Scaling Trust: VM Security with Confidential Computing and Zero Trust Architecture

Priyadarshni Shanmugavadivelu • Stanford Business School

Conf42.com JavaScript 2025

The Cloud Security Imperative

94%

Enterprises on Cloud

Organizations have adopted cloud services for core operations

75%

Sensitive Data

Process confidential information in virtualized environments

Traditional VM security models are rapidly becoming obsolete as enterprises move critical workloads to the cloud.

The challenge: protecting data not just at rest and in transit, but **during active processing**.

Today's Journey

01

Confidential Computing

Hardware-based protection for data in use via Trusted Execution Environments

02

Trusted Launch

VM boot integrity verification through TPM-backed attestation

03

Zero Trust Architecture

Identity-aware micro-segmentation and continuous verification

04

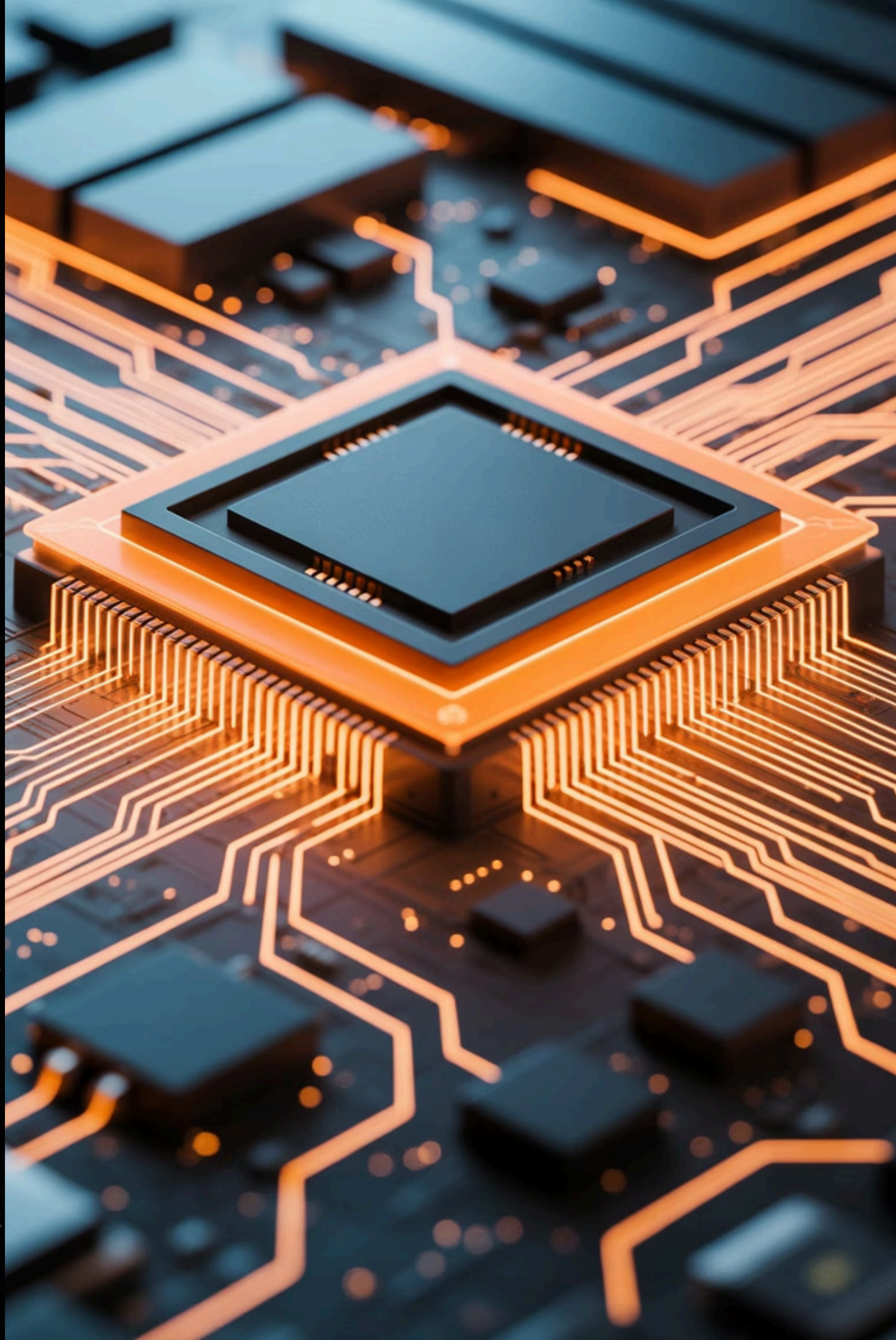
Practical Implementation

Design patterns, performance benchmarks, and compliance mappings

Confidential Computing: Protecting Data in Use

Confidential Computing leverages hardware-based Trusted Execution Environments (TEEs) to encrypt data while it's being processed—addressing the final frontier of data security.

Unlike traditional encryption that protects data at rest or in transit, TEEs create isolated, encrypted enclaves where computations occur, shielding workloads even from cloud providers and privileged administrators.



Leading TEE Technologies

AMD SEV-SNP

Secure Encrypted Virtualization with Secure Nested Paging provides VM-level memory encryption with integrity protection

- Encrypts VM memory with unique keys
- Prevents hypervisor-based attacks
- Attestation for boot integrity

Intel TDX

Trust Domain Extensions isolate VMs into protected trust domains with hardware-enforced boundaries

- CPU-level isolation mechanisms
- Remote attestation capabilities
- Minimal performance overhead

Confidential Computing Use Cases

Secure Multi-Party Analytics

Multiple organizations can jointly analyze sensitive datasets without exposing raw data to each other or the cloud provider. Financial institutions use this for collaborative fraud detection.

Confidential AI Training

Train machine learning models on sensitive data while keeping both the training data and the model weights encrypted. Healthcare providers leverage this for compliant medical AI development.

Protected Key Management

Store and process cryptographic keys in TEEs, ensuring they never exist in plaintext in memory. Critical for payment processing and certificate authorities.

Trusted Launch: Ensuring Boot Integrity

Trusted Launch verifies that VMs boot only with authorized, unmodified components using TPM-backed cryptographic attestation.

This creates a cryptographic chain of trust from hardware through firmware to the operating system, detecting any tampering or rootkit injection before workloads execute.

How Trusted Launch Works

Hardware Root of Trust

TPM 2.0 chip stores cryptographic measurements and generates attestation reports

Measured Boot

Each boot component is measured and recorded in TPM Platform Configuration Registers

Remote Attestation

Boot measurements are verified against known-good baselines before workload execution

Automated Enforcement

Integration with orchestration tools enables policy-driven trust verification at scale

DevOps Integration for Trusted Launch

Integrating Trusted Launch into CI/CD pipelines enables automated trust enforcement across the software delivery lifecycle.

- ### Policy as Code

  Define boot integrity requirements in infrastructure templates

- ### Automated Attestation

  Validate VM integrity before deploying application containers

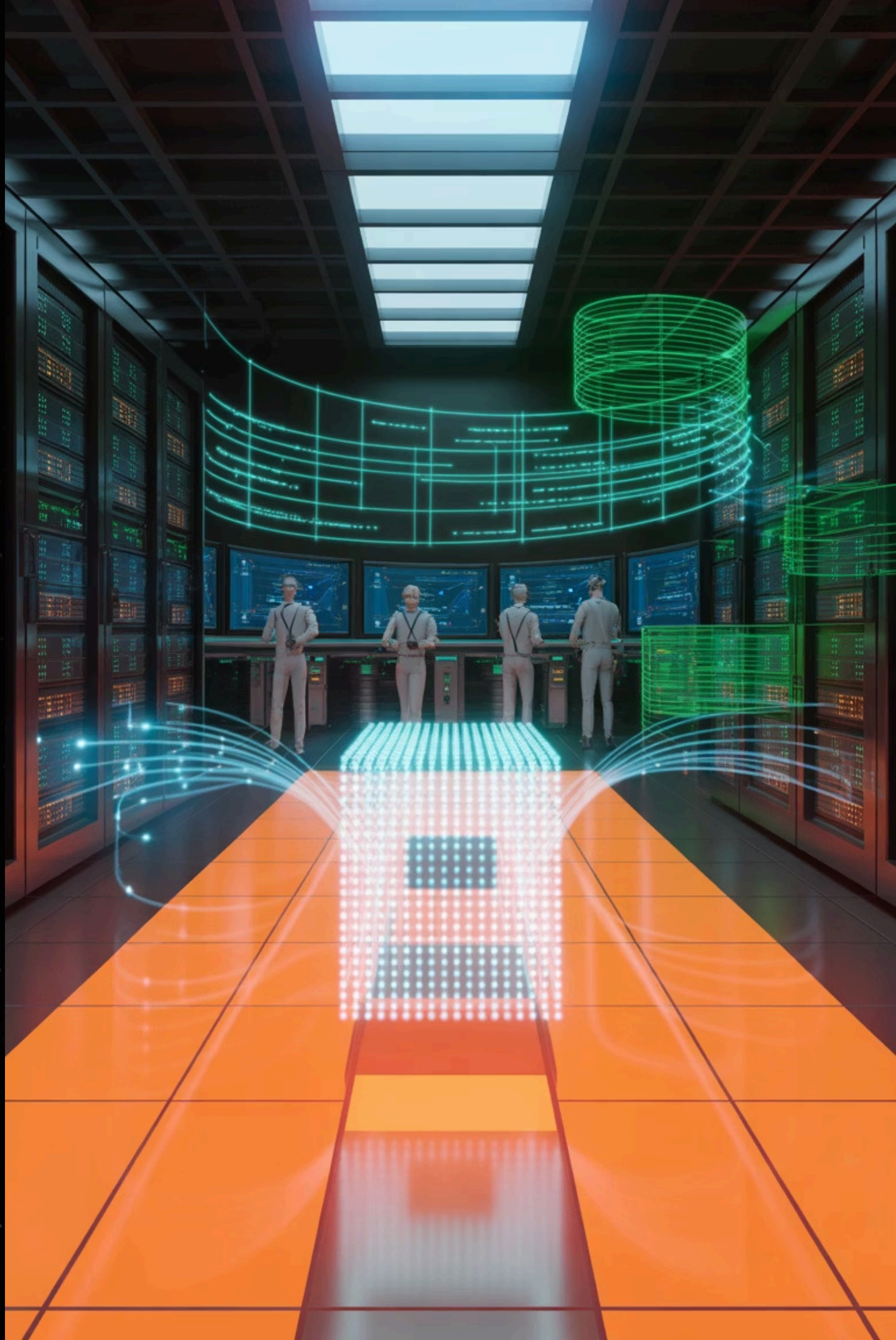
- ### Continuous Monitoring

  Alert on integrity violations in real-time across fleet

Zero Trust Architecture for VMs

Zero Trust operates on the principle: "**Never trust, always verify.**" In virtualized environments, this means eliminating implicit trust between VMs, continuous verification of identity, and enforcing least-privilege access at every interaction.

Traditional perimeter-based security assumes everything inside the network is safe. Zero Trust assumes breach and verifies every request regardless of origin.



Zero Trust Principles in Practice

Identity-Aware Micro-Segmentation

Enforce network policies based on workload identity, not IP addresses. VMs communicate only with explicitly authorized services.

Continuous Verification

Authenticate and authorize every access request in real-time using cryptographic identities and dynamic policy evaluation.

Real-Time Behavioral Monitoring

Monitor VM behavior for anomalies—unusual network connections, privilege escalations, or process executions trigger automatic response.

Mitigating Modern Threats

Lateral Movement Prevention

Micro-segmentation limits blast radius by preventing attackers from moving freely between VMs once inside the perimeter.

Insider Threat Mitigation

Continuous verification and behavioral monitoring detect anomalous actions by privileged users, including compromised admin credentials.

Compliance and Performance Considerations

Regulatory Alignment

PCI DSS 4.0: Confidential Computing and Zero Trust address requirements for cardholder data protection and network segmentation

HIPAA: TEEs provide technical safeguards for PHI during processing

GDPR: Data minimization and encryption requirements met through hardware isolation

Performance Impact

TEE Overhead: Modern implementations add 2-10% performance impact depending on workload

Attestation Latency: Remote attestation typically completes in 100-500ms

Optimization: Caching attestation results and selective TEE usage minimizes overhead

Emerging Trends and Future Directions

1

Post-Quantum Cryptography

Quantum-resistant algorithms being integrated into TEEs to future-proof encrypted workloads against quantum computing threats

2

Homomorphic Encryption

Perform computations on encrypted data without decryption, enabling fully encrypted analytics pipelines

3

ML-Based Anomaly Detection

Machine learning models analyze behavioral patterns to detect zero-day threats and sophisticated attacks in real-time

Thank You

Priyadarshni Shanmugavadivelu

Stanford Business School

Conf42.com JavaScript 2025