

Course Title	Research Methodology in Computer Science
Course Code	AI800
Lecturer	Dr. Mohammed Anbar
Assignment Number	2
Name / ID	[Ahmed Shawky Hewidy] / [253001655]



Assignment 2 “problem statement and research objectives”:

Securing Cloud-Native Infrastructure in Telco-Cloud :

Container Isolation, Kubernetes Control-Plane Risk, and Multitenancy

Securing Cloud-Native Infrastructure in Telco-Cloud:

Container Isolation, Kubernetes Control-Plane Risk, and Multitenancy

Problem Statement: Closing the gap between compliance-based hardening and demonstrated attack resistance of the shared Kubernetes control plane in multitenant telco Containers-as-a-Service (CaaS).

In the field of cloud-native telecommunications infrastructure, there is a need to secure the shared Kubernetes control plane on which multitenant Containers-as-a-Service platforms depend. Telco clouds now run 5G network functions as containers on shared Kubernetes clusters, and operators share one cluster among tenants because edge sites cannot afford a dedicated cluster, or even a dedicated virtual machine, per tenant (Aiello et al., 2026; Şenel et al., 2023). The challenge is that the control-plane interfaces every tenant shares suffer from insufficient access restriction and missing rate limiting. Wang et al. (2025) demonstrated the consequences on Alibaba Cloud and Taikun Cloud: a malicious container leaked sensitive cluster information, drove control-plane CPU to 90%, and cost a co-located victim tenant 70% of its packets.

Solving this problem matters because of what these clusters carry. The workloads at stake are the AMF, SMF, and UPF, the 3GPP functions that handle live 5G signalling and traffic, and container escape ranks among the highest-scored risks against them (Aiello et al., 2026). An attack that crosses the control plane crosses every tenant on the cluster, so a single hostile workload can turn into a cross-function, cross-tenant compromise of infrastructure that carries public communications. Slice isolation, tenant confidentiality, and 5G service availability all rest on that one trust boundary holding.

Existing solutions approach the problem from three directions, and each falls short in the same way. Pattaranantakul et al. (2018) and Alnaim et al. (2022) work at the architecture level, through use-case-driven NFV threat analysis and a pattern-based security reference architecture, but both reason in hypervisors and virtual network functions, a framing that predates Kubernetes role-based access control and container runtimes. Morić et al. (2025) work at the operational level, hardening the API server, etcd, and access control against compliance baselines, yet a cluster can pass those checks and still fall to the interface attacks Wang et al. (2025) executed, because configuration benchmarks do not test for missing rate limits or weak access restriction. Şenel et al. (2023) work at the workload level, isolating tenant pods in Kata Containers and reserving whole nodes through node-level slicing, which wraps the pods but leaves the shared control plane bare. None of these defenses has faced an adversary.

The limitations of current defenses leave operators choosing between tenant density and tenant safety with no data on the trade-off: shared clusters are cheaper (Şenel et al., 2023), yet a hostile tenant can degrade its neighbours through the plane they share (Wang et al., 2025). No published work hardens the control plane for multitenant telco CaaS and then proves the hardening by re-running the attacks against it. Therefore, there is a clear need for research that produces a control-plane hardening approach whose resistance is demonstrated and measured rather than asserted.

Research Objectives

The primary goal of this research is to secure the shared Kubernetes control plane in multitenant telco CaaS, so that tenant density does not come at the price of cross-tenant compromise. Five objectives serve this goal, and each one answers a challenge raised in the problem statement.

1. To identify and classify the Kubernetes control-plane interfaces a hosted container can reach in multitenant telco CaaS, mapping weaknesses of insufficient access restriction and missing rate limiting to containerized 5G network functions (Wang et al., 2025; Aiello et al., 2026). The measurable output is a documented attack-surface taxonomy.
2. To propose and design a control-plane hardening framework that adds per-tenant access restriction and rate limiting on top of existing compliance baselines, closing the weakness classes identified under the first objective (Morić et al., 2025; Wang et al., 2025).
3. To integrate the proposed framework with workload-level isolation, namely Kata Containers and node-level slicing, so that control-plane protection and container isolation operate together on one shared cluster (Şenel et al., 2023).
4. To evaluate the framework by replaying tenant-originated control-plane attacks and measuring information leakage, control-plane CPU load, and co-tenant packet loss, in comparison with a compliance-only hardened baseline (Wang et al., 2025; Morić et al., 2025).
5. To compare the resource cost of the validated defenses against the efficiency that motivates shared clusters in the first place, giving operators a measured basis for weighing tenant density against attack resistance at the edge (Şenel et al., 2023).

Each objective produces something that can be checked: a taxonomy, a framework, an integration, a set of attack measurements, and a cost comparison. The first objective defines the boundaries of the problem, the second and third build the defense, and the fourth and fifth deliver the adversarial and economic evidence that current work on multitenant telco CaaS does not provide.

References

- 1-Aiello, S. T., Rimal, B. P., Sheldon, F. T., & Wang, Y. (2026). Investigating security vulnerabilities in 5G control and user planes: Attack patterns and protection strategies. *Journal of Cybersecurity and Privacy*, 6(1), 37.
- 2-Alnaim, A. K., Alwakeel, A. M., & Fernandez, E. B. (2022). Towards a security reference architecture for NFV. *Sensors*, 22(10), 3750.
- 3-Morić, Z., Dakić, V., & Čavala, T. (2025). Security hardening and compliance assessment of Kubernetes control plane and workloads. *Journal of Cybersecurity and Privacy*, 5(2), 30.
- 4-Pattaranantakul, M., He, R., Song, Q., Zhang, Z., & Meddahi, A. (2018). NFV security survey: From use case driven threat analysis to state-of-the-art countermeasures. *IEEE Communications Surveys & Tutorials*, 20(4), 3330–3368.
- 5-Şenel, B. C., Mouchet, M., Cappos, J., Fourmaux, O., Friedman, T., & McGeer, R. (2023). Multitenant containers as a service (CaaS) for clouds and edge clouds. *IEEE Access*, 11, 144574–144601.
- 6-Wang, C., et al. (2025). Losing control: Exposing security weaknesses of Kubernetes control plane interfaces. *Computers & Security*, 159, 103931.