A Fast and Secure Key-Value Service Using Hardware Enclaves

Ines Messadi und Rüdiger Kapitza, TU Braunschweig

Trusted execution as offered by Intel Software Guard Extensions(SGX) enables confidentiality and integrity for cloud-hosted services. While in principle all kinds of workloads can be secured using trusted execution, key-value stores have gained special attention as these services are an essential building block of most complex cloud deployments.

So far the main design challenge has been to address current performance limitations of SGX.

In addition, we identify the integration of SGX-guarded workloads with recent network technology, especially Remote Direct Memory Access(RDMA) as an upcoming requirement. RDMA allows fast direct access to remote memory at high bandwidth. However, SGX protected memory cannot be directly accessed over the network. Furthermore, due to the more powerful network, secured services might likely be CPU-bound as a result of the necessary cryptographic operations. In the following, we present a new key-value store architecture that utilizes trusted execution to offer confidentiality and integrity, while basing on RDMA for low latency and high bandwidth communication. To prevent a server-side CPU bottleneck clients pre-compute cryptographic operations when possible while data movement in and out of the trusted execution environment has been reduced to the bare minimum.