International Journal of Cloud Applications and Computing
Volume 16 • Issue 1 • January-December 2026

End-to-End Security for SDN Controllers in Distributed K8s Environments for Fog and Cloud

Asad Khan
https://orcid.org/0009-0009-5240-6946
University of Technology, Sydney, Australia

Priyadarsi Nanda
University of Technology, Sydney, Australia
Received: October 20th, 2025 | **Accepted:** December 24th, 2025

ABSTRACT

The deployment of software-defined networking (SDN) in distributed Kubernetes environments across fog and cloud systems introduces complex security challenges. Traditional approaches often fail to ensure secure, resource-efficient control-plane operations and verifiable node coordination at scale. This study proposes a three-layered security framework: (a) flexible control plan (FCP) integrates lightweight SDN controllers with runtime attestation for trusted execution in resource-constrained fog nodes; (b) secure software-defined offloading (SSDO) enforces encrypted, policy-driven inter-node communication and signature verification to prevent unauthorized coordination; and (c) sentinel-adaptive intrusion detection (SAID) uses an unsupervised deep learning autoencoder to detect anomalies and identify zero-day threats. Combined, these layers offer scalable, adaptive, and real-time security for distributed SDN-Kubernetes environments.

KEYWORDS

SDN, FCP, SSDO, SAID, Fog Computing, Cloud Infrastructure

INTRODUCTION

The rapid development of distributed computing paradigms like fog and cloud computing have transformed how modern digital infrastructures operate in the new era of scalable, low latency, and responsive services. Applications that require real-time processing and/or significant data management are now dependent on fog and cloud computing paradigms such as autonomous vehicles, industrial automation, and smart cities (Babou et al., 2024). At the heart of these systems is software-defined networking (SDN), a transformative way of managing networks that provides the ability to separate the control and data plane, enables centralized control, and provides for dynamic behavior of the network (Jin et al., 2025; Scano et al., 2023). The evolution of SDN is in conjunction with cloud and fog environments in fact, in recent years, Kubernetes has become the orchestration behemoth for fog-cloud ecosystems, enabling automatic deployment, scaling and operation of containerized or virtualized applications across multiple distributed nodes in many fog-cloud environments (Arzo et al., 2024; Sellami et al., 2022). The emergence of SDN, Kubernetes, and new distributed computing

DOI: 10.4018/IJCAC.398931

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

environments create numerous new and complicated security issues for the user, especially with respect to the availability, confidentiality, and integrity of the SDN controllers (Zeydan et al., 2022).

SDN controllers serve as the brain of the network, making it a high-value target for adversaries who seek to disrupt or manipulate network operations (Appari, 2022). In a typical distributed Kubernetes deployment, where workloads are distributed across fog and cloud layers, SDN controllers may be deployed across the network domain(s). The controllers will fail into the degrees of differing enforcement levels and security trusts, which increases surface risk considerably (Alamer, 2021). Since the SDN controller can be seen as a centralized tension point, it creates more attack surfaces of man-in-the-middle, denial-of-service, session hijacking, and unauthorized pending access attacks, in particular (Batewela et al., 2025). The impermanence of containerized deployments makes this risk even more challenging; ephemeral services, the constantly shifting network topologies and multi-tenancy situations introduce complexities into the intrinsic behaviours of the security policies that previously used to be instantiated (Carmona-Cejudo et al., 2023; Paolucci et al., 2021). The requirement to deploy situational environments and new attack vectors leads to an urgent need of an end-to-end security framework of SDN controllers which perform in distributed Kubernetes The security framework of Software-Defined Networking (SDN) controllers should comprise secure communication channels, robust authentication and authorization mechanisms, clearly defined policy enforcement domains, and resilience against both internal threats and externally identified adversaries (Prasanth & Uma, 2025). Nevertheless, from a security perspective, modern systems should move beyond traditional perimeter-based security, which assumes implicit trust within network boundaries, and instead adopt zero trust principles, where every access request is continuously verified. This approach enables consistent security enforcement in dynamic Kubernetes environments, including service mesh deployments and application programming interface (API) management layers. An application programming interface (API) is a standardized set of rules and protocols that enable communication and data exchange between software components and services. Fine-grained identity management and architecture are also emerging technologies which can be used as a solution to ensure that security can be handled easily.

Moreover, the integration of security into the orchestration and lifecycle management of SDN elements into Kubernetes environments necessitates a smooth integration between the container orchestration platform and the network layer (Pedone et al., 2021). Security involves automated certificate management, secure API gateways, encrypted service meshes, and audit logging. Also consider the unique characteristics of fog computing nodes, which are typically resource-constrained, have unreliable connectivity, and generally require lightweight and adaptive security protocols (Nunez-Gomez et al., 2021; Sami et al., 2021). This paper will examine the architectural design and implementation of end-to-end security for SDN controllers in distributed Kubernetes environments deployed over both fog and cloud infrastructures (i.e., cloud edge computing). A layered security approach is proposed, encompassing the use of cryptographic primitives, container-level isolation, runtime security tools, and adaptive threat detection to secure SDN controllers by reducing the number of attack vectors while sustaining the level of performance and agility that fog-cloud systems promise. We also analyze the relevant threat models and security mechanisms and discuss how these mechanisms can be integrated into a software-defined network to contribute a secure-by-design approach to managing software-defined networks in the next generation of distributed computing environments.

Such values of degradation are supported by a variety of unbiased measures (Batista Jr et al., 2021) with up to 18% latency inflation in SDN-Kubernetes orchestration through control-plane synchronization overhead and with more than 20% spoofing vulnerability in case of distributed controllers without runtime verification (Singh et al., 2022). Equally, as pointed out by Javanmardi et al. (2023), containerized SDN deployments with the fog workload always report false-positive rates of more than 12% using the traditional support vector machine (SVM)-based intrusion detection system (IDS), indicating the dire need to bridge the gap between adaptive and integrated security mechanisms.

This paper's contributions include the following:

28 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/end-to-end-security-for-sdn-controllers-in-distributed-k8s-environments-for-fog-and-cloud/398931

Related Content

A Hybrid Binary Bird Swarm Optimization (BSO) and Dragonfly Algorithm (DA) for VM Allocation and Load Balancing in Cloud

Thanwamas Kassanukand Khongdet Phasinam (2023). *International Journal of Cloud Applications and Computing (pp. 1-21).*

www.irma-international.org/article/a-hybrid-binary-bird-swarm-optimization-bso-and-dragonfly-algorithm-da-for-vm-allocation-and-load-balancing-in-cloud/318698

Applying the Updated Delone and Mclean is Success Model for Enterprise Cloud Computing Readiness

Omar Sabri (2016). *International Journal of Cloud Applications and Computing (pp. 49-54).*

www.irma-international.org/article/applying-the-updated-delone-and-mclean-is-success-model-for-enterprise-cloud-computing-readiness/159851

A Secure Framework to Prevent Three-Tier Cloud Architecture From Malicious Malware Injection Attacks

B. V. Subba Rao, Vivek Sharma, Neeraj Rathore, Devendra Prasad, Harishchander Anandaramand Gaurav Soni (2023). *International Journal of Cloud Applications and Computing (pp. 1-22).*

www.irma-international.org/article/a-secure-framework-to-prevent-three-tier-cloud-architecture-from-malicious-malware-injection-attacks/317220

Mobile Text Misinformation Identification Using Machine Learning

Sanjaikanth E. Vadakkethil Somanathan Pillaiand Wen-Chen Hu (2024). *Emerging Technologies and Security in Cloud Computing (pp. 236-251).*

www.irma-international.org/chapter/mobile-text-misinformation-identification-using-machine-learning/339403

Detection and Classification of Dense Tomato Fruits by Integrating Coordinate Attention Mechanism With YOLO Model

Seetharam Nagesh Appe, G. Arulselviand Balaji G. N. (2023). *Handbook of Research on Deep Learning Techniques for Cloud-Based Industrial IoT (pp. 278-289).*
www.irma-international.org/chapter/detection-and-classification-of-dense-tomato-fruits-by-integrating-coordinate-attention-mechanism-with-yolo-model/325947