There have been a few studies of user experience based on a large population of cloud computing

users. An empirical study of the experience of a small group of users of the Finish Cloud Computing Consortium is reported in [279]. The main user concerns are security threats, the dependence on fast

Internet connections that forced version updates, data ownership, and user behavior monitoring. All users

reported that trust in the cloud services is important, two-thirds raised the point of fuzzy boundaries of

liability between cloud user and provider, about half did not fully comprehend the cloud functions and

its behavior, and about one-third were concerned about security threats.

The security threats perceived by this group of users are: (i) abuse and villainous use of the cloud;

(ii) APIs that are not fully secure; (iii) malicious insiders; (iv) account hijacking; (iv) data leaks; and

(v) issues related to shared resources. Identity theft and privacy were major concerns for about half of

the users questioned; availability, liability, and data ownership and copyright were raised by a third of

respondents.

The suggested solutions to these problems are as follows: SLAs and tools to monitor usage should

be deployed to prevent abuse of the cloud; data encryption and security testing should enhance the

API security; an independent security layer should be added to prevent threats caused by malicious

insiders; strong authentication and authorization should be enforced to prevent account hijacking; data

decryption in a secure environment should be implemented to prevent data leakage; and compartmentalization

of components and firewalls should be deployed to limit the negative effect of resource

sharing.

A broad set of concerns identified by the NIST working group on cloud security includes:

• Potential loss of control/ownership of data.

• Data integration, privacy enforcement, data encryption.

• Data remanence after deprovisioning.

• Multitenant data isolation.

• Data location requirements within national borders.

• Hypervisor security.

• Audit data integrity protection.

• Verification of subscriber policies through provider controls.

• Certification/accreditation requirements for a given cloud service.

A 2010 study conducted by IBM [176] aims to identify barriers to public and private cloud adoption.

The study is based on interviews with more than 1,000 individuals responsible for IT decision making

around the world. Seventy-seven percent of the respondents cited cost savings as the key argument in

favor of public cloud adoption, though only 30% of them believed that public clouds are “very appealing

or appealing” for their line of business, versus 64% for private clouds and 34% for hybrid ones.

The reasons driving the decision to use public clouds and the percentage of responderswho considered

each element critical are shown in Table 3.6. In view of the high energy costs for operating a data center

(discussed in Section 3.7), it seems strange that only 29% of the respondents seem to be concerned

about lower energy costs.

The top workloads mentioned by the users involved in this study are data mining and other analytics

(83%), application streaming (83%), help desk services (80%), industry-specific applications (80%),

and development environments (80%).

The study also identified workloads that are not good candidates for migration to a public cloud

environment:

• Sensitive data such as employee and health care records.

• Multiple codependent services (e.g., online transaction processing).

• Third-party software without cloud licensing.

• Workloads requiring auditability and accountability.

• Workloads requiring customization.

Such studies help identify the concerns of potential cloud users and the critical issues for cloud

research.