Cloud computing inherits some of the challenges of parallel and distributed computing discussed in

Chapter 2; at the same time, it faces major challenges of its own. The specific challenges differ for

the three cloud delivery models, but in all cases the difficulties are created by the very nature of utility

computing, which is based on resource sharing and resource virtualization and requires a different trust

model than the ubiquitous user-centric model we have been accustomed to for a very long time.

The most significant challenge is security [19]; gaining the trust of a large user base is critical for

the future of cloud computing. It is unrealistic to expect that a public cloud will provide a suitable

environment for all applications. Highly sensitive applications related to the management of the critical

infrastructure, healthcare applications, and others will most likely be hosted by private clouds. Many

real-time applications will probably still be confined to private clouds. Some applications may be best

served by a hybrid cloud setup; such applications could keep sensitive data on a private cloud and use

a public cloud for some of the processing.

The SaaS model faces similar challenges as other online services required to protect private information,

such as financial or healthcare services. In this case a user interacts with cloud services through

a well-defined interface; thus, in principle it is less challenging for the service provider to close some of

the attack channels. Still, such services are vulnerable to DoS attack and the users are fearful of malicious

insiders. Data in storage is most vulnerable to attack, so special attention should be devoted to the

protection of storage servers. Data replication necessary to ensure continuity of service in case of storage

system failure increases vulnerability. Data encryption may protect data in storage, but eventually data

must be decrypted for processing, and then it is exposed to attack.

The IaaS model is by far the most challenging to defend against attacks. Indeed, an IaaS user has

considerably more degrees of freedom than the other two cloud delivery models. An additional source

of concern is that the considerable resources of a cloud could be used to initiate attacks against the

network and the computing infrastructure.

Virtualization is a critical design option for this model, but it exposes the system to new sources of

attack. The trusted computing base (TCB) of a virtual environment includes not only the hardware and

the hypervisor but also the management operating system. As we shall see in Section 9.7, the entire

state of a virtual machine (VM) can be saved to a file to allow migration and recovery, both highly

desirable operations; yet this possibility challenges the strategies to bring the servers belonging to an

organization to a desirable and stable state. Indeed, an infected VM can be inactive when the systems

are cleaned up, and it can wake up later and infect other systems. This is another example of the deep

intertwining of desirable and undesirable effects of basic cloud computing technologies.

The next major challenge is related to resource management on a cloud. Any systematic rather than

ad hoc resource management strategy requires the existence of controllers tasked to implement several

classes of policies: admission control, capacity allocation, load balancing, energy optimization, and last

but not least, to provide QoS guarantees.

To implement these policies the controllers need accurate information about the global state of the

system. Determining the state of a complex system with 106 servers or more, distributed over a large

geographic area, is not feasible. Indeed, the external load, as well as the state of individual resources,

changes very rapidly. Thus, controllers must be able to function with incomplete or approximate knowledge

of the system state.

It seems reasonable to expect that such a complex system can only function based on self-management

principles. But self-management and self-organization raise the bar for the implementation of logging

and auditing procedures critical to the security and trust in a provider of cloud computing services.

Under self-management it becomes next to impossible to identify the reasons that a certain action that

resulted in a security breach was taken.

The lastmajor challenge we want to address is related to interoperability and standardization. Vendor

lock-in, the fact that a user is tied to a particular cloud service provider, is a major concern for cloud

users (see Section 3.5). Standardization would support interoperability and thus alleviate some of the

fears that a service critical for a large organization may not be available for an extended period of time.

But imposing standards at a time when a technology is still evolving is not only challenging, it can be

counterproductive because it may stifle innovation.

From this brief discussion the reader should realize the complexity of the problems posed by cloud

computing and understand the wide range of technical and social problems cloud computing raises. If

successful, the effort to migrate the IT activities of many government agencies to public and private

clouds will have a lasting effect on cloud computing. Cloud computing can have a major impact on

education, but we have seen little effort in this area.