IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, November 2025
Impact Factor: 7.67

A Framework for Zero Trust Architecture in Cloud-Native Ecosystems: Authentication, Anomaly Detection, and Integration

Pavan R. Warule[1], Prajakta Muntode[2], Arati Wakare[3] and Prof. S. A. Wanave[4]
Department of Computer Engineering[1-4]
Adsul's Technical Campus, Ahilyanagar, India
Corresponding author: Pavan R. Warule (pavanwarule4961@gmail.com)
Savitribai Phule Pune University, Pune, India

Abstract: *The enterprise adoption of dynamic, distributed cloud-native architectures has rendered traditional perimeter-based security models obsolete. The implicit trust granted to entities "inside" the network creates a critical vulnerability to lateral movement attacks in microservice environments. Zero Trust Architecture (ZTA), founded on the principle of "never trust, always verify," emerges as the necessary security paradigm for this new ecosystem. This paper proposes a comprehensive, intelligent ZTA framework designed to address the unique challenges of microservices, containers, and serverless functions. The framework is built on three pillars:*

(1) a lightweight, scalable authentication stack utilizing automated workload identity via SPIFFE/SPIRE and performant, sidecarless service mesh enforcement planes; (2) an AI-driven continuous validation engine employing machine learning for behavioral anomaly detection and Explainable AI (XAI) for operational trust; and (3) a domain-specific integration model for applying ZTA principles to the unique constraints of 5G and IoT ecosystems. This work analyzes the critical performance trade-offs of modern ZTA implementations and presents a viable architectural path toward a secure, scalable, and observable cloud-native future..

Keywords: *Zero Trust Architecture.*

DOI: 10.48175/568