ACL Digital
an ALTEN group company

Confidential Computing:

The Future of Cloud Computing Security

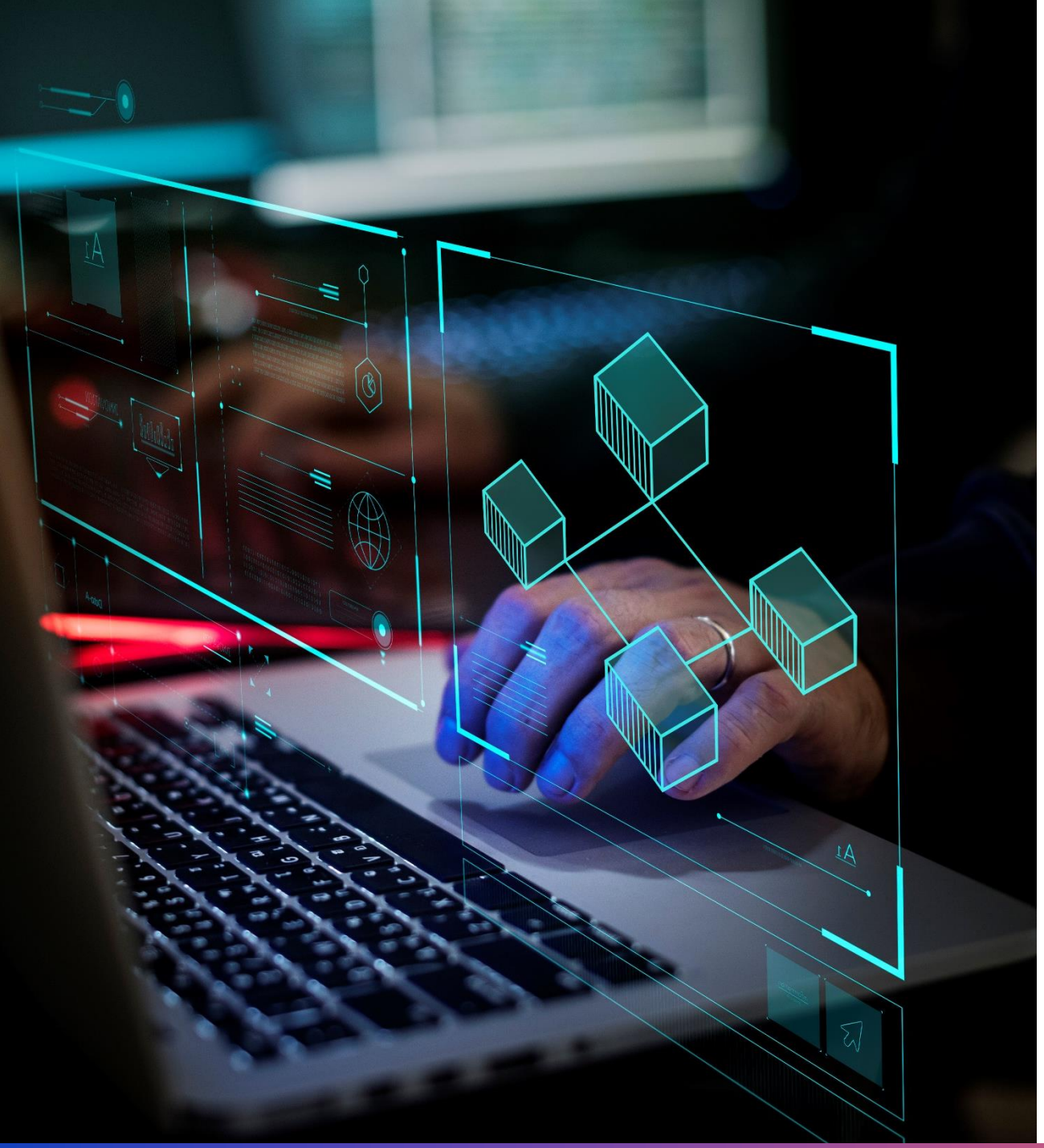


Table of Contents

What is Confidential Computing?

Confidential Computing has created a buzz in the industry with great promises to change the whole equation by encrypting **the 'data in use.'**

Confidential **Computing** has gained in importance. It has grown in popularity recently as enterprises struggled with security concerns associated with **moving workloads to the cloud.**

Confidential Computing is a generic industrial term that enterprises can leverage and exploit to **address security concerns** that sit on a foundation called **a root of trust,** based on a secured key **unique to each processor.**

The **Confidential Computing Consortium (CCC)** aims to define standards for using **Confidential Computing,** computing through open collaboration made up of software developers, hardware vendors, and cloud providers.

The Confidential Computing Consortium **(CCC)** was formed in 2019. It included members such as Facebook, Alibaba, IBM, Accenture, ANT Group, Arm, Google, Huawei, Intel, Microsoft, NVidia VMWare, Xilinx, Red Hat, and 30 others.

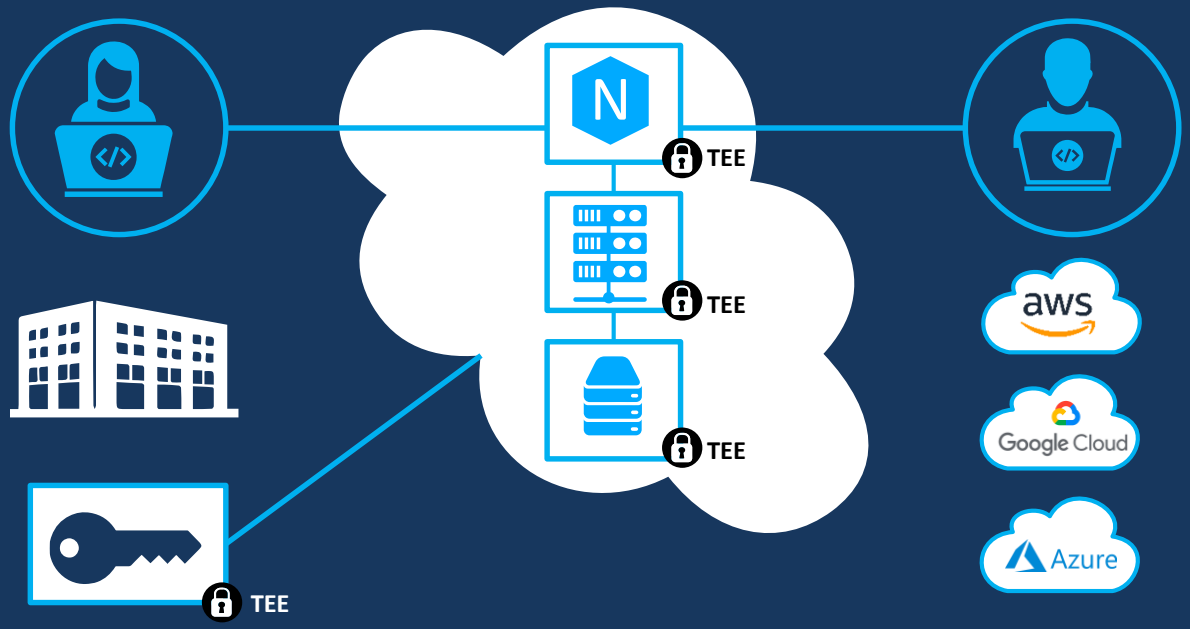
The Confidential Computing-based approach is because **"data in use"** must be protected from malicious insiders, hackers, and third parties. And cloud providers provide a complete circle of data protection features that allow customers to **encrypt data without making any code changes to their applications or compromising performance.**

Multiple established solutions will cover encapsulation, isolation, and data while being transmitted or stored. Still, there must **be control while the data is processed in the memory.** Confidential Computing **solves this problem by focusing on protecting the data in use.**

Confidential Computing has the potential to be a **game changer in cloud security,** where the landscape of tools is rapidly evolving and provides businesses and end-users with the opportunity to protect data when it is most exposed while being processed.

Data privacy has been paramount, as many companies nowadays rely on public and hybrid cloud services. Confidential Computing is a **critical part of a cybersecurity plan, where industries work together to hasten the development of Confidential Computing solutions and provide the right environment to build open-source tools.**

Why do we need Confidential Computing



Trusted Execution Environment (TEE)

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

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

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

The foundation that all the other layers of trust are laid upon in a **trust hierarchy is the hardware itself,** such as the operating system, BIOS, firewalls, physical security, security software, and ultimately organizational and contractual measures.

The basis for confidential cloud computing is the **hardware-based root of trust.**

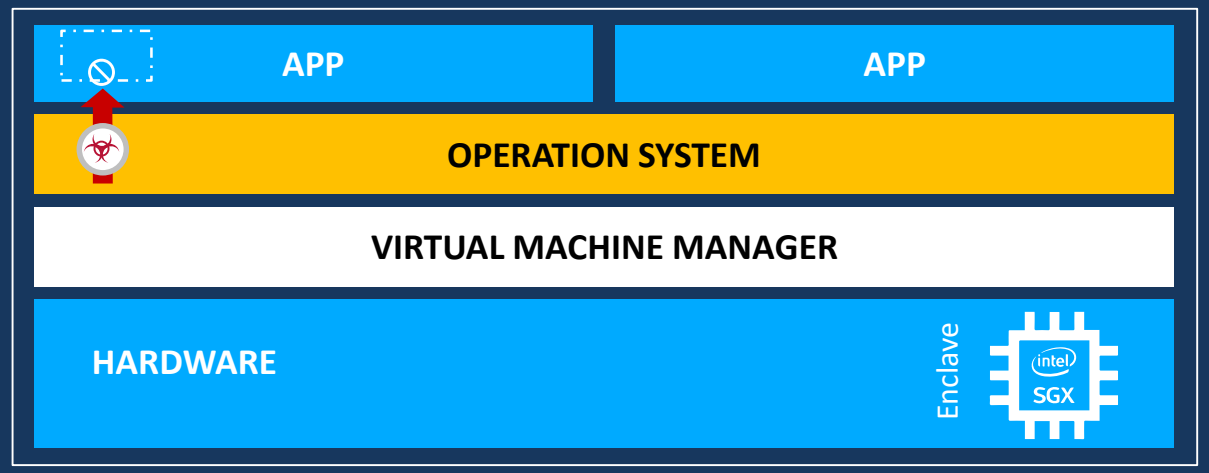
The main element of confidential computing is the **Trusted Execution Environment** (TEE), which protects data and code within **hardware-based secure enclaves,** and applications can be securely executed irrespective of the rest of the system.

A TEE is a secure area within a central processor that runs an isolated environment parallel to the primary operating system. This hardware-level isolation ensures that data and code uploaded cannot be tampered with by malicious agents.

TEE is a memory black box containing data and code, which are enabled through hardware-based isolation technologies like Intel SGX or ARM Trust Zone or through software-based options like VSM (Microsoft's Virtual Secure Mode) implemented by Hyper-V.

Several cloud service providers offer TEE-based Confidential Computing today, and there are multiple choices in deploying TEE-based solutions with different levels of security provided by HW/SW/CSP Vendors.

Intel SGX is the most conspicuous enclave implementation to date, where the contents of an enclave even remain encrypted in memory at runtime.



Enclaves have 4 defining security properties:

- Isolation
- Run time memory encryption
- Sealing
- Remote Attestation

Confidential Computing powered by Intel SGX will continue to play an increasingly important role in providing organizations with robust controls to help safeguard sensitive intellectual property and workload data, wherever that data resides—at rest, in flight, and during processing.

What business use cases can organizations solve with confidential computing today?

Newer technologies with business transformation and market growth drive a growing number of innovative use cases, where organizations can choose use cases that best meet their needs.

Common Use Cases for Confidential Computing

1. Cloud Transformation

Reap the benefits of cloud economics without the threat of attackers or insider eavesdropping

2. Secrets Protection

Run your key management system in a secure enclave to achieve HSM-type protection

3. Sensitive Data privacy

Guarantee trust for PII and other susceptible data with hardware-rooted zero-trust defense

4. Multi-party computation

Allow multiple parties to share code or information without leaking their private data

5. Compliance

Simplify and ensure compliance with a growing number of stringent security regulations

Forward-Thinking Confidential Computing Use Cases

Companies in specific industries, like government, financial services, healthcare, and life sciences, must store particular data types. And if that data is generated by confidential computing, it doesn't need to be stored and will therefore be less vulnerable to hackers.

1

Emerging

- IOT
- Block Chain
- Key Protection
- Secure Containers
- NFV
- HSM

2

Financial Services

- Fraud detection and prevention
- KYC
- Credit Risk Assessment
- Anit-money laundering
- Digital currencies

3

Health care, life sciences

- Drug discovery
- Clinical Trials
- Genomics
- Electronic Health Record

4

Government

- Anti-corruption
- Cyber-crime prevention
- Digital identity

ACL Digital, Intel, Casa Systems Proof Point for Secure Cloud Native 5G Control Plane

ACL Digital as a solution integration partner with Intel and Casa Systems, demonstrated how we could harden security to 5G Core deployment using Intel SGX.

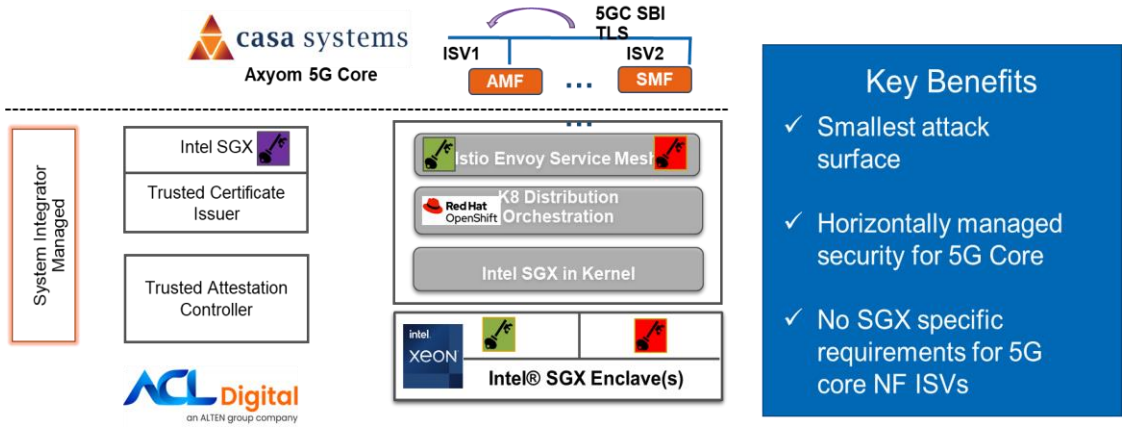


Figure 1: Secured 5G Core signaling using Intel SGX

- **ACL Digital, a system integrator partner of Intel,** has the expertise to provide secure cloud-native infrastructure solutions leveraging Intel SGX features for confidential computing in telecom applications.
- As Intel SGX focuses on securing the minor attack surface, the focus ison security mTLS communication between different microservices in the 5G control plane stack.
- The solution consists tools, including Key Management Reference Application, enhanced Secure Service Mesh with Intel SGX support, Trusted Certificate Issuer and Trusted Attestation Services on top of Red Hat OpenShift Platform and container bare-metal reference platform.
- With these tools, critical 5G Core and Edge and other telecom applications that run on network cloud are secured with hardware-based security.

```
→  kubecon-tcs git:(main) ✗ kubectl get secrets -n istio-system istio-ca-secret -o jsonpath='{.data.ca-key\.pem}' | base64 -d
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAnDXiwgOGuuv2SFXYZMuiqXl4eVP/jOBFgGDn/2/2G1qJKRWE
LQkz8gz+zRs3zJ+dKT2S/SvkRUrlKF7Z2ZkY70EJs8eOEDWXRVc6eONtHn9xfZhG
                    Removed for Privacy
8qFA6A8UNjZajKoW/GjLRAWCUBda7MIBgO8UQV0uhSZEuGyJRSs5vcowuyKs7VYN
eADL/MqM0HVPfOJffKYOUOORV64wQNXtL0kMbCcvQWHfV9y/qNsA07EPVjZNM1I8
```

Figure 2: CA Private Key in kubernetes secret sored in clear text format

```
→  kubecon-tcs git:(main) ✗ k get secrets -n tcs-issuer sgx-signer-secret -o jsonpath='{.data.tls\.key}' | base64 -d
→  kubecon-tcs git:(main) ✗
```

Figure 3: CA Private is not visible in kubernetes secret as it is stored in SGX enclave

- This solution solves the issue of having clear keys, e.g., from Kubernetes secret for service mesh (Figure 2). Trusted Certificate Issuer, a cert-manager-based external certificate issuer, uses Intel SGX to store CA private key and performs certificate signing inside the enclave using the Intel CryptoAPI toolkit. Since the CA key is stored in the SGX enclave, it won't appear in the Kubernetes secret (Figure 3). It is impossible to decrypt data in enclaves, even with privileged access. Hence, it makes the solution more secure when running on public cloud or edge locations.
- Third parties can perform remote/local attestation using a trusted attestation service to ensure they run on the trusted platform using Intel provisioning service before running the applications.
- **ACL Digital, in partnership with Intel Technologies** is well-poised to understand and address customer 5GC security requirements and is the preferred choice for building SGX-based security within a short timeline.

Gramine

Gramine plays a critical role in the ongoing development of Confidential Computing.

CCC's first production-ready TEE is called Gramine 1.0

Gramine was initially called Graphene, where the programmers designed to solve the problem of applications built for one system that would only run on others with extensive modifications.

By bringing unmodified applications into Confidential Computing with Intel SGX, Gramine follows the paradigm **"lift and shift".**

By using **Gramine Shielded Containers (GSC) tool,** we can automatically **convert Docker images to Gramine images** which can be deployed via Kubernetes for confidential containers and microservices.

We at ACL Digital are exploring the local and remote attestation support which Gramine provides and the GSC tool (Gramine Shielded Containers).

Conclusion

Confidential Computing is poised to become one of the **hottest trends in cybersecurity** in the next few years, with a compound annual growth rate of up to **95.6% between 2021 and 2026.**

Confidential Computing is still an emerging field. The community of developers and practitioners is growing, and there are range of online resources and events for beginners and experts.

The Confidential Computing Summit is crucial to help accelerate, educate, and expose organizational initiatives, including unveiling solutions and the latest innovation across the ecosystem of solutions from cloud providers and software/hardware platform providers.

The Confidential Computing Summit represents a unique opportunity to meet experts who will bring together a community of innovators, security experts, data scientists, data privacy experts, and researchers across industries, including but not limited to financial services, insurance, healthcare, manufacturing, and more.

We see a paradigm shift with confidential computing as it is positioned to become the de facto technology **for future computational security**, accelerating the widespread adoption and ushering in a new era of how we secure the Cloud.

With the **"go faster"** push to cloud and DevOps, organizations need a new approach in today's environment to find valuable ways to put their data to work, where rising security concerns and high-visibility attacks collide.

Confidential computing will be widely ubiquitous in the next five years, but now is the time to begin adoption. Required hardware and suitable environments are available via various CSPs and on-premises platforms.

By 2026, the Confidential Computing market will reach a $54B market opportunity, with 15% of heavily regulated organizations will adopt confidential computing technologies to combine and enrich sensitive data critical to multiparty computing applications while preserving privacy.

The companies that provide the necessary tools and technology for confidential computing are poised to succeed and thrive, revolutionizing business operations and security practices across diverse sectors.

We are in a world of zero trust and must act accordingly to secure enterprise assets that will open new business opportunities.

The ACL Digital solution described in this white paper provides an approach to solve the most persuasive security challenges resulting from the shift to 5G and cloud-native architectures and to secure the 5G Edge/Core and other telecom applications using confidential computing services in a multi-cloud environment.

Suresh Galam
Networking & Telecom Consultant and Architect

Nitinkumar Ambulgekar
Senior Technical Lead

References

https://www.intel.ca/content/www/ca/en/architecture-and-technology/software-guard-extensions/hardware-security-sgx-infographic.html

Secure the Future of 5G Networks with Zero Trust for Cloud Native Architectures | Intel® Network Builders

Securing Workloads on OpenShift Container Platform (intel.com)

https://medium.com/@rahul_grover/deep-dive-in-confidential-computing-a227abbba8e1

https://www.globallogic.com/wp-content/uploads/2021/04/Confidential-Computing.pdf

https://www.snia.org/sites/default/files/CSI/Confidential-Compute-Protecting-Data-In-Use-Final.pdf

https://www.alibabacloud.com/knowledge/hot/privacy-security-and-confidential-computing