Trust in the context of cloud computing is intimately related to the general problem of trust in online

activities. In this section we first discuss the traditional concept of trust and then the trust necessary to

online activities.

According to theMerriam-Webster dictionary, trust means “assured reliance on the character, ability,

strength, or truth of someone or something.” Trust is a complex phenomenon; it enables cooperative

behavior, promotes adaptive organizational forms, reduces harmful conflict, decreases transaction costs,

facilitates formulation of ad hoc workgroups, and promotes effective responses to crisis [309].

Two conditions must exist for trust to develop. The first condition is risk, the perceived probability

of loss; indeed, trust would not be necessary if there were no risk involved, if there is a certainty that

an action can succeed. The second condition is interdependence, the idea that the interests of one entity

cannot be achieved without reliance on other entities. A trust relationship goes though three phases:

(1) a building phase, when trust is formed; (2) a stability phase, when trust exists; and (3) a dissolution

phase, when trust declines.

There are different reasons for and forms of trust. Utilitarian reasons could be based on the belief that

the costly penalties for breach of trust exceed any potential benefits from opportunistic behavior. This

is the essence of deterrence-based trust. Another reason is the belief that the action involving the other

party is in the self-interest of that party. This is the so-called calculus-based trust. After a long sequence

of interactions, relational trust between entities can develop based on the accumulated experience of

dependability and reliance on each other.

The common wisdom is that an entity must work very hard to build trust but may lose that trust very

easily; a single violation of trust can lead to irreparable damage. Persistent trust is trust based on the

long-term behavior of an entity, whereas dynamic trust is based on a specific context, e.g., a state of the

system or the effect of technological developments.

The trust in the Internet “obscures or lacks entirely the dimensions of character and personality, nature

of relationship, and institutional character” of traditional trust [258]. The missing identity, personal

characteristics, and role definitions are elements we have to deal with in the context of online trust.

The Internet offers individuals the ability to obscure or conceal their identities. The resulting

anonymity reduces the cues normally used in judgments of trust. The identity is critical for developing

trust relations; it allows us to base our trust on the past history of interactions with an entity.

Anonymity causes mistrust because identity is associated with accountability and, in the absence of

identity, accountability cannot be enforced. The opacity extends immediately from identity to personal

characteristics. It is impossible to infer whether the entity or individual we transact with is who it pretends

to be, since the transactions occur between entities separated in time and distance. Finally, there

are no guarantees that the entities we transact with fully understand the role they have assumed.

To remedy the loss of clues, we need security mechanisms for access control, transparency of identity,

and surveillance. The mechanisms for access control are designed to keep intruders and mischievous

agents out. Identity transparency requires that the relationship between a virtual agent and a physical

person should be carefully checked through methods such as biometric identification. Digital signatures

and digital certificates are used for identification. Surveillance could be based on intrusion detection or

on logging and auditing. The first option is based on real-time monitoring, the second on offline sifting

through audit records.

Credentials are used when an entity is not known. Credentials are issued by a trusted authority and

describe the qualities of the entity using the credential. A Doctor of Dental Surgery diploma hanging

on the wall of a dentist’s office is a credential that the individual has been trained by an accredited

university and hence is capable of performing a set of dental procedures; similarly, a digital signature

is a credential used in many distributed applications.

Policies and reputation are two ways of determining trust. Policies reveal the conditions to obtain

trust and the actions to take when some of the conditions are met. Policies require the verification of

credentials.Reputation is a quality attributed to an entity based on a relatively long history of interactions

with or possibly observations of the entity.Recommendations are based on trust decisions made by others

and filtered through the perspective of the entity assessing the trust.

In a computer science context, “trust of a party A to a party B for a service X is the measurable belief

of A in that B behaves dependably for a specified period within a specified context (in relation to service

X)” [272]. An assurance about the operation of a particular hardware or software component leads

to persistent social-based trust in that component. A comprehensive discussion of trust in computer

services in the semantic Web can be found in [26]. In Section 11.10 we discuss the concept of trust in the context of cognitive radio networks where multiple transmitters compete for free communication

channels. In Section 11.11 we present a cloud-based trust management service.