Confidential Virtual Machine Provisioning in Cloud Environment

J. Deng
Alibaba Group
dengjuan.deng@alibaba-inc.com
Cloud Computing: Benefits together with Concerns

**Benefits:**
- Easy scalability and flexibility
- Better security
- Disaster recovery
- Reduced cost
- ...

**Concerns:**
- Privilege Admin of infrastructure
- Leakage of sensitive and confidential data
- Malicious tampering
- ...

![Diagram showing cloud computing infrastructure with layers including apps, bin/libs, guest OS, hypervisor, container engine, OS, and infrastructure.]
Hardware-Based Security Technology

Memory Encryption
- Protection of confidential and sensitive data

Secure Boot/Trusted Boot Remote Attestation
- Protection of boot process...

Trusted Execution Environment
- Protection of app and confidential and sensitive data

Confidential Virtual Machines
- Malicious tampering
- Protection of virtual machine
The protocols for Confidential Virtual Machine Provisioning in the Cloud environment is missing.
Provisioning of Confidential Virtual Machine in Cloud Environment

Abstract

Confidential virtual machine (CVM) in the cloud environment is a use case of confidential computing where VM confidentiality is enabled by hardware. A cloud user’s CVM is isolated from the hypervisor provided by its cloud service provider, meaning the cloud service provider cannot access the workload and data in the CVM. This is used in the scenario where a cloud user intends to protect its sensitive workload and data from cloud service provider while at the same time desires to utilize the advantages of cloud technology. This document specifies the CVM provisioning in cloud environment including the provisioning process and protocol, and the security requirements.
Provisioning of Confidential Virtual Machine in Cloud Environment

Table of Contents

1. Introduction
2. CVM Provisioning in Cloud
   2.1. Overview
   2.2. Enabling Confidential Computing Feature for CVM
   2.3. Creating CVM Instance
   2.4. Verifying CVM
   2.5. Reviewing Measures
   2.6. Retrieving Remote Attestation Report
   2.7. Migrating a live CVM
   2.8. Message Definitions
3. IANA Considerations
4. Security Considerations

Author's Address