Abstract

Out of the newly emerging and promising technologies is Cloud computing and Infrastructure-as-a-Service (IaaS) which can also be claimed as something the adoption of which is hampered by data security concerns. Simultaneously, Trusted Computing (TC) is also getting its burning interest as security mechanism for IaaS. This paper presents a protocol and addresses the issue of the lack of an implementable mechanism with a proportion that it will ensure the launch of a virtual machine (VM) instance on a trusted remote compute host. A trusted launch protocol for VM instances and images in public IaaS environments has been designed for Relying on Trusted Platform Module operations such as binding and sealing to provide integrity guarantees for clients that require a trusted VM launch. This paper also presents an evidence-of-concept implementation of the protocol that is solely based on Open Stack, an open-source IaaS platform. The proposed results would provide a strong stand for the use of TC mechanisms within IaaS platforms. It will also open the path for a bigger applicability of TC to IaaS security. This technology empowers the companies to take the costs down by outsourcing computations which are on-burning demand. Nevertheless, clients of cloud
computing services at present do not have any means by which they can verify the confidentiality and integrity of their data and computation. This problem is addressed to propose the design of a trusted cloud computing platform (TCCP). To impart a closed box execution environment, TCCP empowers Infrastructure as a Service (IaaS) providers such as Open stack IaaS platform. It also ensures the confidential execution of guest virtual machines. Besides, it also lets the users confirm to the IaaS provider and determine if the service is secure before they launch their virtual machines.

References


**Index Terms**

Computer Science  
Distributed Computing

**Keywords**

IaaS, security, trusted computing, trusted virtual machine launch, OpenStack, Cloud Computing, Scalability, Infrastructure, confidentiality, integrity, trusted cloud computing platform.