

# INFUSE 2025: International Conference on Frontiers of Unified Science and Exploration



Contribution ID: 141

Type: Poster

## Zero Trust Architecture in Digital Forensics: Underlying Vulnerabilities.

The increasing sophistication of cyber incidents and distributed infrastructures has intensified the need for security models that support both resilience and evidentiary reliability. Zero Trust Architecture (ZTA), built on the principle of “never trust, always verify,” represents a significant departure from perimeter-based security by embedding continuous authentication, dynamic policy enforcement, and least-privilege access across systems. For digital forensics, ZTA offers distinct advantages: comprehensive logging, high-resolution telemetry, and strong identity verification generate valuable metadata that strengthens attribution, incident reconstruction, and legal admissibility. Proactive evidence capture and compliance-oriented monitoring further contribute to forensic readiness. However, ZTA also introduces challenges that complicate the reliability of digital evidence. Dependence on identity management systems risks compromised audit trails, insider misuse may appear legitimate within logs, and policy misconfigurations or excessive data volumes can obscure relevant artifacts. Moreover, issues of log integrity, third-party dependencies, and jurisdictional restrictions in cloud environments may undermine evidentiary trust. This paper contributes by systematically analyzing these forensic implications, highlighting both the strengths and vulnerabilities of ZTA, and proposing safeguards such as tamper-evident storage, behavioral analytics, automation, and integrated forensic readiness measures. ZTA, when fortified with these safeguards, can evolve from a security paradigm into a framework that enhances both cyber defense and forensic reliability.

**Keywords:** Zero Trust Architecture (ZTA); Digital Forensics; Forensic Readiness; Evidence Integrity; Insider Threats; Cybersecurity Investigations

**Author:** N BASUTKAR, Sakshi (JAIN (Deemed-to-be University))

**Co-author:** Mr NATARAJAN, VISHNU VENKATESH (JAIN (Deemed-to-be University))

**Presenter:** N BASUTKAR, Sakshi (JAIN (Deemed-to-be University))

**Track Classification:** Forensic Sciences