Securing Private LTE and 5G Deployments in Hybrid Cloud: A Practical Framework

[1]Veeresh Nunavath
[1]Independent Researcher,
[1]University of Southern Indiana & Indiana

***Abstract*—Combining the benefits of the hybrid cloud infrastructures and the private LTE and 5G networks is a significant step ahead in business network operations, as it increases flexibility, performance, and control. Nonetheless, the convergence also creates a broader area of attack and even security challenges that the traditional models can poorly cover. This review introduces a multi-layered and practical network context on how to offer LTE and 5G-based private networks in hybrid cloud settings based on contemporary cloud-first concepts and telecom-grade security demands. The article addresses such critical elements of this framework as identity and access management, zero trust architecture, secure network segmentation, end-to-end encryption, container and supply chain security, and full observability. This paper proposes a practical framework, synthesizing industrial best practices and peer-reviewed insights, to secure private LTE/5G deployments in hybrid cloud environments. This survey shows the need to harmonize paradigms of telecom and IT security to come up with a unified and future-proofed defense paradigm that would sustain the operation of mission-critical services in distributed cloud-edge platforms.**

***Index Terms*—Private 5G, LTE, Hybrid Cloud, Zero Trust Architecture, Network Security, Container Security, 5G Core, Identity and Access Management, Network Segmentation**

I. INTRODUCTION

A combination of the private mobile network and hybrid cloud computing has established a revolutionary basis for industrial and enterprise-level communication. Following an international deployment of proprietary LTE and 5G systems, companies now have the means to have all their own secure and high-performance mobile infrastructures free of any public telecom provider. These networks can be specialized to particular organizational requirements and have greater speed bandwidth, <5ms latency in 5GC deployments, and greater quality of service (QoS) control. The application ranges include smart manufacturing, autonomous vehicle control, telemedicine, and critical infrastructure control, which not only require optimal performance but also reliable security.

At the same time, hybrid cloud systems in which private infrastructure is integrated with public cloud options are becoming crucial in facilitating the demands of the complex, elastic computing needs of 5G solutions. Telecom services that are becoming microservices on containerized cloud-native infrastructure platforms include the 5G Core (5GC), User Plane Function (UPF), and Network Exposure Function (NEF) being dispersed between on-site and cloud data centers. Hybrid cloud 5G brings advantages in elasticity and orchestration, yet it introduces new vulnerabilities across control and user planes [1, 2]. Nonetheless, it also causes major security issues. These are the greater exposure to cyber threats, lengthy attack surfaces across the cloud and the edge, multi-vendor trust complexities, and a deficiency in compliance enforcement. Also, the distributed design of cloud-native 5G networks results in anonymity issues in preserving confidentiality, availability, and integrity of instantiated network entities that are dynamically created and destroyed. There is a need for a practicable and multi-dimensional security framework that secures the deployment of private LTE and 5G hybrid cloud. This involves the securing of the underlying infrastructure, protection of the data and the network flows, secure access management, container run-time protections, and deployment lifecycle visibility. The subsequent sections explain a layered framework regarding these challenges.

II. THREAT LANDSCAPE IN PRIVATE 5G AND LTE HYBRID DEPLOYMENTS

The combination of the hybrid cloud platforms and private wireless networks creates a very dynamic threat environment that crosses physical, virtual, and application planes. Prior research distinguishes cloud-specific vulnerabilities from telecom-specific threats and vulnerabilities of the telecom infrastructure. The threat model should rather incorporate both domains for consideration.

In the case of hybrid LTE and 5G implementation, malicious end-users may have access to vulnerable APIs, plaintext data connections, poor access controls, and tainted container images. There are also more risks because of the Service-Based Architecture (SBA) used in 5G, where work between network functions is carried out by RESTful APIs and, in case they are not designed well, over the internet or badly authenticated [1, 2]. The other common issue is misconfiguration of security groups or permissions over the components provided on cloud platforms, which is further utilized in enterprise cloud attack campaigns.

Additionally, hybrid clouds usually incorporate the multi-access edge computing (MEC) nodes that may be physically located at the sources of data or the end-users. These endpoints might not have that high physical security, which makes them more susceptible to hardware tampering, malicious USB insertion, or even rogue node deployment [3]. As there is a risk that the scope of private networks will extend into operational technology (OT) scenarios, increased attack surfaces include the legacy industrial devices that have not been sufficiently hardened against cyberattacks. Advanced persistent threats (APTs), data interception, credential thefts, and lateral movement are also trending as security issues, as they may be initiated in the trusted segments within hybrid clouds [1, 4]. A combination of these threats requires a 5G security model design that is comprehensive, adaptive, and based in terms of continuity of visibility and risk management.

III. IDENTITY AND ACCESS MANAGEMENT (IAM) AND ZERO TRUST ARCHITECTURES

In a hybrid cloud 5G implementation in the private setting, identity and access control (IAM) is essential to ensure protection over access to the sensitive functions of the network, its data, and privileged operations. IAM policies should include enforcing the least privilege access, multi-factor authentication (MFA), and fine-grained access control, not only telecom-specific interfaces, but also to cloud-native environments. The 5G networks will authenticate user equipment (UE) based on 5G-AKA and EAP-AKA reference improved protocols. Although this provides a high level of identity assurance on mobile devices, IAM on administrative access, particularly that which spans Kubernetes control planes, virtual machines, and API endpoints, must be compatible with contemporary cloud-native identity cubes.

Centralized identity governance can be achieved by federated IAM architectures that can serialize identity with OAuth 2.0, OpenID Connect, or Security Assertion Markup Language (SAML) to span hybrid clouds [5]. These criteria aid in creating confidence with heterogeneous cloud regions and on-site parts, and also make it possible to utilize Single Sign-On (SSO) and remote revocation of permissions.

Zero Trust Architecture (ZTA) supports these IAM practices by considering all the network traffic unsafe, irrespective of its source. ZTA frameworks provide authentication and ensure authorization on any connection, perform ongoing risk analyses, and pay specific attention to micro-segmentation to minimize the attack surface [6]. Access control is based on the policies implemented on an identity basis instead of IP-based firewalls or non-dynamic routing policies.

The lateral movement in the cloud-native 5G core can be limited by micro-segmentation technologies (Istio, Linkerd, or network policy engines (e.g., Calico)) that enforce a service-level access control between containers or services.

IV. SECURE NETWORK ARCHITECTURE AND SEGMENTATION

The architectural design of the network functions and how they are connected is one of the key elements of any hybrid 5G implementation. Segmentation of secure networks allows for to elimination of lateral movement of outsiders through the infrastructure and limits the consequences of any possible attacks.

The aspects of network segmentation in cloud-native environments are founded on logically isolated networks, which are called within the concept of the Virtual Private Clouds (VPCs), and with the policies of the software-defined networking (SDN). Every 5G network function (including the Access and Mobility Management Function (AMF), the Session Management Function (SMF), and the Unified Data Management (UDM)) has to be positioned in separate zones, with the allowed type of inter-component communication being extremely limited to specific channels [7, 8].

All security policies should be applied in a way that disallows by default, and there should be specific allow-rules mentioning the services to communicate with each other. Such a default deny model coincides with the concept of zero trust and is particularly important in 5G networks with many microservices that dynamically interact with each other through a service mesh. Furthermore, the public cloud vendors enable fine-grained access control based on network policies via Security groups, NACL, and IAM-related controls, which associate access controls to service identities. Connection between the components of the hybrid cloud and edge sites must be covered through VPNs or secure cross-connections, like IPSec, WireGuard, or TLS-based proxies [8, 9]. SDN and orchestration mechanisms have to support dynamic response to threats by detecting suspicious flows and redirecting or isolating them, hence controlling them in a proactive security posture.

V. DATA SECURITY: ENCRYPTION, INTEGRITY, AND CONFIDENTIALITY

In hybrid 5G deployments, constant data movement between clouds, edges, and devices necessitates strict encryption and integrity measures across all communication layers. TLS 1.3 with certificate pinning and Perfect Forward Secrecy (PFS) is essential for securing the control plane, while IPsec tunnels are recommended by 3GPP for protecting user plane traffic, particularly when the User Plane Function (UPF) runs on public cloud infrastructure [4]. To protect sensitive assets like SIM profiles, TLS keys, and session tokens, HashiCorp Vault integrates with Kubernetes via the CSI (Container Storage Interface) Secrets Store Driver, dynamically mounting secrets as read-only volumes in pods rather than storing them in plaintext. Vault maps Kubernetes Service Accounts to Vault roles and policies, ensuring workloads only access the secrets they are authorized to use, such as TLS keys for control-plane pods. This method supports automatic rotation and avoids manual secret management, strengthening security. Additionally, FIPS 140-2-compliant encryption, secure hashes (SHA-256+), and digital signatures are employed to verify the integrity of configurations, software updates, and logs [10, 11].

Such secrets as SIM profiles, configuration files, and session keys should not be stored as plaintext. Such secret management tools as Vault and Kubernetes Secrets, when deployed using RBAC and audit logs, can support access policy enforcement and detect unauthorized access requests [10]. When verifying the integrity of information, secure hashes (SHA-256 or stronger) and digital signatures are used to confirm that the configuration files, software updates, and transmitted data have not been altered [11]. Logs and monitoring data should also incorporate confidentiality and integrity, as likely to carry tactical knowledge that can be used by adversaries.

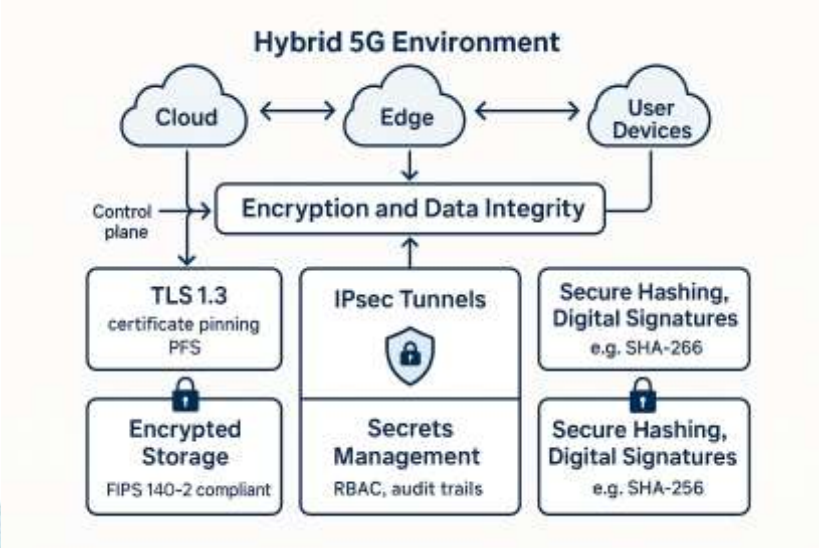

Figure 1: Hybrid 5G Security Framework

A layered security model showing encryption and data integrity across user devices, edge, and cloud. Key features include TLS 1.3, IPsec tunnels, encrypted storage, secrets management, and secure hashing (e.g., SHA-256) to protect control and user plane communications.

VI. CONTAINER AND SUPPLY CHAIN SECURITY

As more and more 5G Core Network Functions (NFs) are offered in the form of containerized workloads, the supply chain and container runtime emerge as very significant security areas of concern. Vulnerable container images can be used by attackers to induce malicious code into CI/CD streams or manipulate container orchestration APIs. The protection of images starts with the application of small base images and, hardened configuration. Misconfigurations and Common Vulnerabilities and Exposures (CVEs) should be scanned with tools like Clair, Trivy, or Anchore that are to be integrated with a build pipeline [12]. All images should be cryptographically signed with systems like Notary or Sigstore to avoid tampering and verify origin.

Table 1: Security Toolchain Across CI/CD and Runtime Layers in Telecom EKS Environments

Layer	Security Tool	Function
CI Pipeline	Trivy, Anchore	CVE Scanning
Signing	Notary, Cosign	Provenance + Tamper Prevention
Runtime	seccomp, SELinux	Host Isolation

Containers have to be run in a limited permissions environment once deployed. Examples of such capabilities are seccomp, AppArmor, and SELinux, which apply the least-privilege execution profiles and isolate workloads on their host OS and between each other [13]. Admission Controllers should be added to Kubernetes, deny running containers not properly signed or that disrespect pod security policies, to eliminate the risk posed by the supply chain. CI/CD pipelines have to incorporate SBOMs (Software Bill of Materials), a way to keep listing dependencies and impose a strict code review and confirmation workflow. Through these mechanisms, the probability of dependency confusion or injection of malicious third-party modules is decreased [14].

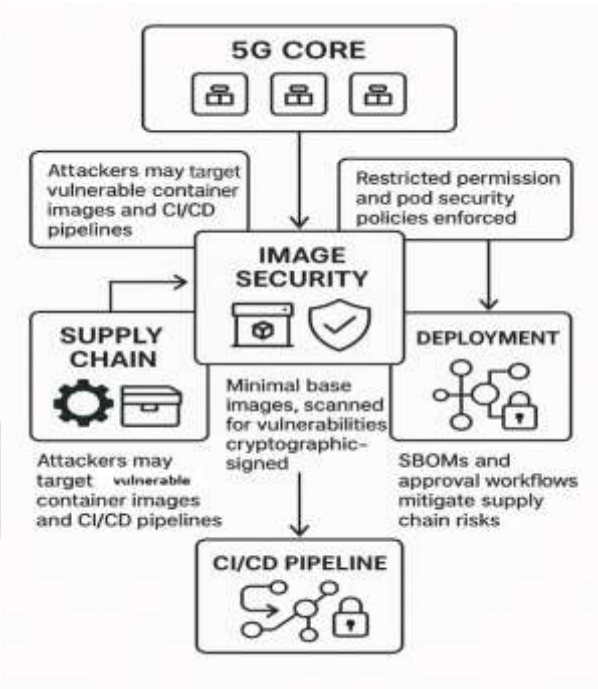

Figure 2: Image Security in 5G Core Deployment Pipelines

This diagram outlines the role of image security in protecting 5G core components from supply chain and CI/CD pipeline threats. It emphasizes the use of minimal, vulnerability-scanned, cryptographically signed container images, with controls including SBOMs, restricted permissions, and secure deployment workflows to mitigate supply chain risks.

VII. Monitoring, Observability, and Compliance

End-to-end observability of hybrid 5G networks not only supports performance tuning but also enables rapid threat detection and regulatory compliance enforcement. Monitoring must span infrastructure, application, and network layers in an integrated manner. Platforms such as Prometheus, Grafana, Fluentd, and ELK (Elasticsearch, Logstash, Kibana) provide container-native observability, aggregating metrics, logs, and traces from network services (NS) under 5G and their orchestrators. These insights are consolidated into secure, centralized logging frameworks that enforce access controls and make tampering detectable [15]. Security Information and Event Management (SIEM) systems ingest this telemetry to detect anomalies such as unexpected traffic flows, repeated failed login attempts, or unauthorized resource provisioning. Advanced intrusion detection systems can apply machine learning to uncover subtle threats. In regulated telecom environments, continuous compliance with standards like GDPR, HIPAA, and ISO 27001 is essential, and automation of compliance scanning ensures both cloud and on-premise environments remain aligned with these standards.

For instance, policy drift detection was observed during a runtime audit, where kube-bench flagged a baseline deviation in the SMF (Session Management Function) container runtime configuration, identifying an unauthorized capability being granted to a pod. Such automated detection enables immediate remediation by reverting the pod's security context to the approved baseline, preventing potential exploitation. Configuration integrity is enforced using auditing and policy validation tools, applying consistent templates across Kubernetes clusters, virtual networks, IAM roles, and firewalls, ensuring that any deviation triggers alerts and automated remediation workflows.

To facilitate a comprehensive approach to organizing security and observability in the hybrid 5G networks, it is vital to figure out the alignment of a particular set of tools with the various layers of functionality of the deployment.
Table 2 below lists some of the main technologies with the security goals and functional advantages on these layers:

Layer	Security/Observability Objective	Representative Tools/Technologies	Outcome / Benefit
Infrastructure Layer	Asset inventory, node integrity, and physical access logs	AWS Systems Manager, Azure Security Center, Guardicore	Visibility into hardware/software assets and state
Container Runtime Layer	Behavioral anomaly detection, runtime policy enforcement	Falco, Sysdig Secure, Aqua Security	Real-time detection of abnormal container behavior
Orchestration Layer	Misconfiguration monitoring, RBAC enforcement	Open Policy Agent (OPA), Kyverno, Kube-bench	Ensures policy compliance and secure orchestration
Service-to-Service Layer	Network behavior tracing, service dependency mapping	Istio, Linkerd, Jaeger	Traces communication flows, identifies latency or risks
Edge Nodes / MEC Layer	Edge device telemetry and zero-trust posture	Zscaler, Illumio Edge, Azure Arc	Maintains consistent policy and observability at edge
Compliance Layer	Policy validation, baseline drift detection	Prisma Cloud, Wiz, Qualys Compliance	Maintains audit-readiness and regulatory compliance

Layer	Security/Observability Objective	Representative Tools/Technologies	Outcome / Benefit
AI/Analytics Layer	Threat pattern learning, predictive risk analytics	Splunk ML Toolkit, Darktrace, IBM QRadar	Proactive threat hunting using behavioral models

VIII. CONCLUSION

An enterprise level of communication and computability opportunities has been opened up with the combination of private LTE and 5G network with a hybrid cloud computing platform. The architecture is offering the hitherto unseen benefits of scalability, performance, and flexibility, and it is a crucial enabler of digital change in industries. But increased security benefits of technologies also bring a broader and more complicated space that needs such an approach as proactive and multilayered security.

As this review has described, 5G and LTE hybrid private security cannot be achieved by an extension of the traditional telecommunications security methodology into the cloud. Rather, it needs a purposefully constructed design that assimilates the safety qualities of cloud-native constructs, zero-trust design, and contemporary containerized conveyors in software delivery. Attacks on these deployments include both API-level attacks and lateral movement, as well as supply chain attacks and insufficient protection of data traffic at rest, all of which require specialized mitigation strategies addressing both distributed and dynamic aspects of hybrid deployments.

The most important architectural capabilities should consist of strong identity and access management fueled by zero trust architecture, micro segmentation of network domains, encrypted communications within the control as well as user planes, and well-controlled secrets and credentials. At the same time, observability and continuous compliance enforcement are necessary in order to sustain visibility of runtime security posture and to enforce compliance with the regulatory requirements. Additional resiliency is achieved on the infrastructure with the implementation of intrusion detection, anomaly monitoring, and integration of threat intelligence. The security of containers and the supply chain deserves specific consideration, as telecom software is becoming more and more modular and dependent on third parties. The best non-negotiable practices of securing the 5G software lifecycle include hardening of runtime environments, container image security, and/or software provenance validation through signed artifacts and SBOMs.

Finally, the safe functioning of the hybrid cloud structure with the use of private LTE and 5G heavily depends not only on technical solutions but also on control, policy, and a proper comprehension of the shared responsibility model as the model of cloud services. Organizations need to derive in-house knowledge or build partnerships with vendors that offer specialization to constantly optimize their security defense and keep abreast with the ever-changing threats. Previously, Lupu covered components of the pathway towards that recognition and set the course of future accomplishments by embracing academic credentials and practical architectural recommendations. This review builds upon these values by providing a baseline framework that can be absorbed and extended by institutions playing that strategy by using secure and compliant private LTE and 5G networks in a hybrid cloud context. The potential of future studies may lie in further building on these bases and considering the incorporation of artificial intelligence into automated threat detection and policy enforcement, or the study of quantum-safe encryption schemes that can be used by future 5G and beyond security implementations.

REFERENCES

[1] M. Kandias, N. Virvilis, and D. Gritzalis, "The insider threat in cloud computing," in Proc. Int. Workshop Critical Inf. Infrastructures Security, Berlin, Heidelberg: Springer, Sept. 2011, pp. 93–103.
[2] N. G. M. N. Alliance, Service-based architecture in 5G: Case study and deployment recommendations, 2019.
[3] T. Senevirathna, V. H. La, S. Marchal, B. Siniarski, M. Liyanage, and S. Wang, "A survey on XAI for 5G and beyond security: Technical aspects, challenges and research directions," IEEE Commun. Surveys Tuts., 2024.
[4] P. Mudgal, A Data-Centric Framework for Implementing AI in Smart Manufacturing, 2025.
[5] E. K. K. Edris, M. Aiash, and J. K. K. Loo, "The case for federated identity management in 5G communications," in Proc. 5th Int. Conf. Fog Mobile Edge Comput. (FMEC), Apr. 2020, pp. 120–127.
[6] H. A. Kholidy, K. Disen, A. Karam, E. Benkhelifa, M. A. Rahman, A. U. Rahman, and R. Jaziri, "Secure the 5G and beyond networks with zero trust and access control systems for cloud native architectures," in Proc. 20th ACS/IEEE Int. Conf. Comput. Syst. Appl. (AICCSA), Dec. 2023, pp. 1–8.
[7] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges," Comput. Netw., vol. 167, p. 106984, 2020.
[8] L. Nkenyereye, L. Nkenyereye, and J. W. Jang, "Convergence of software-defined vehicular cloud and 5G enabling technologies: A survey," Electronics, vol. 12, no. 9, p. 2066, 2023.
[9] A. M. Sheikh, M. R. Islam, M. H. Habaebi, S. A. Zabidi, A. R. Bin Najeeb, and A. Kabbani, "A Survey on Edge Computing (EC) Security Challenges: Classification, Threats, and Mitigation Strategies," Future Internet, vol. 17, no. 4, p. 175, 2025.
[10] P. Somasundaram, "Unified Secret Management Across Cloud Platforms: A Strategy for Secure Credential Storage and Access," Int. J. Comput. Eng. Technol., vol. 15, pp. 5–12, 2024.
[11] I. Al Khatib, A. Shamayleh, and M. Ndiaye, "Healthcare and the internet of medical things: Applications, trends, key challenges, and proposed resolutions," Informatics, vol. 11, no. 3, p. 47, July 2024.
[12] S. Satija, C. Ye, R. Kosgi, A. Jain, R. Kankaria, Y. Chen, et al., "Cloudscape: A Study of Storage Services in Modern Cloud Architectures," in Proc. 23rd USENIX Conf. File Storage Technol. (FAST 25), 2025, pp. 103–121.
[13] S. Paul, T. Keluskar, and M. Vutukuru, "A Scalable and Fault-Tolerant 5G Core on Kubernetes," in Proc. 17th Int. Conf. Commun. Syst. Netw. (COMSNETS), Jan. 2025, pp. 658–666.
[14] T. Adewale, API-Driven Microservices for Seamless Integration Across Global Supply Networks, 2025.
[15] A. Klein, F. Ishikawa, and S. Honiden, "Towards network-aware service composition in the cloud," in Proc. 21st Int. Conf. World Wide Web, Apr. 2012, pp. 959–968.