Virtually all surveys report that security is the top concern for cloud users, who are accustomed to having

full control of all systems onwhich sensitive information is stored and processed. Users typically operate

inside a secure perimeter protected by a corporate firewall. In spite of the potential threats, users have to

extend their trust to the cloud service provider if they want to benefit from the economical advantages

of utility computing. This is a fairly difficult transition, yet it is a critical one for the future of cloud

computing. To support this transition, some argue that cloud security is in the hands of experts, so users

are even better protected than when they are in charge of their own security.

Major user concerns are unauthorized access to confidential information and data theft. Data is more

vulnerable in storage than while it is being processed. Data is kept in storage for extended periods of

time, whereas it is exposed to threats during processing for relatively short periods of time. Hence, close

attention should be paid to the security of storage servers and to data in transit.

This does not mean that threats during processing can be ignored; such threats can originate from

flaws in the VMM, rogue VMs, or a VMBR, as discussed in Section 5.12. There is also the risk of

unauthorized access and data theft posed by rogue employees of a cloud service provider (CSP). The

hiring and security screening policies of the CSP personnel are totally opaque processes to users, and

this justifies users’ concern about insider attacks.

The next concerns regard user control over the life cycle of data. It is virtually impossible for a user

to determine whether data that should have been deleted is actually deleted. Even if it was deleted, there

is no guarantee that the media was wiped and the next user is not able to recover confidential data. This

problem is exacerbated because the CSPs rely on seamless backups to prevent accidental data loss. Such

backups are done without users’ consent or knowledge. During this exercise data records can be lost,

accidentally deleted, or accessible to an attacker.

Lack of standardization is next on the list of concerns. Today there are no interoperability standards,

as we discussed in Section 3.5. Many questions do not have satisfactory answers at this time. For

example: What can be done when the service provided by the CSP is interrupted? How can we access

our critically needed data in case of a blackout? What if the CSP drastically raises its prices? What is

the cost of moving to a different CSP?

It is undeniable that auditing and compliance pose an entirely different set of challenges in cloud

computing. These challenges are not yet resolved.Afull audit trail on a cloud is an infeasible proposition

at this time.

Another, less analyzed user concern is that cloud computing is based on a new technology expected

to evolve in the future. Case in point: autonomic computing is likely to enter the scene. When this

happens, self-organization, self-optimization, self-repair, and self-healing could generate additional

security threats. In an autonomic system it will be even more difficult than at present to determine when

an action occurred, what was the reason for that action, and how it created the opportunity for an attack

or for data loss. It is still unclear how autonomic computing can be compliant with privacy and legal

issues.

There is no doubt that multitenancy is the root cause of many user concerns. Nevertheless, multitenancy

enables a higher server utilization thus, lower costs. Because it is one of the pillars of utility

computing, users have to learn to live with multitenancy. The threats caused by multitenancy differ

from one cloud delivery model to another. For example, in the case of SaaS, private information such

as name, address, phone numbers, and possibly credit card numbers of many users is stored on one

server, and when the security of that server is compromised, a large number of users are affected. We

have already mentioned that multitenancy threats during processing time cannot be ignored.

Users are also greatly concerned about the legal framework for enforcing cloud computing security.

The cloud technology has moved much faster than cloud security and privacy legislation, so users have

legitimate concerns regarding the ability to defend their rights. Because the data centers of a CSP may

be located in several countries, it is difficult to understand which laws apply – the laws of the country

where information is stored and processed, the laws of the countries where the information crossed

from the user to the datacenter, or the laws of the country where the user is located.

To make matters even more complicated, a CSP may outsource the handling of personal and/or

sensitive information. Existing laws stating that the CSP must exercise reasonable security may be

difficult to implement in a case where there is a chain of outsourcing to companies in different countries.

Finally, a CSP may be required by law to share private data with law enforcement agencies.

Now we examine briefly what cloud users can and should do to minimize security risks regarding

data handling by the CSP. First, users should evaluate the security policies and the mechanisms the CSP

has in place to enforce these policies. Then users should analyze the information that would be stored

and processed on the cloud. Finally, the contractual obligations should be clearly spelled out.

The contract between the user and the CSP should do the following [290]:

1. State explicitly the CSP’s obligations to securely handle sensitive information and its obligation to

comply with privacy laws.

2. Spell out CSP liabilities for mishandling sensitive information.

3. Spell out CSP liabilities for data loss.

4. Spell out the rules governing the ownership of the data.

5. Specify the geographical regions where information and backups can be stored.

To minimize security risks, a user may try to avoid processing sensitive data on a cloud. The Secure

Data Connector from Google carries out an analysis of the data structures involved and allows users to

access data protected by a firewall. This solution is not feasible for several classes of application, e.g., processing of medical or personnel records. It may not be feasible when the cloud processing workflow

requires cloud access to the entire volume of user data.

When the volume of sensitive data or the processing workflow requires sensitive data to be stored

on a public or hybrid cloud, then, whenever feasible, data should be encrypted. This poses a dilemma

because encryption prevents indexing and searching the data. For some applications it is possible to

scramble the data to make it unintelligible to an intruder. Though this system is extremely inefficient,

hence impractical at this time, it is possible to process encrypted data using either a fully homomorphic

encryption scheme [134] or secure two-party computations [380].