NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution| Affiliated to JNTUH | Approved by AICTE
Accredited by NBA & NAAC with 'A' Grade

Department of Computer Science and Engineering

Program Name : B.Tech CSE

Subject: CLOUD COMPUTING

Course Code : 23CS706

Semester & Year: I/IV

Faculty Name : G. MAHESH

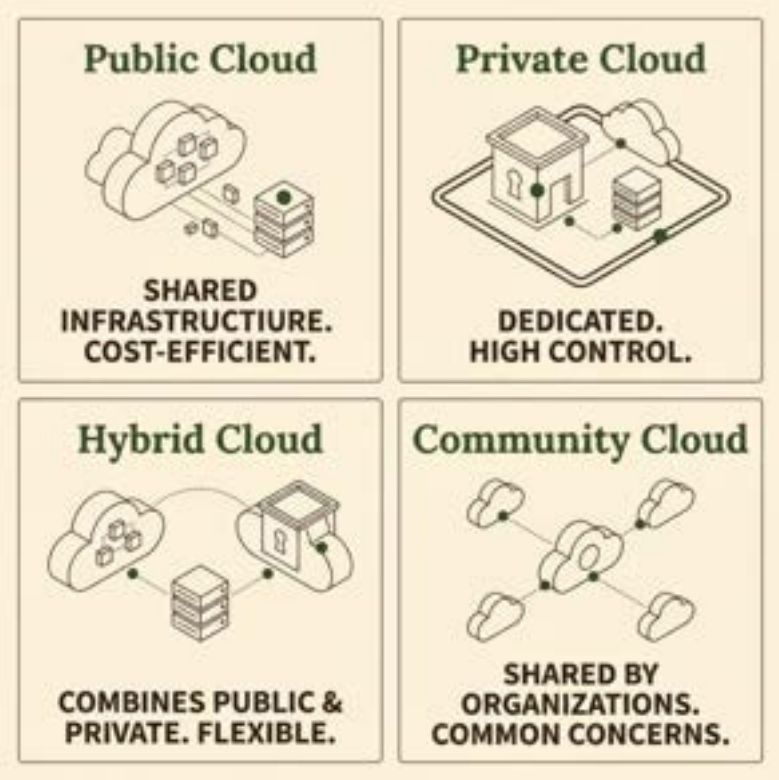
UNIT-V

Cloud Computing: Security Foundations and Advanced Frontiers

A comprehensive exploration of cloud security principles, threat landscapes, and cutting-edge cryptographic techniques — designed for B.Tech students stepping into the cloud-first era.

B.TECH CLOUD SECURITY COURSE

The Cloud Paradigm: Core Concepts



What is Cloud Computing?

NIST defines it as **on-demand access to shared pools of configurable resources** — networks, servers, storage, and applications — over the internet.

Service Models

- **IaaS** — Infrastructure as a Service (raw compute, storage)
- **PaaS** — Platform as a Service (dev tools, runtime environments)
- **SaaS** — Software as a Service (ready-to-use applications)

Virtualization: The Engine of the Cloud

Hypervisors

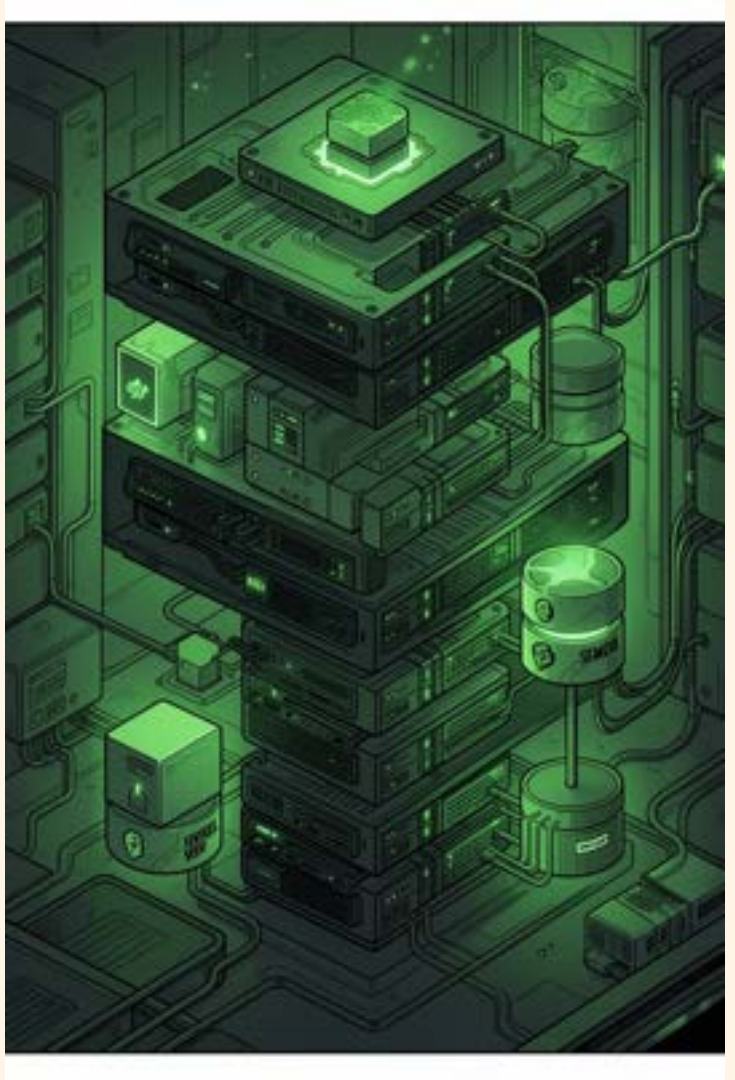
Type 1 (bare-metal) and Type 2 (hosted) hypervisors abstract physical hardware. Xen is a landmark open-source Type 1 hypervisor enabling multi-tenant isolation.

Containerization

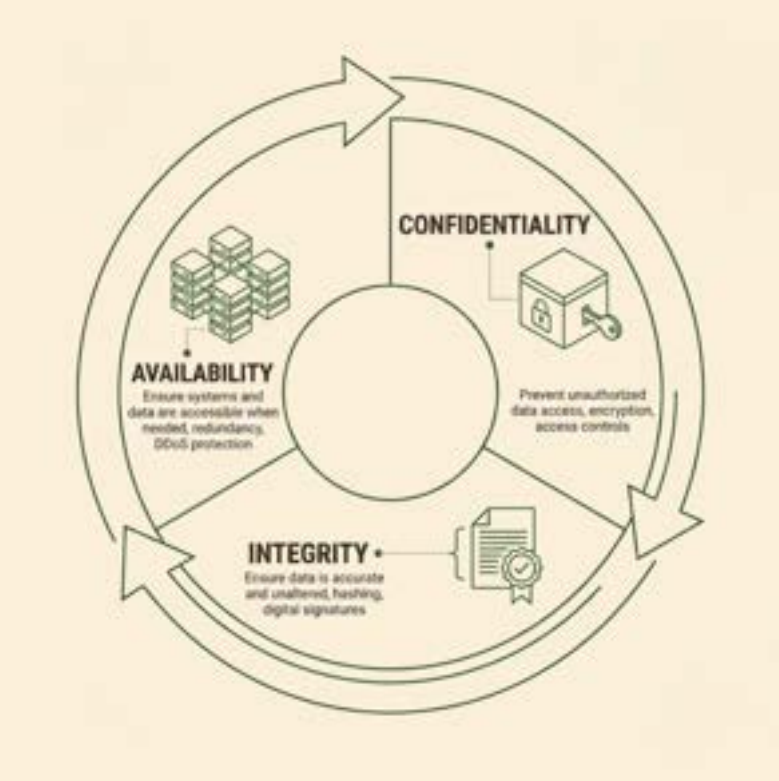
Docker packages applications with dependencies into lightweight containers. Microservices architecture leverages containers for scalable, independent deployment.

Hardware Abstraction

CPU, memory, and I/O devices are virtualized to enable resource pooling, live migration, and elastic scaling across cloud infrastructure.



The Security Landscape: CIA Triad and Threats



Top Cloud Threats

- **Malicious Insiders** — Privileged users abusing access
- **Account Hijacking** — Credential theft via phishing or brute force
- **Insecure APIs** — Weak interfaces exposing backend systems
- **Data Leakage** — Unintended exposure through misconfiguration

⚠ **Unique Challenge:** Multi-tenant architectures introduce shared technology vulnerabilities where one tenant's compromise can affect others.

Securing the Cloud Environment

Identity & Access Management

Multi-factor authentication (MFA) and Role-Based Access Control (RBAC) ensure only authorized users reach sensitive resources.

Technical Controls

CASB monitors cloud app usage. **DLP** prevents sensitive data exfiltration. **IRM** enforces persistent protection on files.

Compliance Frameworks

CSA, NIST SP 800-53, ISO/IEC 27001, and ENISA provide structured guidelines for governance, risk management, and audit readiness.

The Malicious Insider Problem

The Black Box Challenge

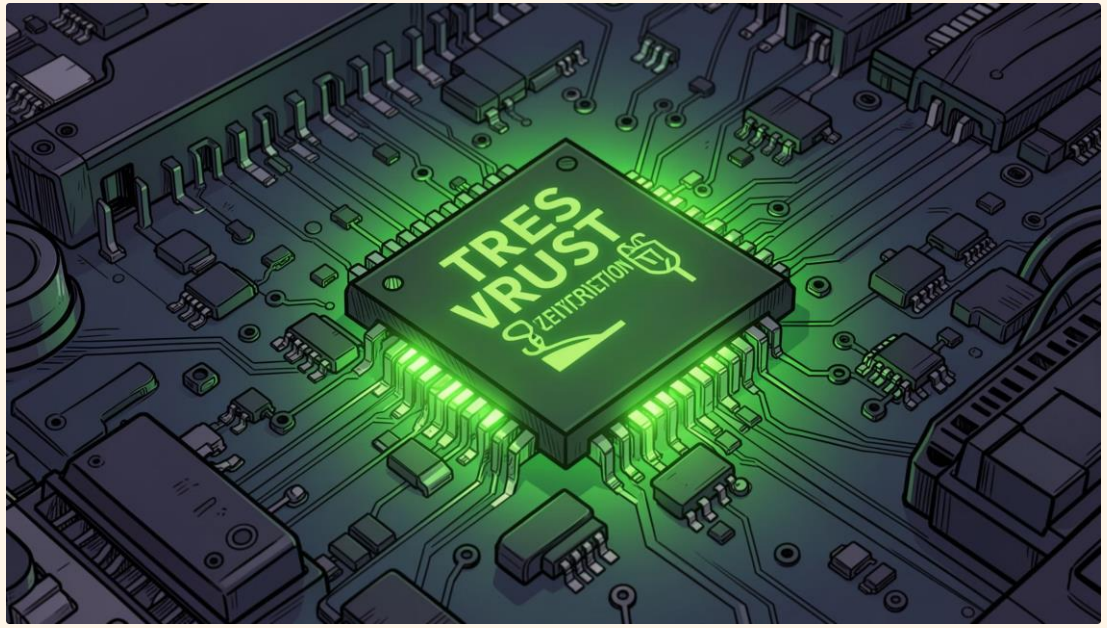
Even reputable cloud providers cannot eliminate risk from rogue system administrators with privileged access to customer data.

Trusted Platform Module (TPM)

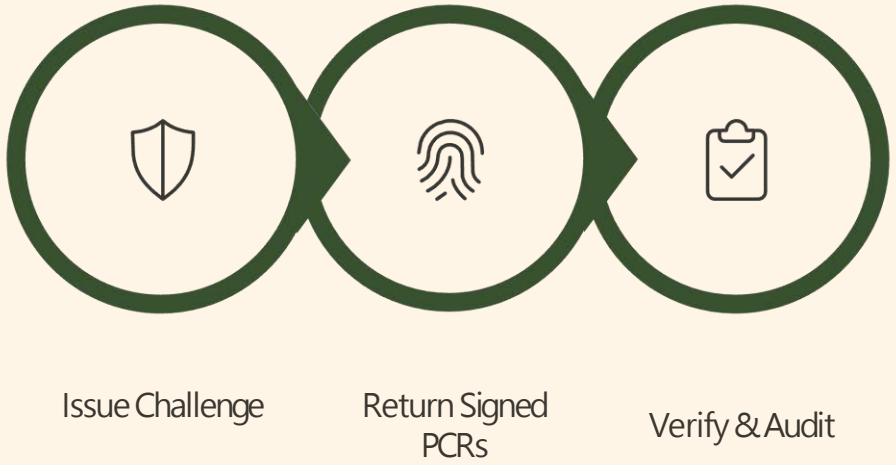
A hardware chip that **bootstraps trust** using Endorsement Keys (unique device identity) and PCR hashes (measured boot integrity).

TCCP Architecture

The Trusted Cloud Computing Platform ensures each node runs only **verified, attested software** before processing any tenant workload.



Auditing and Attestation



Traditional audits fail in the cloud because providers restrict physical access. **Third-party attestation** solves this by cryptographically proving system integrity without exposing infrastructure.

Virtual Machine Introspection (VMI)

Tools like **CloudHedge** and **NvCloudIDS** monitor VM behavior from outside the guest OS, enabling signature-based intrusion detection without agent installation.

Advanced Cryptography: Privacy-Preserving Computation

Fully Homomorphic Encryption (FHE)

Allows **computation directly on encrypted data** — results decrypt to the correct answer without ever exposing plaintext to the cloud provider.

Functional Encryption

Reveals only a **specific function of the plaintext** (e.g., "is age > 18?") without exposing the underlying dataset.

Learning With Errors (LWE)

A lattice-based hardness assumption enabling **efficient, quantum-resistant** cryptographic schemes tailored for cloud workloads.

Future Trends and Emerging Challenges

Secure Provisioning

Protecting VM migrations and automated deployments from interception or tampering during live scaling events.

Serverless Security

Event-driven architectures (AWS Lambda, Azure Functions) expand the threat model — ephemeral functions require new monitoring paradigms.

Quantum-Resistant Cryptography

Post-quantum algorithms (CRYSTALS-Kyber, CRYSTALS-Dilithium) must replace RSA/ECC before large-scale quantum computers break current encryption.

Conclusion: Architecting the Future

Shared Responsibility

Security is a **joint obligation** — providers secure infrastructure; subscribers secure their data, identities, and applications.

Layered Defense

Effective cloud security blends **policy governance, hardware-backed trust (TPM), and advanced mathematics (FHE, LWE)**.

Your Call to Action

Master these layers to **innovate securely** in the cloud-first era — the next generation of cloud architects starts here.

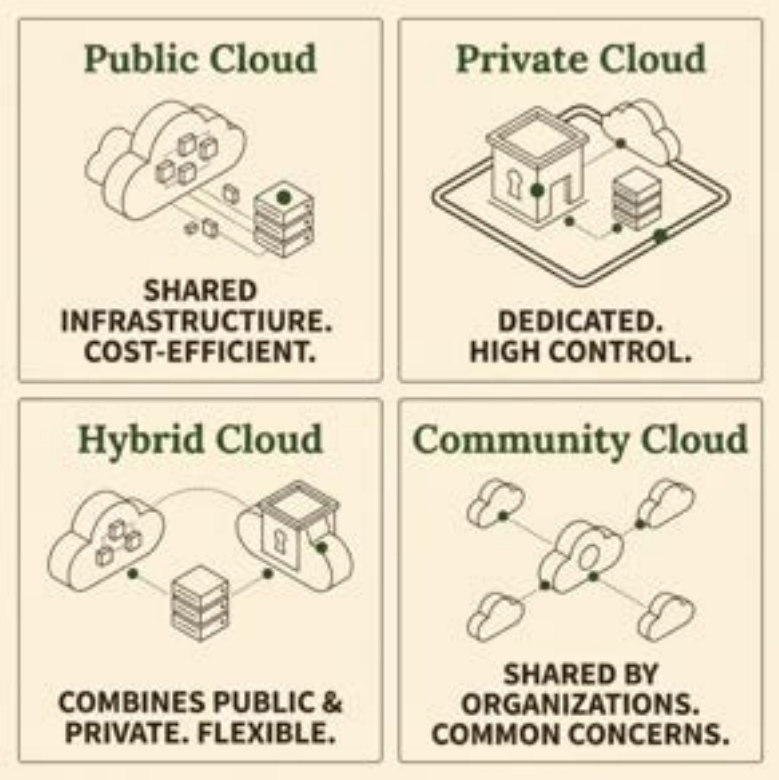
UNIT-V

Cloud Computing: Security Foundations and Advanced Frontiers

A comprehensive exploration of cloud security principles, threat landscapes, and cutting-edge cryptographic techniques — designed for B.Tech students stepping into the cloud-first era.

B.TECH CLOUD SECURITY COURSE

The Cloud Paradigm: Core Concepts



What is Cloud Computing?

NIST defines it as **on-demand access to shared pools of configurable resources** — networks, servers, storage, and applications — over the internet.

Service Models

- **IaaS** — Infrastructure as a Service (raw compute, storage)
- **PaaS** — Platform as a Service (dev tools, runtime environments)
- **SaaS** — Software as a Service (ready-to-use applications)

Virtualization: The Engine of the Cloud

Hypervisors

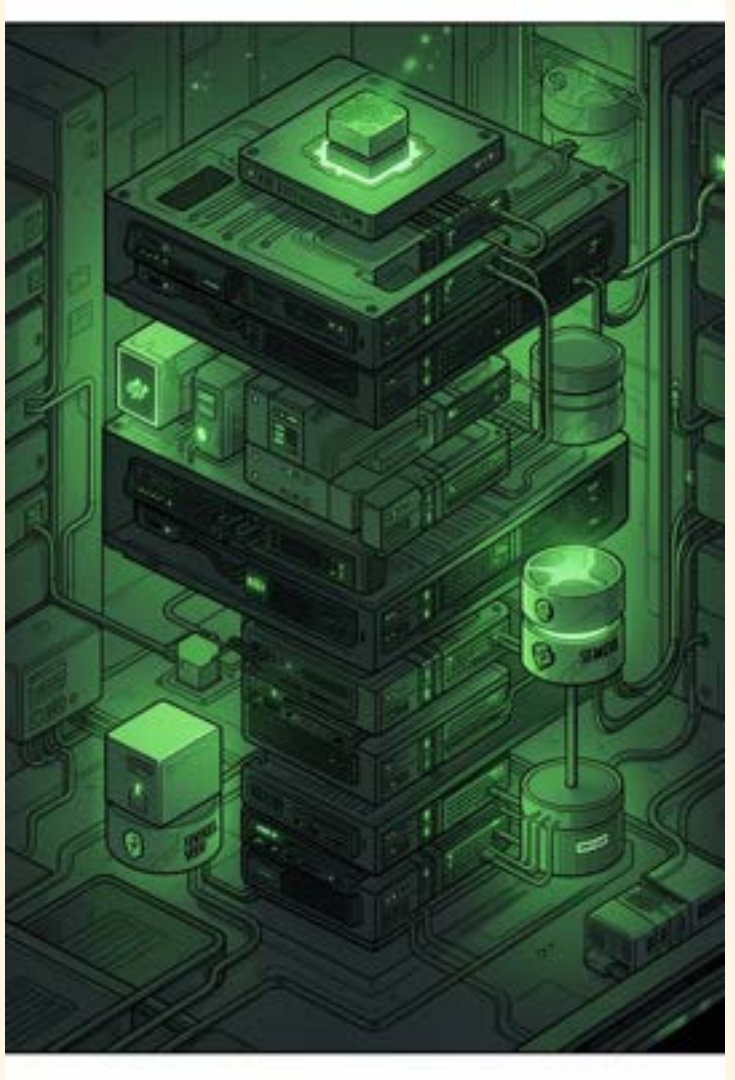
Type 1 (bare-metal) and Type 2 (hosted) hypervisors abstract physical hardware. Xen is a landmark open-source Type 1 hypervisor enabling multi-tenant isolation.

Containerization

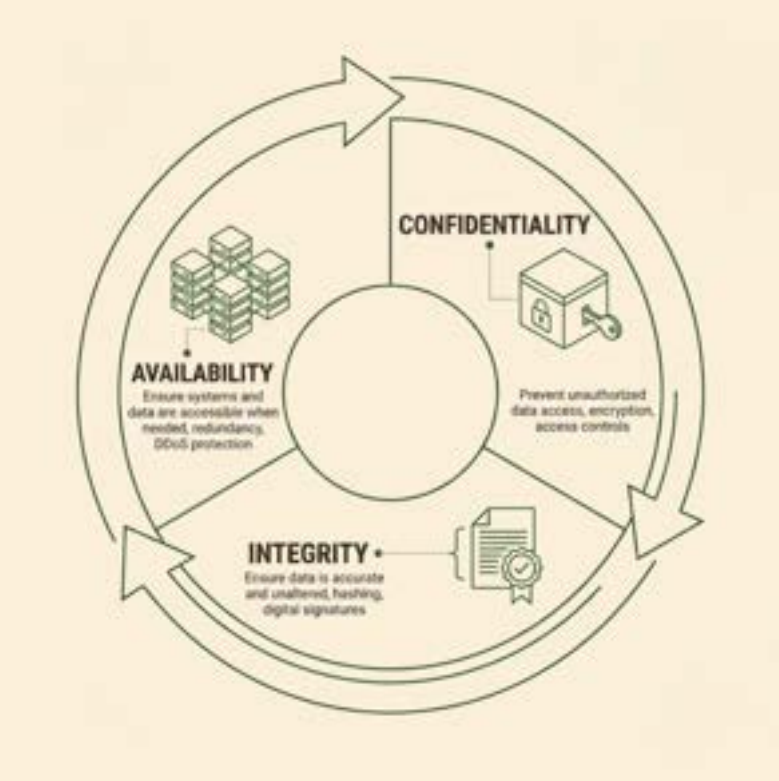
Docker packages applications with dependencies into lightweight containers. Microservices architecture leverages containers for scalable, independent deployment.

Hardware Abstraction

CPU, memory, and I/O devices are virtualized to enable resource pooling, live migration, and elastic scaling across cloud infrastructure.



The Security Landscape: CIA Triad and Threats



Top Cloud Threats

- **Malicious Insiders** — Privileged users abusing access
- **Account Hijacking** — Credential theft via phishing or brute force
- **Insecure APIs** — Weak interfaces exposing backend systems
- **Data Leakage** — Unintended exposure through misconfiguration

⚠ **Unique Challenge:** Multi-tenant architectures introduce shared technology vulnerabilities where one tenant's compromise can affect others.

Securing the Cloud Environment

Identity & Access Management

Multi-factor authentication (MFA) and Role-Based Access Control (RBAC) ensure only authorized users reach sensitive resources.

Technical Controls

CASB monitors cloud app usage. **DLP** prevents sensitive data exfiltration. **IRM** enforces persistent protection on files.

Compliance Frameworks

CSA, NIST SP 800-53, ISO/IEC 27001, and ENISA provide structured guidelines for governance, risk management, and audit readiness.

The Malicious Insider Problem

The Black Box Challenge

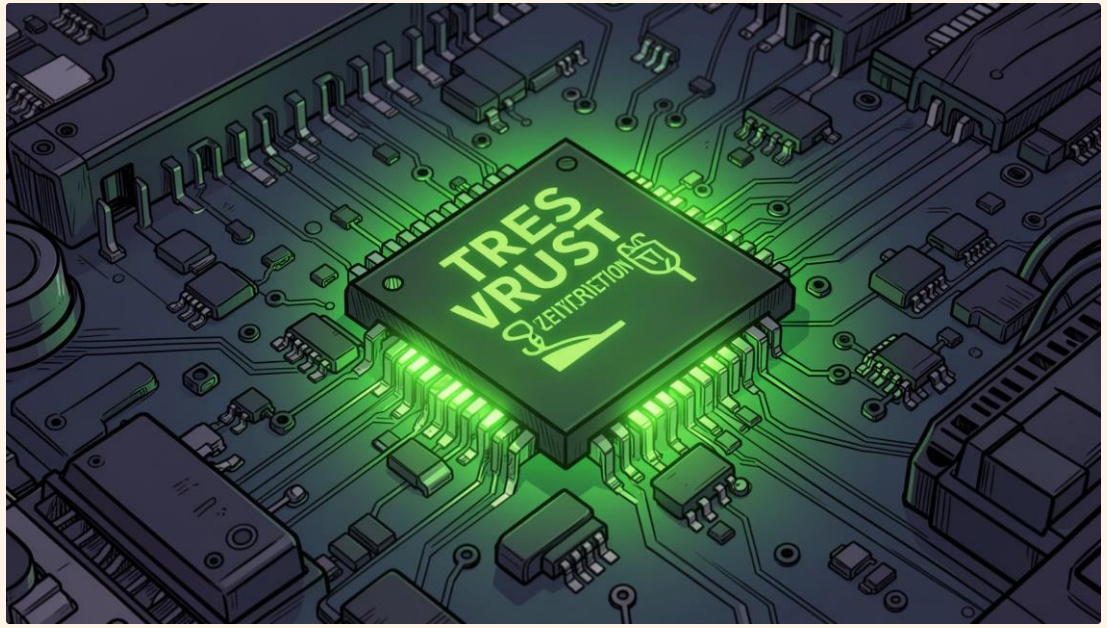
Even reputable cloud providers cannot eliminate risk from rogue system administrators with privileged access to customer data.

Trusted Platform Module (TPM)

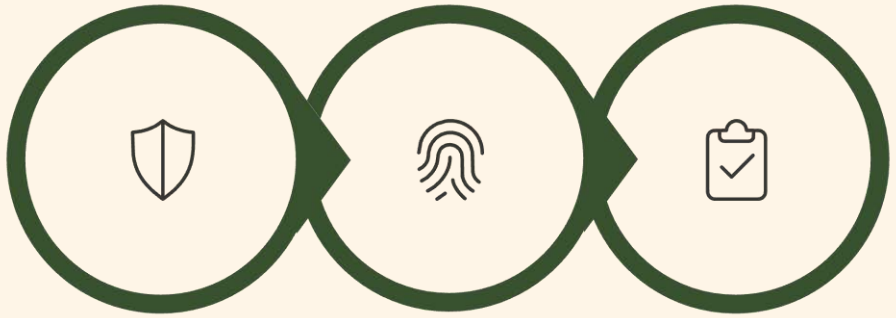
A hardware chip that **bootstraps trust** using Endorsement Keys (unique device identity) and PCR hashes (measured boot integrity).

TCCP Architecture

The Trusted Cloud Computing Platform ensures each node runs only **verified, attested software** before processing any tenant workload.



Auditing and Attestation



Issue Challenge

Return Signed PCRs

Verify & Audit

Traditional audits fail in the cloud because providers restrict physical access. **Third-party attestation** solves this by cryptographically proving system integrity without exposing infrastructure.

Virtual Machine Introspection (VMI)

Tools like **CloudHedge** and **NvCloudIDS** monitor VM behavior from outside the guest OS, enabling signature-based intrusion detection without agent installation.

Advanced Cryptography: Privacy-Preserving Computation

Fully Homomorphic Encryption (FHE)

Allows **computation directly on encrypted data** — results decrypt to the correct answer without ever exposing plaintext to the cloud provider.

Functional Encryption

Reveals only a **specific function of the plaintext** (e.g., "is age > 18?") without exposing the underlying dataset.

Learning With Errors (LWE)

A lattice-based hardness assumption enabling **efficient, quantum-resistant** cryptographic schemes tailored for cloud workloads.

Future Trends and Emerging Challenges

Secure Provisioning

Protecting VM migrations and automated deployments from interception or tampering during live scaling events.

Serverless Security

Event-driven architectures (AWS Lambda, Azure Functions) expand the threat model — ephemeral functions require new monitoring paradigms.

Quantum-Resistant Cryptography

Post-quantum algorithms (CRYSTALS-Kyber, CRYSTALS-Dilithium) must replace RSA/ECC before large-scale quantum computers break current encryption.

Conclusion: Architecting the Future

Shared Responsibility

Security is a **joint obligation** — providers secure infrastructure; subscribers secure their data, identities, and applications.

Layered Defense

Effective cloud security blends **policy governance, hardware-backed trust (TPM), and advanced mathematics (FHE, LWE)**.

Your Call to Action

Master these layers to **innovate securely** in the cloud-first era — the next generation of cloud architects starts here.