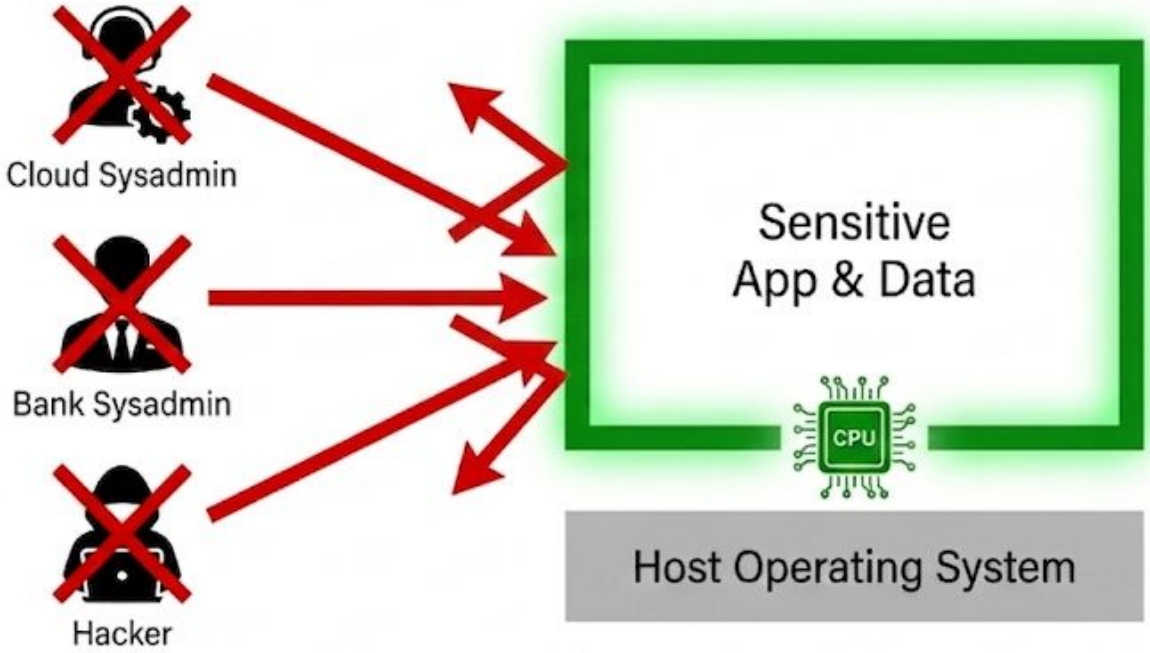


In a traditional cloud environment, anyone with elevated infrastructure privileges can bypass your security policies and peek at the data.

CONFIDENTIAL COMPUTING CONSORTIUM

Confidential Computing

Isolation via hardware-based controls

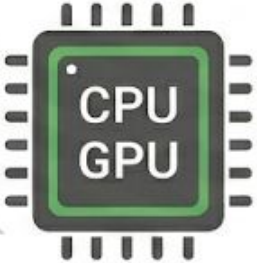


- 1. Isolation: Hardware-enforced separation from the host.
- 2. Confidentiality: Memory encryption; data is invisible even to the hypervisor.
- 3. Integrity: Code and data are protected from tampering.

CONFIDENTIAL COMPUTING CONSORTIUM

Remote Attestation: Cryptographic Proof of Policy

Step 1: Measure.
Measure our CPU/GPU.



Step 2: Sign.
To sign.

Step 3: Verify.
Attest to service.

Auditor Takeaway: "We no longer say 'Trust our application.' We hand the regulator a cryptographic receipt."

CONFIDENTIAL COMPUTING CONSORTIUM

The Security Paradigm Shift

Feature	Traditional Cloud Security	Confidential Computing
Core Mechanism	Software policies and Identity Access Management (IAM)	
Data Protection	Encrypted at rest & in transit	
Root of Trust	The Cloud Provider & Host OS	
Compliance Proof	“Read our internal SOC2 doc”	
Regulator View	Opaque black box; relies on promises	

CONFIDENTIAL COMPUTING CONSORTIUM

The Security Paradigm Shift

Feature	Traditional Cloud Security	Confidential Computing
Core Mechanism	Software policies and Identity Access Management (IAM)	Silicon-level hardware isolation (TEEs)
Data Protection	Encrypted at rest & in transit	
Root of Trust	The Cloud Provider & Host OS	
Compliance Proof	“Read our internal SOC2 doc”	
Regulator View	Opaque black box; relies on promises	

CONFIDENTIAL COMPUTING CONSORTIUM

The Security Paradigm Shift

Feature	Traditional Cloud Security	Confidential Computing
Core Mechanism	Software policies and Identity Access Management (IAM)	Silicon-level hardware isolation (TEEs)
Data Protection	Encrypted at rest & in transit	**Encrypted in use**
Root of Trust	The Cloud Provider & Host OS	
Compliance Proof	“Read our internal SOC2 doc”	
Regulator View	Opaque black box; relies on promises	

CONFIDENTIAL COMPUTING CONSORTIUM

The Security Paradigm Shift

Feature	Traditional Cloud Security	Confidential Computing
Core Mechanism	Software policies and Identity Access Management (IAM)	Silicon-level hardware isolation (TEEs)
Data Protection	Encrypted at rest & in transit	**Encrypted in use**
Root of Trust	The Cloud Provider & Host OS	Physical chip hardware (CPUs, GPUs, xPUs)
Compliance Proof	“Read our internal SOC2 doc”	
Regulator View	Opaque black box; relies on promises	

CONFIDENTIAL COMPUTING CONSORTIUM

The Security Paradigm Shift

Feature	Traditional Cloud Security	Confidential Computing
Core Mechanism	Software policies and Identity Access Management (IAM)	Silicon-level hardware isolation (TEEs)
Data Protection	Encrypted at rest & in transit	**Encrypted in use**
Root of Trust	The Cloud Provider & Host OS	Physical chip hardware (CPUs, GPUs, xPUs)
Compliance Proof	“Read our internal SOC2 doc”	“Verify this real-time attestation signature”
Regulator View	Opaque black box; relies on promises	

CONFIDENTIAL COMPUTING CONSORTIUM

The Security Paradigm Shift

Feature	Traditional Cloud Security	Confidential Computing
Core Mechanism	Software policies and Identity Access Management (IAM)	Silicon-level hardware isolation (TEEs)
Data Protection	Encrypted at rest & in transit	**Encrypted in use**
Root of Trust	The Cloud Provider & Host OS	Physical chip hardware (CPUs, GPUs, xPUs)
Compliance Proof	“Read our internal SOC2 doc”	“Verify this real-time attestation signature”
Regulator View	Opaque black box; relies on promises	Transparent vault: relies on hardware & cryptography

CONFIDENTIAL COMPUTING CONSORTIUM

Home appliances ;-)

The vacuum cleaner dilemma

(Almost) nobody buys a vacuum cleaner because they **want** to!

Most security technologies are vacuum cleaner technologies.

We want enabling technologies instead

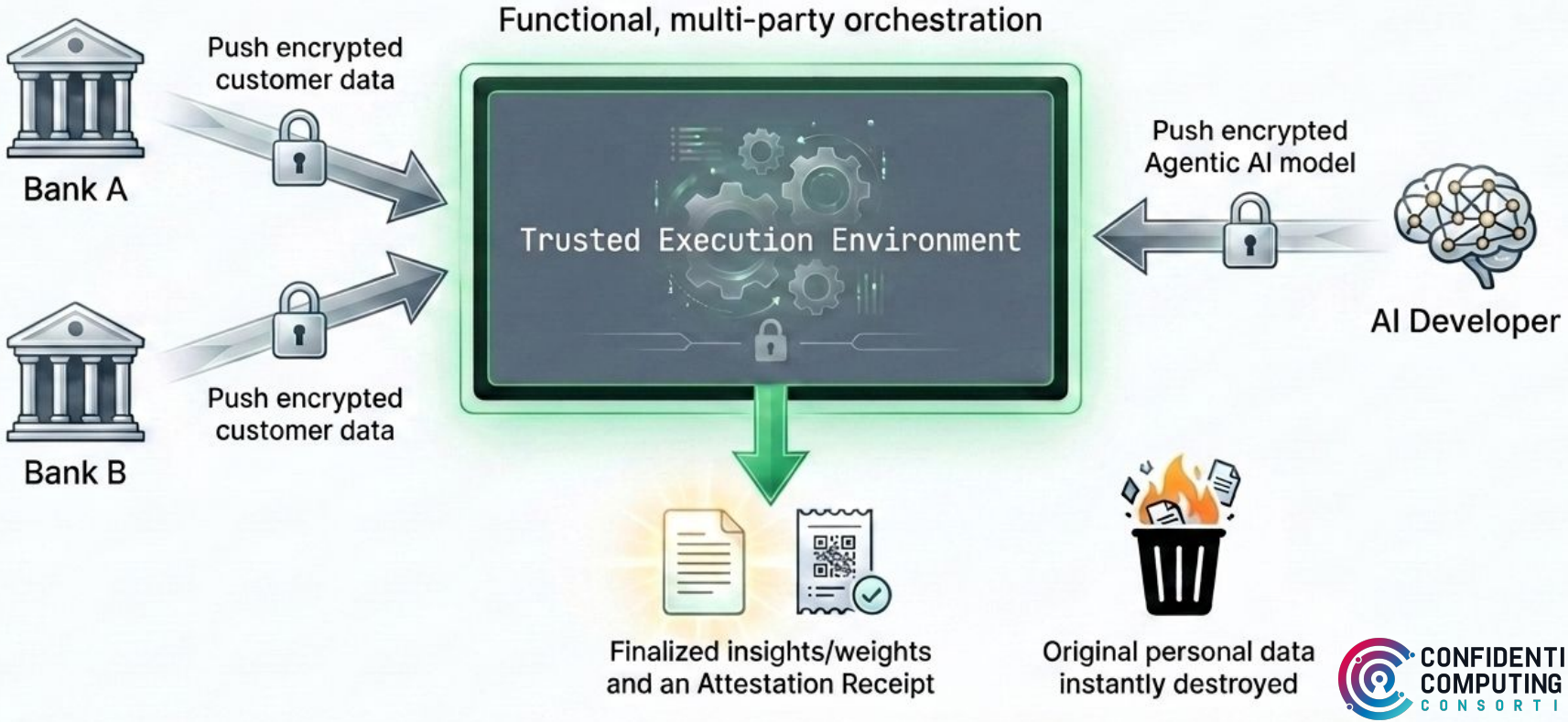
CONFIDENTIAL COMPUTING CONSORTIUM

Unlocking the Future of Digital Public Infrastructure

What can we build when trust is guaranteed?

Confidential Computing doesn't just prevent ₹250 Crore fines. It acts as the foundational enabling layer for next-generation, multi-party computing.

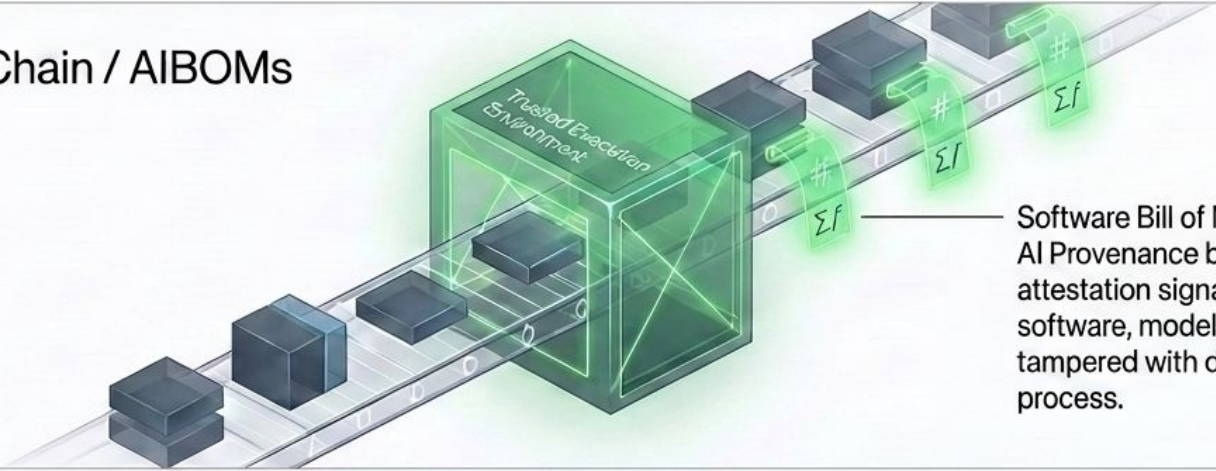
The Confidential AI Clean Room



DPDPA Compliance Check: *"Zero data leakage. Cryptographic proof of purpose limitation. Complete algorithmic IP protection."*

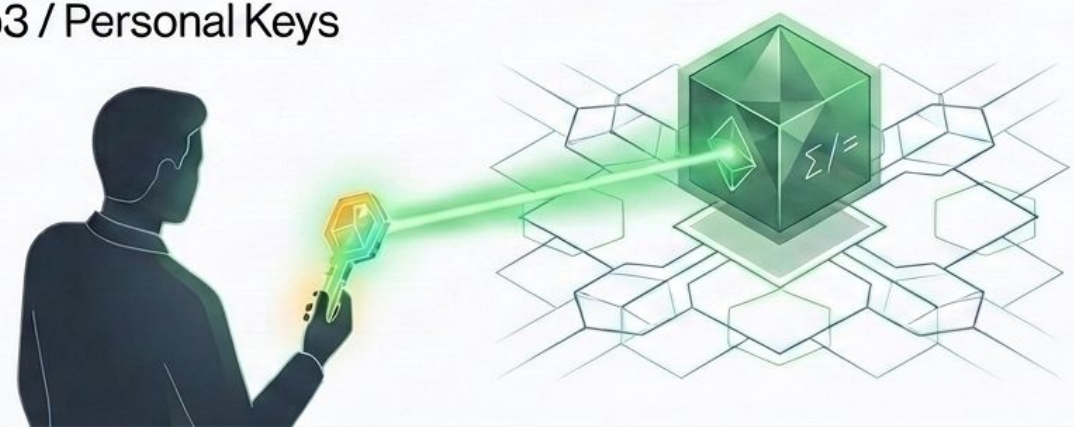
Verifiable Provenance: Supply Chains & Web3

Digital Supply Chain / AIBOMs



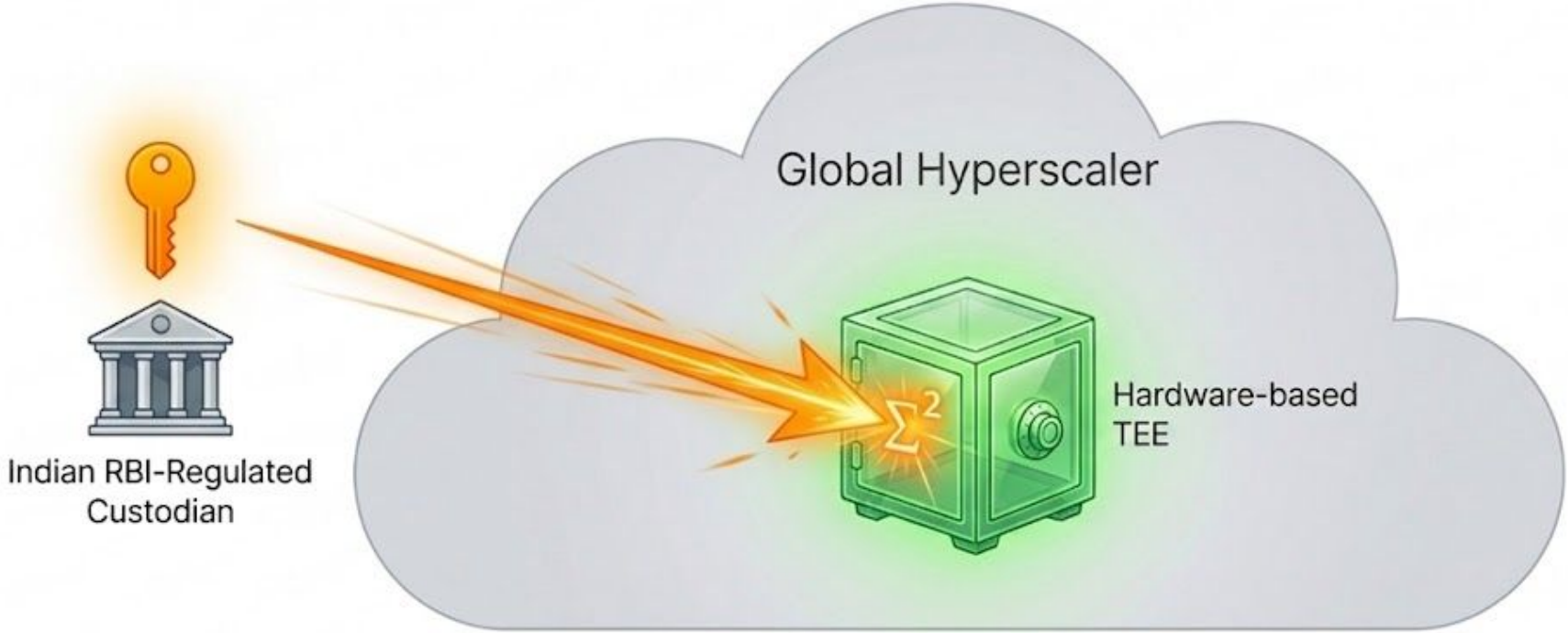
Software Bill of Materials (SBOM) or AI Provenance backed by an attestation signature, proving the software, models or weights weren't tampered with during the build process.

Web3 / Personal Keys



Secure personal key management. Equipping citizens with sovereign keychains to sign/encrypt their own data, shielding them from insider threats and cloud provider overreach.

Solving the Data Swaraj Equation



We can leverage the compute power of global hyperscalers while maintaining absolute, hardware isolated sovereign control over the encryption keys and the data execution. Data Swaraj achieved.

Synthesis: The Trust Layer Ecosystem

The Confidential Computing Consortium

CONFIDENTIAL COMPUTING CONSORTIUM

The Confidential Computing Consortium

- Promoting Confidential Computing
- Home to open source projects
- Sponsoring academic research
- Linux Foundation project
- Safe place for technical discussions
- Thought leadership

Built on Open Standards: The CCC

Confidential Computing is not a vendor-locked walled garden. It is an open, cross-industry initiative defining standards, open-source tools, and vendor-neutral attestation architectures.

CONFIDENTIAL COMPUTING CONSORTIUM

Accountability Flows Upward. Cryptography Scales Infinitely.

> “Alan Turing asked if machines could think. Under the DPDPA, we must ask how machines are accountable. Humans bear the moral responsibility, but we now have the mathematics to prove our compliance.”

1. **Assume Breach:**
   Your data is exposed in memory.
2. **Demand Proof:**
   Move from policy checklists to Remote Attestation.
3. **Build the Future:**
   Deploy Confidential Computing to achieve Data Swaraj and unlock AI.

CONFIDENTIAL COMPUTING CONSORTIUM

Questions