

Digital Forensic Investigation in Cloud Computing Environments

Presented By: Md Abu Sayeed

Research Context & Background

The Cloud Migration

Enterprise computing has shifted to IaaS, PaaS, and SaaS models.

The Paradigm Shift

Due to abstract virtualization, investigators must now rely exclusively on logical.

The Core Issue

This profound shift threatens forensic principles: immutability, provenance, and legal admissibility.

Research Problem

Evidence Volatility

Auto-scaling instantly wipes volatile RAM and ephemeral storage upon VM termination.

Multi-Tenant

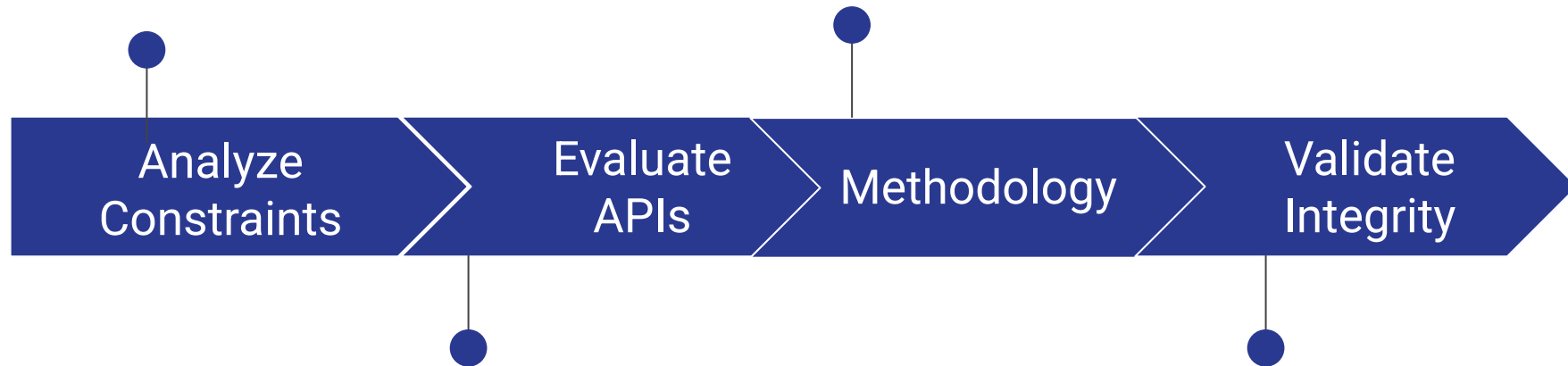
Hypervisor-level acquisition risks capturing innocent third-party data, violating the GDPR.

Chain of Custody

CSP APIs act as an opaque black box making cryptographic provenance highly difficult.

Evaluate Type-1
hypervisor
mechanics

Engineer Python
automation to
quarantine VMs



Assess logging
fidelity and
latency of CSP

Benchmark acquisition
speed and mathematically
prove

Literature Review & Identified Gap

Cloud Forensics

Wright & Smith (2023) established that dead-box methods are void in IaaS deployments.

Isolation Risks

Strom et al. (2024) highlighted that capturing collateral multi-tenant data breaks the CLOUD Act.

Conclusion

There is no unified, automated methodology that mathematically guarantees isolated, single-tenant acquisition.

Research Methodology & Architecture



Design Science
Research (DSR) &
Quantitative
Experimental
Simulation

Data Collection & Evaluation

- Synthesized dynamic artifacts (snapshots, RAM dumps, JSON logs) from the cloud testbed. Public datasets lack real-time hypervisor-level API telemetry.
- Evaluation Metrics (Quantitative)
 - Acquisition Latency
 - Cryptographic Integrity
 - Isolation Verification



Project Planning Timeline

The research follows a strict 10-week schedule to ensure completion prior to the submission deadline.

- Literature Review (Week 1-2)
- Cloud VPC Testbed Setup (Week 3-4)
- API Scripting (Week 5-6)
- Simulate Breaches (Week 7-8)
- Forensic Benchmarking (Week 9-10)

Impact & References

Equips DFIR teams and law enforcement with a repeatable, legally defensible blueprint for cloud investigations, replacing obsolete dead-box forensics.

- [1] R. Wright & J. Smith, "The Death of Dead-Box...", IEEE TIFS, 2023.
- [2] M. Al-Dosari & T. Hughes, "Evidence Volatility...", JCST, 2024.
- [3] B. Strom et al., "Jurisdictional Boundaries...", MITRE, 2024.

