Confidential Computing: Moving the needle on Cloud security

Amit Gupta
CEO & founder at Rapyder Cloud Solution

Cloud computing is omnipresent. Literally every organization have adopted cloud in one form or the other. A significant part of enterprise workloads is already on cloud. However, there is another side to the cloud story. While organizations are clearly aware about the broader benefits of cloud, security puts a spoke in the wheel. Many organizations still shy away from moving more core functions and sensitive data to cloud purely for security and privacy concerns.

Lack of skilled resources internally, legacy approach, misconfigurations of the cloud platform –all of this contribute to the problem. A recent survey indicates that over 75 percent of enterprise security experts are overly concerned about public cloud security.

Enterprises are increasing their cloud spend, moving more critical applications and optimizing existing investments on cloud as the global pandemic compel them to cope with the new market realities. It's all the more critical for leading cloud providers to effectively fill the existing gap in cloud security to help enterprises make this transition smoother and to unlock the next phase of cloud adoption.

Fortunately, the answer might be around the corner—in the form of a new hardware-based security approach dubbed 'confidential computing'.

What is confidential computing?

Data security traditionally has been built around three fundamental approaches to prevent unauthorised access –protecting data at rest, in transit and in use. Security strategies so far have been predominantly centred around the first two states of data. As a result, at-rest and in-transition encryption standards are already well evolved. Securing 'data in use' however has been a challenge. Encryption as a method is largely inadequate in this area as applications need access to data in unencrypted form.

A number of data-intensive and regulated industries (eg: finserv, insurance, healthcare, media & entertainment etc.) have significantly higher data protection requirements in terms of safeguarding customers' PII or intellectual property assets of the organization. In many of these use cases, there is an increasing need to secure 'data in use'. For example, healthcare dashboards accessing sensitive patient data to arrive at treatment decisions. Encryption is not a possible option in this case and access to sensitive data is inevitable.

Confidential computing promises to change the whole equation by encrypting the 'data in use'. Through this emerging approach, data can be encrypted while its running in memory without exposing it to the rest of the system and even to privileged users. Data is further decrypted within the CPU using embedded hardware keys, which the cloud provider has no control over. Confidential computing is typically built on hardware-based Trusted Execution Environments (TEE), also known as Enclaves.

AWS' Nitro Enclave, for example, provides CPU and memory isolation for EC2 instances by offering an isolated and highly constrained environment to host security-critical applications.

Consider it as virtual machines that have no persistent storage, operator or administrator access. Nitro Enclave uses Cryptographic attestation techniques, which allows customers to verify that only authorized code is running in their enclave. AWS' aim is to enable customers to easily move sensitive workloads to the cloud while protecting their resources more efficiently.

What lies ahead?

Confidential computing comes with great promises and is touted to be a game changer for the cloud computing industry. Its benefits go beyond the realms of security. In future, confidential computing has the power to promote collaboration among competitors (for example, companies working together on genomic research on cloud platforms) as it assures complete protection and privacy of sensitive data.

Confidential computing also has the potential to enable more innovative machine learning, microservices and Blockchain use cases among enterprises. It's considered to be the only standard that can potentially secure Blockchain transactions in which sensitive data is transmitted across the decentralized network. It can also address the security concerns around moving mission-critical workloads to a container or Kubernetes environments.

That said, the technology is still at nascent stage. Gartner anticipates a five- to 10-year wait before confidential computing is in regular use. But once it's there, it has the potential to truly redefine cloud security.