Cloud interoperability could alleviate the concern that users could become hopelessly dependent on a

single cloud service provider, the so-called vendor lock-in discussed in Section 3.5. It seems natural to

ask the question whether an Intercloud – a “cloud of clouds,” a federation of clouds that cooperate to

provide a better user experience – is technically and economically feasible. The Internet is a network

of networks; hence, it appears that an Intercloud seems plausible [47–49].

Closer scrutiny shows that the extension of the concept of interoperability from networks to clouds

is far from trivial. A network offers one high-level service, the transport of digital information from

a source, a host outside a network, to a destination, another host, or another network that can deliver

the information to its final destination. This transport of information through a network of networks is feasible because before the Internet was born, agreements on basic questions were reached: (a) how

to uniquely identify the source and the destination of the information; (b) how to navigate through a

maze of networks; and (c) how to actually transport the data between a source and a destination. The

three elements on which agreements were reached are, respectively, the IP address, the IP protocol, and

transport protocols such as TCP and UDP.

The situation is quite different in cloud computing. First, there are no standards for storage of

processing; second, the clouds we have seen so far are based on different delivery models: SaaS, PaaS,

and IaaS. Moreover, the set of services supported by each of these delivery models is not only large, it

is open; new services are offered every few months. For example, in October 2012 Amazon announced

a new service, the AWS GovCloud (US).

The question ofwhether cloud service providers (CSPs) are willing to cooperate to build an Intercloud

is open. Some CSPs may think that they have a competitive advantage due to the uniqueness of the added

value of their services. Thus, exposing how they store and process information may adversely affect

their business. Moreover, no CSP will be willing to change its internal operation, so a first question is

whether an Intercloud could be built under these conditions.

Following the concepts borrowed from the Internet, a federation of clouds that does not dictate the

internal organization or the structure of a cloud but only the means to achieve cloud interoperability

is feasible. Nevertheless, building such an infrastructure seems a formidable task. First, we need a set

of standards for interoperability covering items such as naming, addressing, identity, trust, presence,

messaging, multicast, and time. Indeed, we need common standards for identifying all the objects

involved as well as the means to transfer, store, and process information, and we also need a common

clock to measure the time between two events.

An Intercloud would then require the development of an ontology11 for cloud computing. Then

each cloud service provider would have to create a description of all resources and services using this

ontology. Due to the very large number of systems and services, the volume of information provided by

individual cloud service providers would be so large that a distributed database not unlike the Domain

Name Service (DNS) would have to be created and maintained. According to [47] this vast amount of

information would be stored in Intercloud root nodes, analogous to the root nodes of the DNS.

Each cloud would then require an interface, a so-called Intercloud exchange, to translate the common

language describing all objects and actions included in a request originating from another cloud in terms

of its internal objects and actions. To bemore precise, a request originated in one cloud would have to be

translated from the internal representation in that cloud to a common representation based on the shared

ontology and then, at the destination, it would be translated into an internal representation that can be

acted on by the destination cloud. This raises immediately the question of efficiency and performance.

This question cannot be fully answered now, since an Intercloud exists only on paper, but there is little

doubt that performance will be greatly affected.

Security is a major concern for cloud users, and an Intercloud could only create new threats. The

primary concern is that tasks will cross from one administrative domain to another and that sensitive

information about the tasks and users could be disclosed during this migration. A seamless migration

of tasks in an Intercloud requires a well-thought-out trust model.

The Public Key Infrastructure (PKI),12 an all-or-nothing trust model, is not adequate for an Intercloud,

where the trust must be nuanced. A nuanced model for handling digital certificates means that

one cloud acting on behalf of a user may grant access to another cloud to read data in storage, but not

to start new instances.

The solution advocated in [48] for trust management is based on dynamic trust indexes that can

change in time. The Intercloud roots play the role of Certificate Authority, whereas the Intercloud

exchanges determine the trust indexes between clouds.

Encryption must be used to protect the data in storage and in transit in the Intercloud. The OASIS13

Key Management Interoperability Protocol (KMIP)14 is proposed for key management.

In summary, the idea of an Intercloud opens up awide range of interesting research topics. The practicality

of the concepts can only be discussed after the standardization efforts underway at NIST bear fruit.