After reviewing cloud services provided by Amazon, Google, and Microsoft, we are in a better

position to understand the differences among SaaS, IaaS, and PaaS. There is no confusion about SaaS;

the service provider supplies both the hardware and the application software, and the user has direct

access to these services through aWeb interface and has no control over cloud resources. Typical examples

are Google with Gmail, Google Docs, Google Calendar, Google Groups, and Picasa and Microsoft

with the Online Services.

In the case of IaaS, the service provider supplies the hardware (servers, storage, networks) and

system software (operating systems, databases); in addition, the provider ensures system attributes such

as security, fault tolerance, and load balancing. The representative of IaaS is Amazon AWS.

PaaS provides only a platform, including the hardware and system software, such as operating systems

and databases; the service provider is responsible for system updates, patches, and software maintenance.

PaaS does not allow any user control of the operating system, security features, or the ability to install

applications. Typical examples are Google App Engine, Microsoft Azure, and Force.com, provided by

Salesforce.com.

The level of user control over the system in IaaS is different form PaaS. IaaS provides total control,

whereas PaaS typically provides no control. Consequently, IaaS incurs administration costs similar to

a traditional computing infrastructure, whereas the administrative costs are virtually zero for PaaS.

It is critical for a cloud user to carefully read the SLA and to understand the limitations of the

liability a cloud provider is willing to accept. In many instances the liabilities do not apply to damages

caused by a third party or to failures attributed either to the customer’s hardware and software or to

hardware and software from a third party.

The limits of responsibility between the cloud user and the cloud service provider are different for

the three service-delivery models, as we can see in Figure 3.7. In the case of SaaS the user is partially

responsible for the interface; the user responsibility increases in the case of PaaS and includes the

interface and the application. In the case of IaaS the user is responsible for all the events occurring in

the virtual machine running the application.

For example, if a distributed denial-of-service attack (DDoS) causes the entire IaaS infrastructure to

fail, the cloud service provider is responsible for the consequences of the attack. The user is responsible

if the DDoS affects only several instances, including the ones running the user application. A recent

posting describes the limits of responsibility illustrated in Figure 3.7 and argues that security should be a

major concern for IaaS cloud users, (see www.sans.org/cloud/2012/07/19/can-i-outsource-mysecurity-

to-the-cloud).