Shielding the Cloud: Security in Platform Services Demystified

Topic 1: Introduction

Hello, everyone. Welcome to the ACL Digital Cloud Native Platform Services Podcast Show. I'm Sagar Nangare, your host for the show and a member of the Marketing Strategy Team at ACL Digital. Today's podcast focuses on Kubernetes-based cloud-native platform services. In this episode, we will explore how we assist organizations in accelerating product development by leveraging digital technologies with confidential computing. Additionally, we'll also delve into using HSM-based secure mTLS communication between 5G workloads.

For this discussion, we have Suresh Galam, an expert with over 20 years of experience in the Telecom & Networking Domain, serving as a Consultant and Architect. He has extensive experience working with Tier-1 Telecom service providers and leading global network OEM vendors. Let's hear from Suresh Galam and gain insights into his perspectives on Platform Services, Confidential Computing, and their future.

Hi Suresh, thanks for joining us on the ACL Digital Cloud Native Platform Services Podcast Show. I'd like you to introduce yourself to our audience here.

I'm Suresh Galam, Director of R&D Engineering Services at ACL Digital. I have over 20 years of experience in Product Transformation and Strategy, Collaboration, Digital Transformation, Technology, and End-to-End Delivery. I've collaborated with almost all major telecom service providers, including Cisco, Juniper, Ericsson, Microsoft, Intel, Verizon, T-Mobile, and Comcast. I'm passionate about Networking, SDN/NFV, SDWAN, 5G, Cloud, and Open-Source technologies.

Thanks, Suresh, for the introduction. You have spent almost two decades in the Telecom & Networking industry, and we have witnessed the transition of the communication industry from voice to SMS to data access to video calls, and now a new era in the way enterprises operate. How do you believe this entire journey has changed us?

Our lives are gradually becoming increasingly reliant on connectivity. We are already entering a fascinating phase of our times. It is the best time for the transformation that I'm witnessing all around us. One thing is sure: the amount and maturity of dialogues this time, with the advent of 5G, are unlike before. Whether a 5G wave or a potential 6G wave, the focus is discussing business value—how do we create business value? What is the business intent behind any transformation we embrace onto the network?

The pandemic has shown us that we can now live largely Connected without meeting physically. This will change how enterprises carry out their business, with online customers, employees working from home, and virtual and physical worlds becoming closely connected.

Topic 2: Platform Solution

The topic of this podcast is ACL Digital Cloud Native Platform Solution. What do you mean by Cloud native solution, can you explain it to us?

You started on the right note by mentioning a term called **Cloud-native**. But before we delve into that, it's essential to understand that two fundamental transformations are occurring, and I'll use the word "**Network Disaggregation**." That's what the entire concept of the cloud is based on.

Cloud-native is all about workloads, network functions, and disaggregation. It involves taking a workload, taking software, and applying it to any part of the network—whether it's radio, routing, the core of the network, or operations and assurance. With cloud-native principles, what we are observing is the disaggregation of network functions and workloads into smaller chunks, which we commonly refer to as **Microservices**.

Each one is independently capable of scaling, handling each of these functionalities independently, allowing us to embrace the maximum concept of reuse. So, you know, this whole notion of when we talk about 5G, and when we talk about the cloud, these extrapolations to cloud-native then become a norm. Keep in mind, we're talking about network disaggregation as well as network function disaggregation when we discuss the telco world.

In preparation for today's podcast, you sent over a couple of your collaterals, and I read through them. I pulled out a couple of data points that I found fascinating. What are the security concerns associated with moving workloads to the cloud?

Since the COVID-19 pandemic began, privacy and security have been at the forefront of many technologists' minds.

The COVID-19 pandemic saw a colossal interest in Confidential Computing, with millions of employees working from home and companies raising various issues related to securing data in transit, at rest, and while being processed.

Confidential computing has gained importance and popularity recently as enterprises grapple with security concerns associated with moving workloads to the cloud.

The reason for a confidential computing-based approach is that "**data-in-use**" must be protected from malicious insiders, hackers, and third parties. Cloud providers offer robust data protection features that enable customers to encrypt data without making any code changes to their applications or compromising performance.

Confidential computing has the potential to be a game-changer in cloud security, where the landscape of tools is rapidly evolving, providing businesses and end-users with the opportunity to protect data when it is most exposed during processing.

It's more challenging when running in the cloud because you don't own the hardware. You're using somebody else's hardware—Amazon's hardware or Google's hardware. So, you must rely on them to inform you whether that's there. How many people are currently asking for that? I would guess it's probably a small number.

One of the core principles behind confidential computing is **Zero Trust Security**, which helps customers verify that they are running on **trusted hardware**.

How do you see specific users or industries embracing the concept of confidential computing to address use cases across various sectors?

While multiple established solutions take care of the encapsulation, isolation, and data encryption during transmission or storage, there was previously a need for control over the data. At the same time, it was being processed in the memory. Confidential computing addresses this problem by focusing on protecting the data in use.

Data privacy has become extremely important, as many companies now rely on **public and hybrid cloud** services. Confidential computing is sure to be a critical component of a cybersecurity plan, where industries work together to accelerate the development of confidential computing solutions and provide the right environment to build **open-source tools**.

Individuals, companies, and organizations are becoming increasingly vulnerable to hacks, data breaches, and malicious attacks. Threats to data have intensified, making securing data a top business imperative.

While the benefits of cloud-native methodologies are substantial and play a pivotal role in industrial digitalization, they also present notable security challenges related to **secrets management**. These challenges include the proliferation of secrets, decentralization, the absence of centralized secrets control and revocation, limited insight into secrets usage across segments, and the requirement to support traditional IT systems and cloud-native environments.

In conjunction with confidential computing, **Vault** presents an exceptionally secure solution that empowers organizations to fortify their valuable data with hardware-based security. This approach minimizes the attack surface, thanks to the use of **Intel SGX** enclaves. Moreover, Vault's inclusion of a Public Key Infrastructure (PKI) engine bolsters its capabilities.

This versatile feature allows Vault to operate as an external Certificate Authority (CA), thereby facilitating the establishment of secure TLS/mTLS communication between microservices running within the cloud-native platform. This multi-faceted approach underscores Vault's significance in safeguarding information and fortifying the security framework.

This solution helps to solve the problem of exposing keys from vault while signing IoT secure boot.

What exactly is this ACL Digital Cloud-native platform solution that you are offering as part of this solution, and who will be potential customers?

ACL Digital offers a cutting-edge solution built on a Kubernetes-based cloud-native platform providing a plug-and-play architecture, allowing seamless integration of any applications into its ecosystem, and enabling the operation of workloads in public and private clouds.

In this ACL Digital Platform Solution, we have employed a cloud-agnostic approach, providing a stable, resilient, and scalable environment consistent across different infrastructures.

This lightweight and flexible platform ensures the software works the same no matter where it's used. Plus, we can run it on any container orchestration solution.

This platform delivers a set of critical Kubernetes services as managed cluster add-ons. ACL Digital manages each add-on's lifecycle and configuration. We have successfully conducted a Proof of Concept (PoC) by deploying open 5G core network functions as workloads and effectively managing them.

Features:

Seamless Integration

- Plug-and-play architecture for easy application integration
- Operate workloads in public and private clouds as desired

Wide Ecosystem Integration

Incorporates major Kubernetes tools like Cluster Management, Service Mesh, Confidential Computing, High Availability, GitOps, Zero Trust Access, Observability, Backup, and Restore

Multi-Cloud Support

Runs containerized workloads on any infrastructure, including Bare Metal, AWS, GCP, Azure, and Hybrid Clouds

Security Enhancements

Role Based Access Control (RBAC), AD/LDAP Integration, Multi-Cluster, Multi-Tenancy, Multi-Cloud, Cluster Scanning, Benchmarking, Service Mesh, Admission Controllers and much more - tailored to your security posture needs.

Managed Cluster Add-ons

ACL Digital takes care of the lifecycle and configuration of critical Kubernetes services.

Benefits:

- **Simplified Operations**: Manage complex cloud-native environments with ease.
- **DevOps Empowerment**: Efficiently deploy and monitor containerized workloads.
- **Scalability and Flexibility**: Seamlessly adapt to diverse infrastructures.
- **Comprehensive Security**: Ensure data and infrastructure security for peace of mind.
- **Managed Services**: Focus on innovation while ACL Digital handles critical cluster add-ons.

Potential Customers: We can have any workloads deployed in this platform and can be able to solve the use cases related to 5G, MEC, AI/ML and IOT.

Topic 3: Proof of Concept (PoC)

In confidential computing, I understand that your team has conducted a Proof of Concept (PoC) in partnership with Intel and Casa Systems. Could you kindly provide additional insights into the collaborative effort, detailing the partnership dynamics, the particulars of the PoC, and the specific applications within the use case?

At **ACL Digital**, we partnered with Intel, and Casa Systems helped assemble a couple of tools along with **Casa Systems**' **5G core workloads**. The goal was to demonstrate how we can enhance the security of 5G Core deployment using **Intel SGX**.

We've worked with Intel for the past decade and have been early adopters of Intel hardware features, functioning as a system integration and solution partner.

Through our robust partner ecosystem, we aim to be a leading solution partner for 5G implementations. We provide technology solutions and consulting to ensure our customers succeed in adopting 5G technology.

ACL Digital, in **partnership** with **Intel Technologies**, has proven that we are the preferred choice for building SGX-based security quickly.

Intel SGX has been used to help enhance security within multiple use cases and applications.

Use cases:

Artificial Intelligence (AI)/Machine Learning (ML)
Protect your AI and ML workloads and applications while they are running.

Cloud Infrastructure
Confidentiality of customer applications and workloads in public cloud infrastructures.

Trusted Multi-Party Compute/Multi-Party Analytics
Enable multiple parties to collaborate on shared data while keeping sensitive data confidential.

Secure Key Management
Use enclaves to help protect cryptographic keys and provide HSM-like functionality.

Blockchain
Increase privacy and security for transaction processing, consensus, smart contracts, and key storage.

Network Function Virtualization
Establish trust for virtualized network functions.

While this Proof of Concept (POC) was initially targeted toward Communications Service Providers (CoSPs), one can apply it to any cloud-native platform that utilizes **a Service Mesh solution** for enhanced security.

Could you elaborate on Intel SGX and explain how it safeguards data while in use? Additionally, could you provide a brief overview highlighting the critical factors of the PoC solution?

In collaboration with Intel, we have showcased a commercial 5G control plane on OpenShift, utilizing Intel SGX enclaves to store the private key essential for service mesh communication securely.

While a **zero-trust approach** with Service Mesh addresses security concerns to a certain extent, vulnerabilities arise when the platform is compromised. These security issues are mitigated by using mTLS over trusted workload identities, ensuring the secure data **in-transit**.

However, as we transition to **edge**, **core**, and **far edge** environments, the conventional network perimeter dissolves, necessitating data protection at the level of individual network functions **while in use**.

This solution involves using an HSM, which stands for Hardware Security Module—a specialized "trusted" environment capable of performing various cryptographic operations, such as key management, key exchange, and encryption.

By employing this solution, we address the issue of storing keys in plain text. Additionally, it resolves the vulnerability associated with the envoy proxy, as private key generation and CSR request creation occur within the SGX enclave.

Intel SGX serves as the HSM in this context, securing the minor attack surface, specifically the private keys used for mTLS communication within the service mesh. The service mesh mechanism is enhanced to facilitate consistent and secure communication among various 5G functions, making it a crucial component protected by SGX.

Deploying 5G functions like AMF, SMF, and PCF involves communicating over 5G core service-based interfaces, which are mTLS-protected, ensuring a secure exchange of information.

In a service mesh like Istio, enabling mTLS can secure communication, but why do we need SGX?

While mTLS can be activated, the security of the entire service mesh relies on the confidentiality of the private key that signs the certificates used in communication. An intruder could decrypt, observe, and monitor the service mesh if compromised.

Upon examination of the current service mesh solution, it is revealed that the root CA keys are stored in a Kubernetes secret in a base64-encoded format, making them susceptible to easy decoding. This vulnerability opens the possibility of introducing malicious services into the cluster.

To fortify the security of the service mesh architecture, we need to render these keys inaccessible to both the infrastructure and the cluster administrator. With the **Intel SGX solution**, the keys and secrets are safeguarded.

The private key used for mTLS communication will differ even if the secrets are exported. Thus, we provide security for critical data protection "**at rest, in transit, and execution**."

This use case is crucial, and its applicability extends to other scenarios related to **Data Privacy, Edge Computing, and Analytics**.

Topic 4: Platform Use Cases

Earlier, you mentioned the managed cluster add-ons included in this platform solution. Could you elaborate on the distinctive features of each add-on?

This platform provides a suite of essential Kubernetes services through managed cluster add-ons.

Cluster Management: Manages the complete life cycle of Kubernetes clusters deployed in Edge, Private, and Hybrid clouds.

Confidential Computing: This add-on provides Intel SGX-based platform attestation and key provisioning specifically designed for Edge applications.

Zero Trust Access: Ensures secure workload identities with HSM-based zero-trust access. It includes support for SSO, strong authentication (OAUTH2), user management, and identity federation.

Automated Deployments: Utilizes Ansible playbook to automate Kubernetes cluster provisioning, allowing for automatic rollout and rollback of upgrades.

Secure Service Mesh: Offers an enhanced service mesh for HSM-based mTLS communication, featuring integration with SGX-based external CA and proven interoperability with commercial 5G stack.

High Availability: Implements horizontal and vertical resource scaling based on resource demands. Manages and monitors critical data protection through backup solutions, mitigating the risk of data loss or corruption.

Observability with AI/ML: Provides customized application-specific metrics and traces for 5G CNFs. Implements proactive alerting and monitoring using AI/ML to minimize application failures.

We've delved into various platform services, but are there other primary use cases we aim to address? Feel free to provide more details.

Indeed, there's an emerging array of use cases, likely varying across different verticals, as we've briefly touched upon in a couple of examples.

Here are some typical use cases we are working to solve:

- Utilizing SGX to safeguard cryptographic keys and serve as an HSM for various workloads.
- Gaining visibility and control over platform and application performance.
- Securing AI/ML workloads and applications by executing them within the SGX enclave.
- Establishing HSM-based secure mTLS communication between 5G workloads.
- Implementing customized observability for application-specific metrics and traces across diverse workloads.
- Employing HSM-based external CA, critical server, and attestation services to ensure secure communications over the Edge.
- Providing multi-cloud support for disaster recovery, enhancing resilience and availability.
- Facilitating application deployment across clusters in multi-cloud environments to prevent vendor lock-in.

Interesting, you've covered various use cases, and it's well known that many open-source and commercial platform solutions are available in the market. What, in your opinion, are the key differentiating factors of the ACL Digital cloud-native platform?

Great question. The primary differentiators, when compared to other solutions, include:

Custom Observability Integration: We offer the ability to integrate custom observability, allowing visualization of application-specific metrics for 5G or any other application/workload. Users can set their templates based on their needs and add the metrics they want to monitor.

Service Mesh Integration: Our platform seamlessly integrates with external CA or any other HSM-based CA.

- **Flexibility with Service Mesh Solutions**: For instance, if a customer prefers to use a different Service Mesh solution apart from Istio, such as Gloo Mesh/Kong Mesh, we can align with them and integrate the Intel SGX solution to cater to their specific use cases.

Expertise in Kubernetes Management: We possess the expertise to manage and maintain Kubernetes clusters, ecosystem tooling, and the platform infrastructure effectively, with or without SGX.

Custom Resource Definitions (CRDs): We provide our CRDs for easy deployment of specific functions, addressing usability issues efficiently.

Topic 5: Conclusion

Help us peek around the corner and share what's on your radar for the future of this area.

One aspect involves staying vigilant on the cutting edge of technology. Changes persist, whether on the connectivity front, in artificial intelligence analytics, or the evolving landscape of machines on the shop floor. We'll continue to monitor these developments closely.

However, how can we implement these technologies and integrate them with management innovations to enhance productivity genuinely? How effectively can we leverage competition to drive companies forward? These factors will significantly influence the events unfolding, especially as we navigate the challenges of recovering from the pandemic-related recession.

You just wrapped up a fantastic journey at FYUZ#23. Could you share your experiences and insights on FYUZ#23?

At the Telecom Infra Project's (TIP) annual event, Fyuz#2023, we had the privilege of attending and sponsoring this remarkable gathering. This event, set against an awe-inspiring backdrop, provided an opportunity to learn and network, marking a pivotal moment that reshaped our business.

The event served as a unique platform for discussions with experts, exchanging ideas, and exploring collaborative opportunities.

One of the most striking aspects of the event was the impressive turnout at our booth. Witnessing many professionals eager to connect and delve deeper into our products and services was heartening.

The highlight of our participation at #Fyuz 2023 was not limited to connecting with industry peers; it was about constructing a complete partnership ecosystem. Our focus on 5G, cybersecurity, OSS, BSS, automation/orchestration, and testing took a giant leap forward during this event. We firmly believe in the power of collaboration, and this year’s event was pivotal in cementing our partnerships.

Before #Fyuz 2023, we had already established connections with several key partners in these areas, but the event offered a unique opportunity to showcase these partnerships to our customers. In the dynamic world of 5G and open networking, collaboration is paramount, and this event helped us establish a solid foundation for future endeavors. We realized that the event catalyzed the creation of new opportunities in the 5G and open networking space, and we are thrilled about the possibilities.

It was a resounding success for our company, opening new doors with prospects in the European region. The power of collective intelligence, shared experiences, and mutual support was evident throughout the event.

We thank all the attendees who visited our booth, contributing their valuable insights. We also sincerely appreciate our SI/PS partners, whose support and active participation in our booth underscore their keen interest in prospects.

We eagerly anticipate our company's continued growth and development in the ever-evolving landscape of telecommunications and 5G technology, fueled by the incredible experience at FYUZ 2023.

Looking ahead, over the next year or two, what other opportunities do you foresee? Are there any best practices or recommendations you would suggest in the realm of hardened security, like what we've been discussing? Are there additional insights or advice you would like to share with our listeners?

In the next five years, confidential computing will become widely ubiquitous, but the present is the opportune time to initiate adoption. The required hardware and suitable environments are available through various CSPs and on-premises platforms.

By 2026, the Confidential Computing market is expected to reach a $54 billion market opportunity. Approximately 15% of heavily regulated organizations will embrace confidential computing technologies to amalgamate and enhance sensitive data crucial to multiparty computing applications while maintaining privacy.

Companies that provide the necessary tools and technology for confidential computing are poised for success and rapid growth. They are set to redefine how business and security are conducted across various sectors.

We are in an era of zero trust and must secure enterprise assets to unlock new business opportunities.

With hardware roots of trust, we can run our most sensitive workloads in secure enclaves—whether in the cloud, on-premises or at the edge. Confidential computing allows us to enhance privacy, establish more trusted systems, and continually generate data-driven insights. The collaboration of hardware innovation with accessible, consistent software equips us with the tools needed to shape the trusted future we desire.

The ACL Digital platform solution discussed here addresses the most pressing security challenges arising from the transition to 5G and cloud-native architectures. It ensures the security of the 5G Edge/Core and other telecom applications using confidential computing services in a multi-cloud environment.

At ACL Digital, we recognize the significance of being early adopters in Confidential Computing. We heavily invest in solutions, accelerators, and labs while working closely to expedite our customers' 5G security journey.

Thank you for listening. Stay tuned for our next episode.