Some believe that it is very easy, possibly too easy, to start using cloud services without a proper

understanding of the security risks and without the commitment to follow the ethics rules for cloud

computing. A first question is: What are the security risks faced by cloud users? There is also the

possibility that a cloud could be used to launch large-scale attacks against other components of the

cyber infrastructure. The next question is: How can the nefarious use of cloud resources be prevented?

There are multiple ways to look at the security risks for cloud computing. A recent paper identifies

three broad classes of risk [83]: traditional security threats, threats related to system availability, and

threats related to third-party data control.

Traditional threats are those experienced for some time by any system connected to the Internet, but

with some cloud-specific twists. The impact of traditional threats is amplified due to the vast amount of

cloud resources and the large user population that can be affected. The fuzzy bounds of responsibility

between the providers of cloud services and users and the difficulties in accurately identifying the cause

of a problem add to cloud users’ concerns.

The traditional threats begin at the user site. The user must protect the infrastructure used to connect

to the cloud and to interact with the application running on the cloud. This task is more difficult because

some components of this infrastructure are outside the firewall protecting the user.

The next threat is related to the authentication and authorization process. The procedures in place

for one individual do not extend to an enterprise. In this case the cloud access of the members of an

organization must be nuanced; individuals should be assigned distinct levels of privilege based on their

roles in the organization. It is also nontrivial to merge or adapt the internal policies and security metrics

of an organization with the ones of the cloud.

Moving from the user to the cloud, we see that the traditional types of attack have already affected

cloud service providers. The favorite means of attack are distributed denial-of-service (DDoS) attacks,

which prevent legitimate users accessing cloud services; phishing;2 SQL injection;3 or cross-site

scripting.4

Cloud servers hostmultiple VMs, and multiple applications may run under each VM.Multitenency in

conjunction with VMM vulnerabilities could open new attack channels for malicious users. Identifying

the path followed by an attacker is much more difficult in a cloud environment. Traditional investigation

methods based on digital forensics cannot be extended to a cloud, where the resources are shared among

a large user population and the traces of events related to a security incident are wiped out due to the

high rate of write operations on any storage media.

Availability of cloud services is another major concern. System failures, power outages, and other

catastrophic events could shut down cloud services for extended periods of time. When such an event

occurs, data lock-in, discussed in Section 3.5, could prevent a large organization whose business model

depends on that data from functioning properly.

Clouds could also be affected by phase transition phenomena and other effects specific to complex

systems (see Chapter 10). Another critical aspect of availability is that users cannot be assured that an

application hosted on the cloud will return correct results.

Third-party control generates a spectrum of concerns caused by the lack of transparency and limited

user control. For example, a cloud provider may subcontract some resources from a third party whose

level of trust is questionable. There are examples when subcontractors failed to maintain the customer

data. There are also examples when the third party was not a subcontractor but a hardware supplier and

the loss of data was caused by poor-quality storage devices [83].

Storing proprietary data on a cloud is risky because cloud provider espionage poses real dangers.

The terms of contractual obligations usually place all responsibilities for data security with the user.

The Amazon Web Services customer agreement, for example, does not help boost user confidence as

it states: “We . . . will not be liable to you for any direct, indirect, incidental . . . damages . . . nor . . . be

responsible for any compensation, reimbursement, arising in connection with: (A) your inability to use

the services . . . (B) the cost of procurement of substitute goods or services . . . or (D) any unauthorized

access to, alteration of, or deletion, destruction, damage, loss or failure to store any of your content or

other data.”

It is very difficult for a cloud user to prove that data has been deleted by the service provider. The lack

of transparencymakes auditability a very difficult proposition for cloud computing. Auditing guidelines

elaborated by the National Institute of Standards and Technology (NIST), such as the Federal Information

Processing Standard (FIPS) and the Federal Information Security Management Act (FISMA), are

mandatory for U.S. government agencies.

The first release of the Cloud Security Alliance (CSA) report in 2010 identifies seven top threats to

cloud computing. These threats are the abuse of the cloud, APIs that are not fully secure, malicious

insiders, shared technology, account hijacking, data loss or leakage, and unknown risk profiles [97].

According to this report, the IaaS delivery model can be affected by all threats. PaaS can be affected

by all but the shared technology, whereas SaaS is affected by all but abuse and shared technology.

The term abuse of the cloud refers to the ability to conduct nefarious activities from the cloud – for

example, using multiple AWS instances or applications supported by IaaS to launch DDoS attacks or to

distribute spam and malware. Shared technology considers threats due to multitenant access supported

by virtualization. VMMs can have flaws allowing a guest operating system to affect the security of the

platform shared with other virtual machines.

Insecure APIs may not protect users during a range of activities, starting with authentication and

access control to monitoring and control of the application during runtime. The cloud service providers do not disclose their hiring standards and policies; thus, the risks of malicious insiders cannot be ignored.

The potential harm due to this particular form of attack is great.

Data loss or leakage are two risks with devastating consequences for an individual or an organization

using cloud services. Maintaining copies of the data outside the cloud is often unfeasible due to the

sheer volume of data. If the only copy of the data is stored on the cloud, sensitive data is permanently

lost when cloud data replication fails and is followed by a storage media failure. Because some of the

data often includes proprietary or sensitive data, access to such information by third parties could have

severe consequences.

Account or service hijacking is a significant threat, and cloud users must be aware of and guard against

all methods of stealing credentials. Finally, unknown risk profile refers to exposure to the ignorance or

underestimation of the risks of cloud computing.

The 2011 version of the CSA report, “Security Guidance for Critical Area of Focus in Cloud Computing

V3.0,” provides a comprehensive analysis of and makes recommendations to minimize the risks

inherent in cloud computing [98].

An attempt to identify and classify the attacks in a cloud computing environment is presented in [147].

The three actors involved in the model considered are the user, the service, and the cloud infrastructure,

and there are six types of attacks possible (see Figure 9.1). The user can be attacked from two directions:

from the service and from the cloud. SSL certificate spoofing, attacks on browser caches, or phishing

attacks are examples of attacks that originate at the service. The user can also be a victim of attacks that

either originate at the cloud or spoofs that originate from the cloud infrastructure.

The service can be attacked from the user. Buffer overflow, SQL injection, and privilege escalation

are the common types of attacks from the service. The service can also be subject to attack by the cloud

infrastructure; this is probably the most serious line of attack. Limiting access to resources, privilege related

attacks, data distortion, and injecting additional operations are only a few of the many possible

lines of attack originated at the cloud.

The cloud infrastructure can be attacked by a user who targets the cloud control system. The types of

attack are the same ones that a user directs toward any other cloud service. The cloud infrastructure may

also be targeted by a service requesting an excessive amount of resources and causing the exhaustion

of the resources.