

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



Assignment Report:

Securing Cloud-Native Infrastructure in Telco-Cloud : Container Isolation, Kubernetes Control-Plane Risk, and Multitenancy

Table of Contents

Table of Contents	2
1. Summary Research Paper's:.....	3
2. Critical Analysis:	5
3. Connections:	5
4. Conflicts Between the Findings:.....	6
5. Synthesis Matrix.....	7
7. References	9

1. Summary Research Paper's:

Paper 1. Pattaranantakul et al. (2018), NFV Security Survey

This survey builds its threat analysis from use cases rather than a generic checklist. It walks through the ETSI NFV architecture, the infrastructure layer (NFVI), the virtual network functions, and the MANO stack, and shows where each use case creates exposure. The authors catalog threats such as hypervisor breakout, tampered VNF images, insecure MANO interfaces, and insider misuse from the orchestrator's privileged position. They then map those threats to countermeasures: access control, remote attestation, topology and configuration validation, and a security orchestration layer they call a security manager. Their argument is that NFV's programmability, the same property that makes it useful, widens the attack surface because control becomes centralized and software-defined. They position security orchestration as the missing piece, rather than bolting point defenses onto individual functions. For anyone working on virtualized telco infrastructure, it remains a broad reference point for the NFV threat space.

Paper 2. Senel et al. (2023), Multitenant Containers as a Service (CaaS)

Senel and colleagues tackle a cost problem in CaaS: giving each tenant its own Kubernetes cluster wastes resources, which is unworkable at the edge where capacity is tight. They built EdgeNet, a framework that lets tenants share one cluster while keeping their workloads apart. Isolation is the hard part of sharing, so they route multi-tenant pods through Kata Containers, which wrap each pod in a lightweight VM, and add node-level slicing so a tenant can reserve whole nodes when it needs stronger separation. The target is the edge, where resources are too tight to spend a whole VM per tenant. It ships as liberally-licensed open-source software. The design shows you can trade some isolation strength for density without giving it all up, by letting each tenant pick the runtime that fits the workload.

Paper 3. Aiello, Rimal, Sheldon & Wang (2026), Security Vulnerabilities in 5G Control and User Planes

This PRISMA-aligned review catalogs weaknesses specific to 5G Standalone and maps each one directly to 3GPP network functions and interfaces: the AMF, SMF, and UPF, the N2 and N4 reference points, and the service-based architecture APIs. Every vulnerability is tagged by evidence level, from theoretical analysis to documented live-network exploitation, and given a transparent risk score. The headline risks are control-plane signaling floods, PFCP misuse on N4, and container escapes. The authors argue that the user plane and slice isolation get far less attention than they deserve.

They close with hardening priorities per plane and a research agenda pointing toward 6G. The container-escape finding is the direct bridge to CaaS, because 5G network functions run as containers, so a breakout becomes a cross-function compromise. Its value is tying otherwise abstract 5G threats to concrete 3GPP interfaces.

Paper 4. Moric, Dakic & Cavala (2025), Security Hardening and Compliance Assessment of Kubernetes

The reference lists Cavala alone, but the published authors are Moric, Dakic, and Cavala. The paper combines a walk-through of Kubernetes security with hands-on hardening and compliance testing. It covers architecture, networking, and storage first, then moves to practical controls: image scanning, authentication and authorization, admission control, and monitoring and logging. The compliance angle checks configurations against recognized baselines rather than treating hardening as ad hoc. The emphasis lands on the control plane, the API server, etcd, and the access-control layer, and on the workloads running above it. It reads as a hardening playbook backed by assessment, aimed at operators who need to know which knobs to turn. It comes out of Algebra Bernays University in Zagreb, and it complements the attack papers by describing the defensive baseline they assume.

Paper 5. Wang et al. (2025), Losing Control: Weaknesses of Kubernetes Control Plane Interfaces

This is the empirical attack paper of the set. Using static analysis of Kubernetes control-plane interfaces, the authors find two recurring flaws: insufficient access restriction and missing rate limiting. A malicious container can therefore fire unrestricted requests at those interfaces. They define four attack strategies and run seven attacks across four case studies, testing on Alibaba Cloud and Taikun Cloud. Four attacks succeed on Alibaba and five on Taikun, with the difference coming from default settings and component choices. The impact is concrete: sensitive cluster information leaks, the control plane drops packets and consumes up to 90% of CPU, and a co-located victim container loses up to 70% of its packets and cannot resolve non-local DNS. They disclosed the issues to the vendors and communities, who confirmed them and committed to fixes.

Paper 6. Alnaim, Alwakeel & Fernandez (2022), Towards a Security Reference Architecture for NFV

This paper builds a security reference architecture for NFV using a pattern-based method. Rather than list threats loosely, the authors model them as misuse patterns, structured descriptions of how an attack unfolds against the NFV architecture, and use those to derive where security controls belong. The reference architecture is expressed in UML and covers the NFV stack including its role in 5G. Fernandez's pattern approach gives the work a systematic backbone: enumerate misuse patterns, then position countermeasures against them in a reusable blueprint. The aim is an architecture teams can instantiate, not a one-off analysis. It sits at the design end of the spectrum, upstream of operational hardening and attack demonstrations, and offers a structured way to reason about NFV security before deployment.

2. Critical Analysis:

The strongest work here is the kind that tests something against an adversary or ships running code. Wang et al. carry the most weight, because they attacked real commercial clouds, Alibaba and Taikun, got vendor confirmation, and turned control-plane exposure from a warning into measured harm: up to 90% CPU consumption and 70% victim packet loss. Senel et al. earn credit for the opposite reason, working open-source multitenancy running in production on EdgeNet, with node-level slicing that hands tenants Kata-grade isolation only where they need it. The reviews and the architecture papers do the framing well. Pattaranantakul's use-case method keeps its threat list grounded, Alnaim's misuse-pattern approach makes the NFV reference architecture reusable across deployments, Aiello's PRISMA scoring is honest about which 5G vulnerabilities are theoretical versus live-exploited, and Moric and Cavala give operators a concrete hardening and compliance baseline instead of loose advice.

The shared weakness is evidence. Four of the six, Pattaranantakul, Alnaim, Aiello, and to a degree Moric and Cavala, describe or prescribe without an adversary in the room, so their resistance is asserted rather than shown. Compliance-to-baseline is the clearest case: a cluster can pass a benchmark and stay open to the exact interface attacks Wang demonstrates. The second recurring gap is framing. The older NFV papers reason in hypervisors and VNFs, which needs translation before it applies to containers and Kubernetes RBAC, the layer a CaaS-in-5G study actually cares about.

3. Connections:

1. All six circle the same problem from different distances: how to secure virtualized, multitenant infrastructure that carries telecom traffic. Pattaranantakul (2018) and Alnaim (2022) frame it at the NFV architecture level. Aiello (2026) brings it down to 5G-specific 3GPP functions. Senel (2023), the two Kubernetes papers, and Aiello all converge on containers and orchestration as the layer that now matters most.
2. Isolation runs through every one of them. Whether it's hypervisor breakout in Pattaranantakul, Kata Containers and node slicing in Senel, container escape in Aiello, or cross-tenant control-plane impact in Wang, each paper is really arguing about where the trust boundary sits and how strong it is.
3. The control plane keeps surfacing as the high-value target. Aiello names control-plane signaling floods among the top risks. Moric and Cavala center their hardening on the API server, etcd, and access control, and Wang attacks exactly those interfaces. The three describe the same component as defenders, assessors, and attackers respectively.
4. Multitenancy is the risk multiplier that connects the systems work to the attack work. Senel wants shared clusters for edge density; Wang shows what a hostile tenant does to co-located victims on a shared control plane. Same architecture, opposite lens. Taken together the six span the full lifecycle: design and taxonomy (Alnaim, Pattaranantakul), operational hardening (Moric and Cavala), systems building (Senel), 5G-specific synthesis (Aiello), and empirical attack (Wang).

4. Conflicts Between the Findings:

1. Senel and Wang disagree on shared tenancy. Senel argues a shared Kubernetes cluster with selective Kata isolation is efficient enough for the edge and safe enough for most workloads. Wang's results cut against that: on real clouds, a malicious tenant degraded co-located victims through the shared control plane, up to 70% packet loss. Both can hold, since Senel offers Kata for the workloads that need it, but the default posture differs sharply. One side leans toward density, the other treats the shared control plane as a live liability.
2. Compliance and demonstrated resistance pull apart. Moric and Cavala treat hardening plus baseline compliance as the route to a secure cluster. Wang implicitly disputes that a compliant cluster is a safe one, since the weaknesses they exploit, missing rate limits and weak access restriction, aren't necessarily caught by configuration benchmarks. A defensive checklist and an adversarial proof are not the same evidence.
3. The studies split on what counts as evidence. Alnaim and Pattaranantakul build frameworks and taxonomies with no measurement. Wang measures on production clouds. Aiello sits between, scoring findings by how well-documented each is. The surveys assert coverage; the attack paper proves specific gaps. They disagree on what it means to know a threat is real.
4. The set is divided between NFV framing and container framing. Pattaranantakul and Alnaim reason in hypervisors and VNFs. Senel, Moric and Cavala, and Wang reason in containers, runtimes, and orchestrators. Aiello bridges the two by mapping 3GPP functions onto containerized deployments. For a CaaS-in-5G study the container framing is the relevant one, and the older NFV papers need translation before they apply.

5. Synthesis Matrix

#	Study	Authors	Year	Type / Design	Key findings	Methodology	Limitations
1	NFV Security Survey: From Use Case Driven Threat Analysis to State-of-the-Art Countermeasures	Pattaranantakul, M.; He, R.; Song, Q.; Zhang, Z.; Meddahi, A.	2018	Survey / Case study	Identifies NFV-specific threats across NFVI, VNFs, and the MANO stack. Threats: hypervisor breakout, VNF image tampering, insecure orchestration interfaces, insider abuse. Argues for a security orchestration layer (security manager) over isolated point defenses.	Approach: use-case-driven threat analysis mapped to the ETSI NFV reference architecture. Data: qualitative synthesis of prior work; no experiments.	VM/hypervisor centric; little on containers, orchestrator RBAC, or container escape. No measurement or validation (survey only). Predates wide Kubernetes use in telco.
2	Multitenant Containers as a Service (CaaS) for Clouds and Edge Clouds	Şenel, B. C.; Mouchet, M.; Cappos, J.; Fourmaux, O.; Friedman, T.; McGeer, R.	2023	Experimental	Native multitenancy on a shared cluster is more resource-efficient than one-cluster-per-tenant. Kata Containers give VM-grade isolation where needed; node-level slicing reserves isolated subclusters. Released open-source; runs in production on the EdgeNet testbed.	Approach: framework engineering extending Kubernetes. Isolation via Kata Containers and programmable node-level slicing. Assessment: real deployment on the EdgeNet testbed.	No adversarial evaluation of the shared control plane under a hostile tenant. Isolation is demonstrated functionally, not stress-tested against attacks.
3	Investigating Security Vulnerabilities in 5G Control and User Planes: Attack Patterns and Protection Strategies	Aiello, S. T.; Rimal, B. P.; Sheldon, F. T.; Wang, Y.	2026	Observational	Maps 5G SA vulnerabilities to 3GPP functions/interfaces (AMF, SMF, UPF; N2, N4; SBA APIs). Top risks: control-plane signaling floods, PFCP misuse on N4, container escapes. Flags the user plane and slice isolation as under-studied.	Approach: PRISMA-aligned systematic review. Mapping to 3GPP interfaces; evidence tagged theoretical to live-exploited. Assessment: transparent risk scoring per vulnerability.	Review only; no new empirical data. Risk scoring carries subjectivity. Stays at 3GPP-function level; container/Kubernetes internals not dissected.
4	Security Hardening and Compliance Assessment of Kubernetes Control Plane and Workloads	Morić, Z.; Dakić, V.; Čavala, T. (reference cites Čavala only)	2025	Experimental	Practical hardening path: image scanning, authN/authZ, admission control, monitoring and logging. Configurations checked against recognized compliance baselines. Concentrates on the control plane (API server, etcd, access control) and workloads.	Approach: conceptual review plus hands-on hardening and compliance assessment. Covers architecture, networking, storage, then applied controls. Assessment: configuration checks against baselines.	Compliance-to-baseline can become checkbox security. No red-team of the hardened configuration. Passing a benchmark is not resistance to specific interface attacks.
5	Losing Control: Exposing Security Weaknesses of Kubernetes Control Plane Interfaces	Wang, C. et al. (authors to confirm against source)	2025	Experimental (Case Study)	Control-plane interfaces suffer insufficient access restriction and missing rate limiting. 4 strategies, 7 attacks, 4 case studies: 4 succeed on Alibaba, 5 on Taikun. Impact: info leakage; control plane up to 90%	Approach: static analysis of control-plane interface mechanisms. Design and execution of attacks across four case studies.	Only two providers; the 4-vs-5 results don't generalize cleanly. Static analysis plus case studies may miss runtime behavior.

					CPU; co-located victim up to 70% packet loss. Vendors confirmed and committed to fixes.	Assessment: experiments on Alibaba Cloud and Taikun Cloud; responsible disclosure.	Tied to the tested platforms' defaults and components.
6	Towards a Security Reference Architecture for NFV	Alnaim, A. K.; Alwakeel, A. M.; Fernandez, E. B.	2022	Conceptual research	Produces a reusable NFV security reference architecture from misuse patterns. Expressed in UML; covers NFV's role in 5G. Misuse patterns drive where controls belong; a blueprint teams can instantiate.	Approach: pattern-based method (design-science). Enumerate misuse patterns against the NFV architecture; position countermeasures. Assessment: formalized as a UML reference architecture.	Abstract and unvalidated; no implementation or measurement. Inherits NFV/VM framing; containers and Kubernetes RBAC not first-class. Real-world resistance asserted, not demonstrated.

7. References

1. 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.
2. 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.
3. 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.
4. 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.
5. Wang, C. et al. (2025). Losing Control: Exposing Security Weaknesses of Kubernetes Control Plane Interfaces. *Computers & Security*, 159, 103931. (Author list to confirm against source.)
6. Alnaim, A. K., Alwakeel, A. M., & Fernandez, E. B. (2022). Towards a Security Reference Architecture for NFV. *Sensors*, 22(10), 3750.