Performance Evaluation of Confidential Containers in the Edge-Cloud Computing Continuum

Itsuki NAKAI
Toyohashi University of Technology
i2tree@perf.cs.tut.ac.jp

Takaaki FUKAI
National Institute of Advanced Industrial Science and Technology
takaaki.fukai@aist.go.jp

Takahiro HIROFUCHI
National Institute of Advanced Industrial Science and Technology
t.hirofuchi@aist.go.jp

Yukinori SATO
Toyohashi University of Technology
yukinori@cs.tut.ac.jp

There is growing interest in Edge-Cloud computing continuum, which is composed of massive IoT devices and large clusters of servers running at Multi-access Edge Computing (MEC) at network edge, regional data centers, and flagship data centers. Services utilizing Edge-Cloud computing continuum perform multi-tiered processing in response to user requests. Especially, offloading tasks from edge devices to MEC is an emerging approach that could not be seen in traditional cloud environment. In this computing model, it is expected that MEC will execute processes with high security requirements and low latency. Therefore, when utilizing MEC, it is necessary to achieve both low latency and security.

Some of the MEC services, such as AWS Wavelength, provide computing resources in a multi-tenancy model. In multi-tenant services, computer resources such as CPU and memory are shared among multiple users. Therefore, it is essential to protect the services against attacks from service vendors and other users. Proper isolation of shared resources and access control are required to ensure security and integrity.

One technology for achieving advanced isolation to prepare against attacks is confidential computing, which enhances security by encrypting data in the phase of processing in CPU. Confidential computing is a technology that uses processor-level hardware support to encrypt the memory of a virtual machine, which makes impossible for the hypervisor or any host software to access the memory contents in Confidential VM (CVM)[1]. As examples of technologies enabling CVM, AMD provides Secure Encrypted Virtualization (SEV) and SEV-Secure Nested Paging (SEV-SNP). SEV and SEV-SNP protect virtual machine memory, thereby preventing attacks such as data theft from VMs or containers by other users or service vendors. In this presentation, VM-based containers using these technologies are referred to as confidential containers such as Kata container.

While security is enhanced in CVM, there are some concerns about potential performance impacts. Further, CVM are primarily intended for cloud environments, and detailed analyses of their impact on processing latency against MEC in the Edge-Cloud computing continuum have not been reported. Therefore, this presentation aims to evaluate the effects of confidential container with CVM on processing latency at the MEC in a multi-tenant Edge-Cloud computing continuum. Specifically, we investigate the impact of memory protection mechanisms on processing latency.

We evaluate the service responsiveness of microservices deployed using confidential container environments in terms of HTTP communication. To measure the impact, we utilized DeathStarBench, a benchmarking tool that mimics microservices. For measuring latency in HTTP communication, we use a tool called wrk. In our measurement environment, we assume DeathStarBench was deployed to servers at MEC, and wrk was executed on edge devices. For deploying DeathStarBench, we used Kubernetes as the container orchestration tool and Kata Containers, which support technologies like SEV and SEV-SNP, for confidential containers. To our best knowledge, this is the first time that the actual end-to-end latency performance in the above environment is evaluated.

From the evaluation, we observed an increase in latency for HTTP communication with microservices when using SEV and SEV-SNP. Using SEV-SNP, we observed performance degradation ranging from 30% to 60%. These results are preliminary, and additional measurements and validation are planned before presentation.

ACKNOWLEDGMENTS

This presentation is based on results obtained from the project, "Research and Development Project of the Enhanced infrastructures for Post-5G Information and Communication Systems" (JPNP20017), commissioned by the New Energy and Industrial Technology Development Organization (NEDO). This work was supported by JST, CREST Grant Number JPMJCR22M3, Japan.

REFERENCES

[1] Mingjie Yan and Kartik Gopalan. 2023. Performance Overheads of Confidential Virtual Machines. In *2023 31st MASCOTS*. p1–8.