

Chapter 2

Cloud Dimensions for Requirements Specification

Ana Sofia Zalazar, Luciana Ballejos and Sebastian Rodriguez

Abstract Cloud computing is a business paradigm that changes the way to evaluate information systems and computing resources. Cloud requirements can rapidly change and new service capabilities are often requested in order to adapt to new business scenarios. The existing works are generally focused in a limited number of requirements and capabilities. The aim of this contribution is to understand the multifaceted components of a service and to give guidelines towards requirements engineering for cloud computing. Thus, cloud services are analyzed by different aspects called dimensions and five dimensions are proposed (i.e., Contractual, Financial, Compliance, Operation, and Technical). Cloud dimensions are graphically presented in conceptual models, because each dimension has specific entities, properties, and relationships. Different specialists and experts may be requested to evaluate particular dimensions in the service level agreement and cloud service adoption, and this approach can guide those activities, support requirements specification, and guide system analysis for cloud computing.

Keywords Cloud computing • Requirements engineering • Requirements specification • Cloud dimension • Service level agreement • Conceptual model • System analysis

A.S. Zalazar (✉) · S. Rodriguez
GITIA (UTN-FRT), CONICET, Rivadavia 1050, 4000 Tucumán, Argentina
e-mail: ana.zalazar@gitia.org

S. Rodriguez
e-mail: sebastian.rodriguez@gitia.org

L. Ballejos
CIDISI (UTN-FRSF), Lavaisse 610, 3000 Santa Fe, Argentina
e-mail: lballejo@frsf.utn.edu.ar

2.1 Introduction

Cloud Computing is a business paradigm, where cloud service providers offer services (e.g., software, storage, computing, and network) managed in their physical infrastructure and cloud service consumers pay per-use after accepting to the service level agreement. Consumers usually move the functionality of their legacy systems to cloud computing or acquire new functionality contracting cloud service to minimize costs of maintenance and to get the advantages of rapidly adaptation to changes.

The NIST introduces a cloud definition framework [17], where there are five main characteristics (i.e., broad network access, rapid elasticity, measured service, on-demand self-service, and resource pooling), five roles (i.e., consumer, provider, auditor, carrier, and broker), three service models (i.e., Software as a Service, Platform as a Service, and Infrastructure as a Service), and four deployment models (i.e., public cloud, private cloud, community cloud, and hybrid cloud). In this paper, the NIST cloud definition framework is extended and five cloud dimensions are added (i.e., contractual, financial, compliance, operational, and technical).

The five proposed cloud dimensions link static properties (e.g., contractual aspects) and dynamic requirements (e.g., technical and operational aspects). Some dimensions may be separately analyzed by domain experts (e.g., compliance dimension is analyzed by lawyers in small- and medium-sized enterprises). The final purpose is to bind different service perspectives in order to manage cloud service adoption. The contribution aims to consolidate different cloud aspects to fluidly satisfy consumer dynamic requirements. Requirements must be clear and interpreted in one way, so this approach proposes an alternative to carry on cloud contracts and manage requirements in a simple and concise manner. In conclusion, cloud consumers (i.e., organizations and users) are provided with accurate information to address their requirements to service offers and cloud providers are fitted with precise attributes to offer service capabilities. This avoids potentially ambiguous terms.

Cloud service agreements may change often according to the service business context, so this type of contract has to be modifiable. Consumers may often require changing quality of service and scalability values. However, dimensions make possible to specify requirements and capabilities for creating cloud contracts. In this paper, requirements specification, dimensions, metrics, and service level agreements are explained in cloud context.

The rest of the paper is organized as follows. In Sect. 2.2, the background is explained. In Sect. 2.3, the proposed dimensions and some models are proposed in order to facilitate cloud requirements specification and to understand contracts. Section 2.4 is focused on the application and integration of cloud dimensions in service contracts using a sample scenario. Finally, Sect. 2.5 concludes this contribution.

2.2 Background

Cloud computing has been defined by multiple authors [1, 7, 25], and the National Institute of Standard and Technology (NIST) proposes a definition that encompasses general aspects of cloud environment [17]: “*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*”.

This definition introduces also five essential characteristics attributed to Cloud Computing [17]: (a) *On-demand self-service*: cloud consumers automatically access to cloud capabilities according to their needs without human interaction; (b) *Broad network access*: cloud capabilities are available in the network and accessed through heterogeneous client platforms; (c) *Resource pooling*: cloud provider resources are shared to serve multiple cloud consumers using virtualization and tenancy mechanisms; (d) *Rapid elasticity*: cloud provider resources are added and released according to cloud consumers demand, so cloud capabilities appears unlimited; and (e) *Measured service*: cloud resources are measured at a granular level in a transparent manner for both cloud provider and cloud consumer of the used service.

The different deployment models defined by NIST [17] are: (a) *Private cloud*: Under this model, cloud services delivered from a data center are accessed by a single organization with multiple internal users, while preserving management and control of the resources; (b) *Public cloud*: cloud services are allocated under the providers or third parties control, and the underlying infrastructure is shared by multiple consumers and open for public use, using multi-tenancy mechanism; (c) *Community cloud*: physical and virtual resources are shared between several users and organizations from a specific community with common concerns, so this model may require specific policies among users; and (d) *Hybrid cloud*: this type of model is a combination of two or more clouds, which safeguards sensitive data and applications on restricted manner and it takes advantage of the rapid provisioning of other models.

Cloud service models indicate the level of control and abstraction in cloud services. There are three principal service models, and other models can be derived from them [17]: (a) *Software as a Service (SaaS)*: cloud providers offer software applications over the Internet, and users can access them from any location using a computer or mobile device that has Internet access, without managing any infrastructure and platform where the application runs; (b) *Platform as a Service (PaaS)*: this type of services are containers within programming environments, libraries, database, and tools that support development in virtual platforms, so consumers can develop and run their software applications without the cost and responsibility of buying and maintaining the underlying hardware and software; and (c) *Infrastructure as a Service (IaaS)*: cloud service providers offer virtual server instance and storage, and abstract the consumer from the details of infrastructure

taking responsibility of all resource physical maintenance, workload balance, technical staff, connectivity devices, and virtual machine (VM) management.

Service characteristics have to be well-defined and specified in order to identify the consumer requirements and to compare different service offers. However, requirements specification approaches in the cloud domain are mostly focused on quality of service [5], pricing and costing [16], access control, privacy, and security [10, 18, 19]. Since the term cloud computing includes other aspects and perspectives, the existing approaches also need to be extended.

2.3 Cloud Dimensions, Requirements, and Capabilities

In order to understand cloud computing, the NIST cloud definition framework [17] is extended and five dimensions are proposed in this contribution, presented in Fig. 2.1. Each proposed dimension represents a specific aspect of cloud computing, and cloud adoption process should consider those dimensions in order to completely satisfy service requirements.

The proposed dimensions support the integration of requirements specifications raised by consumers and capabilities owned by providers into cloud computing. *Requirement* is what cloud consumers want from cloud service and *capability* is what cloud providers offer related to their competences in cloud services. SLA can be used as a specification artifact to assist the selection of cloud service considering consumer requirements and service capabilities. The SLA is a legal format [2] that

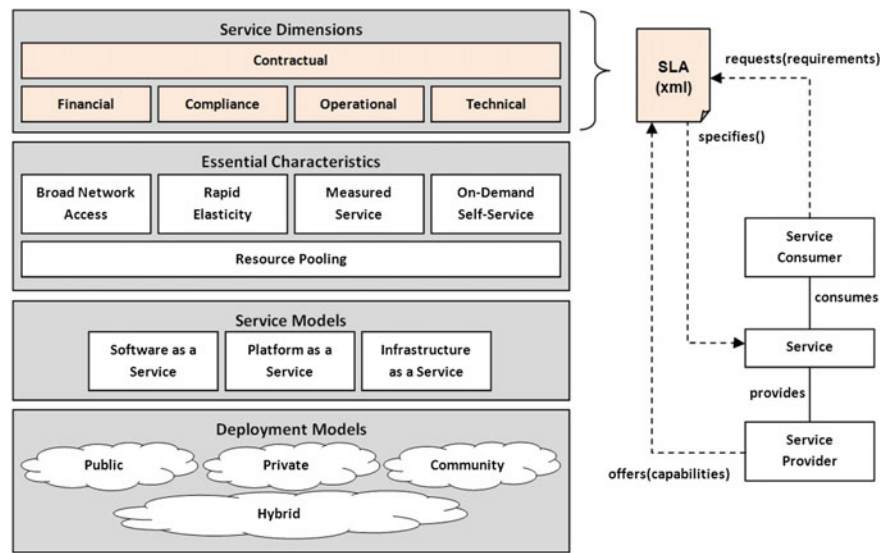


Fig. 2.1 Cloud computing definition framework [17]

helps to negotiate agreements. Cloud consumer hopes to see all his requirements in the corresponding SLA, and cloud provider makes sure that only capabilities that they can meet in his service are included in the agreement. Due to the dynamic nature of the cloud, continuous monitoring on SLA is requested in these contexts [20].

However, practitioners also deal with other requirements and capabilities. For example, IT contracts include terms regarding technical properties, financial factors, compliance restrictions, operational responsibilities, and contractual aspects in cloud computing. The idea of cloud computing as a multidimensional paradigm is not new [21, 22]. This approach grouped cloud aspects in the following dimensions based on the academic community and the practitioners' concerns:

1. *Contractual Dimension* covers all organizational aspects of cloud service level agreement. It includes actors, time periods, and objects like binding service level agreements (SLA), similar to the information of business contractual headlines. Communication between actors is very important, thus contractual dimension also specifies roles, responsibilities, and relations between actors.
2. *Financial Dimension* is defined considering cloud computing as a utility [7], where economic and financial capabilities play a central role in cloud adoption [8]. Cloud service provider employs pricing plan (i.e., renting, usage-based pricing), in which cloud service consumers pay proportionally to the amount of time or resource they use [4]. This dimension considers all aspects of cloud agreements for billing and accounting, such as pay methods, credit management, and cost variables.
3. *Compliance Dimension* describes all legal and regulatory restrictions for cloud service adoption [3], and it also specifies government regulation, business standards, security policy, and privacy certifications which cloud service should be compliant with [15]. The restrictions are strictly imposed in order to respect laws and regulations in the jurisdiction where data resides or is collected.
4. *Operational Dimension* is based on usual events (such as restore, maintain, configuration, and backups) and unusual events (such as incident management and recovery). By considering operational aspects, the cloud providers must have efficient means to support resource allocation and scheduling decisions to remain competitive [13]. Simultaneously, it is important to ensure the confidentiality of cotenants who share the same infrastructure by monitoring virtual behavior. Operative dimension explains all aspects to keep the service running and meet the changes in runtime.
5. *Technical Dimension* encompasses functional properties and measurable aspects of cloud service. Values, units, functions, and methods are requested to define cloud services. Some key performance indicators are measured using a set of measureable properties. Technical aspects are specified in SLAs to understand, compare, and control SLAs.

There is a number of overlapping properties within the five dimensions, such as monitoring and auditing aspects. Audits are requested to ensure that cloud services do not break the laws and regulations in the jurisdiction where data resides or is

collected, simultaneously ensuring the confidentiality of cotenants who share the same infrastructure [21]. Thus, frequent audits should be performed on the dimensional properties to monitor compliance with security terms and to ensure adherence to SLA terms, performance standards, procedure, and regulations [6, 23]. Most of the time services are like “black boxes” to cloud consumers, so services are evaluated by their behavior (i.e., comparing its inputs, outputs, and performance level) with the expected results [27].

In this contribution, cloud service dimensions are considered the basis for building dynamic SLAs and specifying cloud requirements and capabilities. In the next subsection, more details about each dimension are presented and all aspects related to cloud dimensions are introduced in a conceptual framework for capturing and integrating cloud requirements and capabilities.

2.3.1 Contractual Dimension

Contractual Dimension specifies general information of SLAs and cloud contracts, such as supporting parties, policy of contracting third parties, agreed time, and term conditions. Contractual properties are mostly static during service runtime. Figure 2.2 presents the conceptual model for *Contractual Dimension*, and it is based on SLA services presented by Patel et al. [20]. The shadowy entities in the

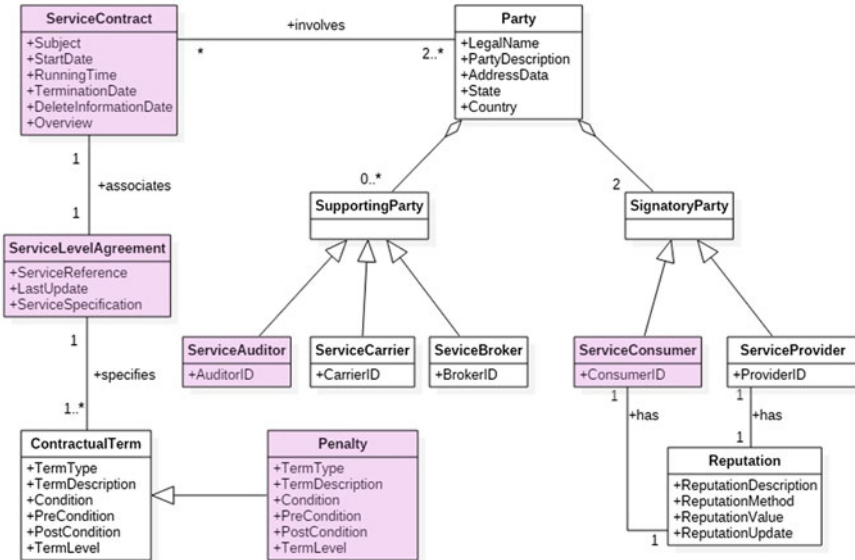


Fig. 2.2 Conceptual model of cloud computing dimension

proposed models represent classes which appear in more than one dimension (e.g., Service Contract and Service Level Agreement).

This dimension also introduces involved parties (“Party” in Fig. 2.2) and their roles during the contract duration. The five cloud roles proposed by the NIST are included in the model [17]: (a) *Provider*: entity that owns the deployed service in its physical servers, and it is responsible for service maintenance and availability; (b) *Consumer*: entity that use the service for completing its business process; (c) *Carrier*: intermediary that provides data transportation and service connectivity; (d) *Broker*: intermediary that is involved in the business contract and the relation between other roles; and (e) *Auditor*: external agent responsible for keeping track all business process, reporting failures, and analyzing the quality of services considering the SLA. “*Signatory Party*” is mandatory and involves “*Service Consumer*” and “*Service Provider*”. The mandatory roles have “*Reputation*” that represents a big impact on organization credibility and trust, and it is also about confidentiality, integrity, and resilience of the service actors. “*Supporting Party*” is optional and involves third parties such as “*Service Auditor*”, “*Service Carrier*”, and “*Service Broker*”.

“*Service Contract*” presents all information about contract starting time, termination date, service overview, and definitive delete information date that is when the provider must destroy all information about the use of service (consumer data and workload). The terms and conditions within the contract that would cause the termination of the service agreement are presented in *Compliance Dimension*.

“*Contractual Term*” is probably the most important entity in this model, because it involves all policies and clauses about SLA. It describes expressions and implied terms in the contract [12]. “*Term Type*” defines contractual clauses about termination, modification, suspension, disclaimer, indemnification, remedy, warranty, guarantee, obligation, money refund, support, notification, government request, collecting information, limitation of liability, etc. “*Penalty*” is a category of “*Term Type*” and it is a term used for compensation of non-delivery of service or inadequate service level.

The differences between “*Service Contract*” and “*Service Level Agreement*” are that the former generally describes contracting parties and dates, and the latter describes service parameters, quality of service, agreement terms, and service level.

2.3.2 Financial Dimension

Financial Dimension involves all economic factors of cloud services and contracts, and Fig. 2.3 shows the most relevant classes and their relationships in this dimension. It is universally acknowledged that “*Service Consumer*” associates his “*Billing Account*” to the “*Payment*” processes of the “*Service Contract*”. “*Billing*” is defined by the sum of “*Service Charging*” (cardinality is “*” which means “many”) that is refined by “*Cost Description*” of different resources (i.e. “*Storage Cost*”, “*Processing Cost*”, “*Network Cost*”, etc.) related to a “*Service Description*”. “*Billing Frequency*” is regarding the cost calculation and it can be daily, weekly,

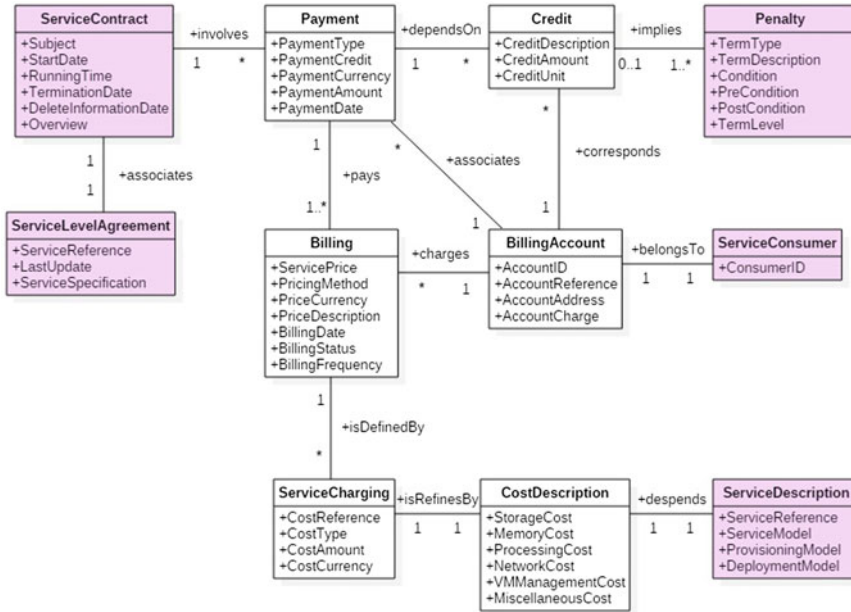


Fig. 2.3 Conceptual model of cloud financial dimension

biweekly, monthly, semi-annual, and annual. Billing processes may use metering mechanisms on the consumption of cloud resources in order to calculate the cost. “*Cost Type*” is related to service adoption phases, and the resource costs can be calculated during service acquisition, service on-going, service composition, and service contract termination. “*Payment Type*” is concerning to payment methods such as debit card, credit card, electronic note, bank transfer, Bitcoins, Pay-Pal, and other credit mechanisms.

From the early years of cloud computing, most of the interest was focused on service pricing of cloud computing [4], and cost reduction was a central factor to the uptake of cloud services. This business paradigm is considered as a fifth utility [7], where resource optimization, pricing models, and virtualization were fundamentals to introduce cloud computing into the market. Therefore, “*Pricing Method*” is probably the most studied attribute of *Financial Dimension*. “*Service Consumer*” can freely choose a service provider with better “*Pricing Method*” and more favorable “*Billing*” terms. Youseff et al. [26] present three models for calculating prices: (a) *tiered pricing*: each service tier has a specific price per unit of time; (b) *per-unit pricing*: cost is applied to the usage units during data storing, data processing, and data transferring; and (c) *subscription-based pricing*: the cost is periodically the same. Other authors [3, 24] similarly list diverse pricing models: (a) *per-use*: resources are billed per unit of time usage; (b) *subscription*: resources can be reserved and renewed for the same price; (c) *prepaid per-use*: the billing is performed against a prepaid credit; and (d) *combined method*: resources can be

rented for a period of time and also requested on demand. Karunakaran et al. [14] divulge four extensive subthemes: pricing schemes, user welfare, pricing elements, and collaborative pricing; and they indicate that the key elements for pricing included, hardware, maintenance, power, cooling, staff, and amortization. However, “*Service Consumer*” may subscribe to free services or dynamically adjust pricing method according to his workload and security requirements.

Any change in prices and payments must be notified to “*Service Consumer*” in advance, according to obligations explained in *Contractual* and *Compliance Dimensions*. It may seem like *Financial Dimension* can be also part of *Compliance Dimension*, but governance is a very wide term that mostly involve more legal, security, and standard aspects. *Financial Dimension* is mainly focused on reducing operative costs by sharing infrastructure instead of investing in physical servers.

“*Penalty*” can have a direct impact to “*Payment*” process through “*Credit*” application. When there are violations of contractual terms, such as inappropriate service level or non-delivered capabilities, “*Penalty*” implies a “*Credit Amount*” that is discounted to the “*Payment Amount*”. This indemnification mechanism is very important; because it involves a compensation for the negative impact on consumer economy. Monitor algorithms must inform about services level changes and violations of contractual terms, before applying any compensation. Cloud providers know through “*Penalty Level*” about the importance and criticism of cloud capabilities in consumer business processes.

2.3.3 *Compliance Dimension*

Cloud governance and security can be considered the trend topic nowadays [21]. They are also considered challenges, because users no longer have control over the complete system. *Compliance Dimension* specifies legal information, security methods, and service compliance with standards, agreement terms, procedures, and law. Figure 2.4 shows the conceptual model of *Compliance Dimension*.

“*Governance*” implies a collection of compliance attributes, norms, and certifications. “*Standard Compliance*” has the information about standards that service contract has to conform in order to attain the agreed service level and quality. “*Standard Type*” details the scope of the standardized norms, and it can be focused on communication, virtualization, security, green computing, cloud federation, data interoperability, and syndication. “*Certification Compliance*” specifies information about international certifications that determine capabilities in cloud computing. Certifications and standards are used to formalize security and technical aspects of a procurement agreement, and they ensure that business objectives are met while meeting compliance requirements (e.g., TOSCA, OCCI, OVF, SOAP, ISO 14000, Green Star, HIPAA, PCI, SAS70, FISMA, SSAE16, SCOC1, SCOC2, ISAE3402, IS027001, etc.). “*Legal Compliance*” and “*Security Compliance*” are contractual agreements that covers data protection and laws application in cloud computing. Legal experts can infer internal and external security risks by considering those

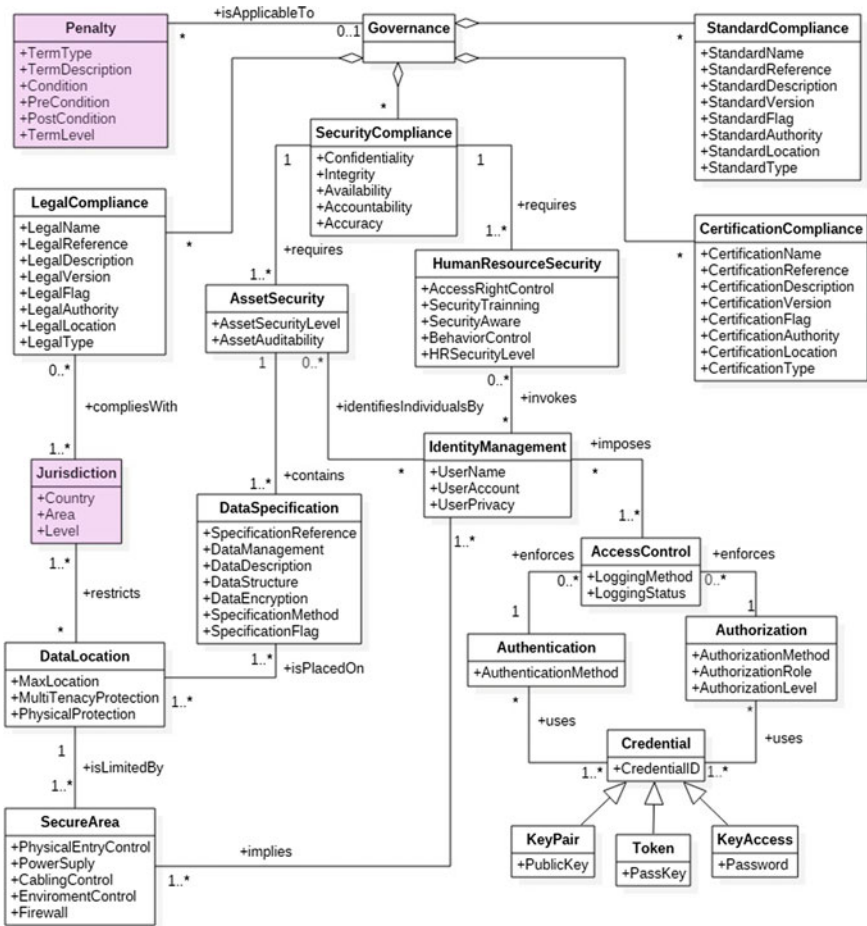


Fig. 2.4 Conceptual model of cloud compliance dimension

compliance terms. “*Legal Type*” specifies terms of uses (ToU), terms of service (ToS), user licensing agreement (ULA), intellectual property clauses, copyright terms, acceptable use, and other legal aspects that limit responsibilities and rights about cloud services. Finally, “*Penalty*” represents the conditions and the compensation when those established governance terms are not met.

“*Security Compliance*” saves information about levels of confidentiality, integrity, availability, accountability and accuracy, and it requires terms for “*Human Resource Security*” and “*Asset Security*”. “*Human Resource Security*” demands human resources and employers to provide required security level, and some security triggers are created in other to monitor their behaviors. This entity includes all security measures for avoiding internal attacks and unauthorized accesses.

“Identity Management” uses account and name to identify individuals, and it imposes *“Access Control”* to restrict entrance (physically or logically) to the resources and applications.

“Access Control” put into effect *“Authentication”* and *“Authorization”* by granting access based on *“Credential”*. *“Credential”* is a security binding and the most common type of credential are *“Key Pair”*, *“Token”*, and *“Key Access”*. Control algorithms compare credential to an access control list, grant or deny accesses to cloud resources, and keep transaction logs. *“Secure Area”* is a trust location where facilities are installed and capabilities are deployed.

Data are particularly heterogeneous due to the fact the number of databases and files for specific operations [9], thus providers should indicate the efficiency of data management preventing security breaches in runtime [6]. *“Data Specification”* is the entity in the conceptual model that contains all information about data manipulation and management. *“Data Management”* is about data store, data transfer, data regulation, data governance, data portability, data migration, data protection, data controller, data security (i.e., mechanisms for availability, integrity, confidentiality, authentication, and non-repudiation), data access (i.e., mechanism for accounting, credentials, and security logs), data recovery, data backup, data replication, data persistency, data deletion (e.g., right to be forgotten), data sanitization, data preservation, data import and data export.

“Data Location” is limited by *“Secure Area”* and *“Jurisdiction”*. Service consumer and service provider should divide their attention to the jurisdictions over the contract terms (i.e., where signing parties come from) and the jurisdictions over the data is divided, subcontracted, outsourced, collected, processed, and transferred; because each jurisdiction has laws and restrictions. However, *“Jurisdiction”* and its law applications depend on the physical location of the data [21]. If the data is replicated to other countries, *“Legal Compliance”* terms must compliance with one or more *“Jurisdiction”* instances. Before adopting cloud services, *“Service Consumer”* must agree to know and respect jurisdiction laws and legal policy wherein the data is physically stored.

“Support for Forensic” is referenced to *“Legal Compliance”*, and it is the reserved right of the service provider to make available evidences, user data and process to external government and to collaborate with its investigations [2, 21]. Moreover, all compliance terms are guidelines for security, manipulation and visualization of data and workload in cloud environments.

“Data Encryption” is part of *“Data Specification”* and it is increasingly relevant for cloud computing. Data should always be encrypted considering *“Data Structure”* and *“Data Description”* in order to evade external intrusions and data leakages. There are many mechanisms for encryption and *“Service Provider”* generally offers an API for this process [21].

Compliance Dimension represents an analysis of governance terms in cloud contracts. It covers regulations and agreements to ensure that cloud service do not breach security policies and laws imposed by the jurisdictions.

2.3.4 Operational Dimension

Operational Dimension covers requirements about service management and business continuity. This dimension ensures that service workload and data are continuously available or not disrupted for longer than is permissible. Operational tasks are defined in this approach as service maintenance, service recovery, systems powering, systems update, scaling up, and scaling down. Figure 2.5 shows the conceptual model of *Operational Dimension*.

“*Service Description*” is the most important entity in this conceptual model, because it specifies the requirements and capabilities of cloud services. “*Service Description*” indicates relevant information about “*Service Model*” (i.e., Software as a Service, Platform as a Service, and Infrastructure as a Service), “*Deployment Model*” (i.e., Public cloud, Private cloud, Community cloud, and Hybrid cloud) and “*Provisioning Model*” (i.e., on demand, static Provisioning, or dynamic

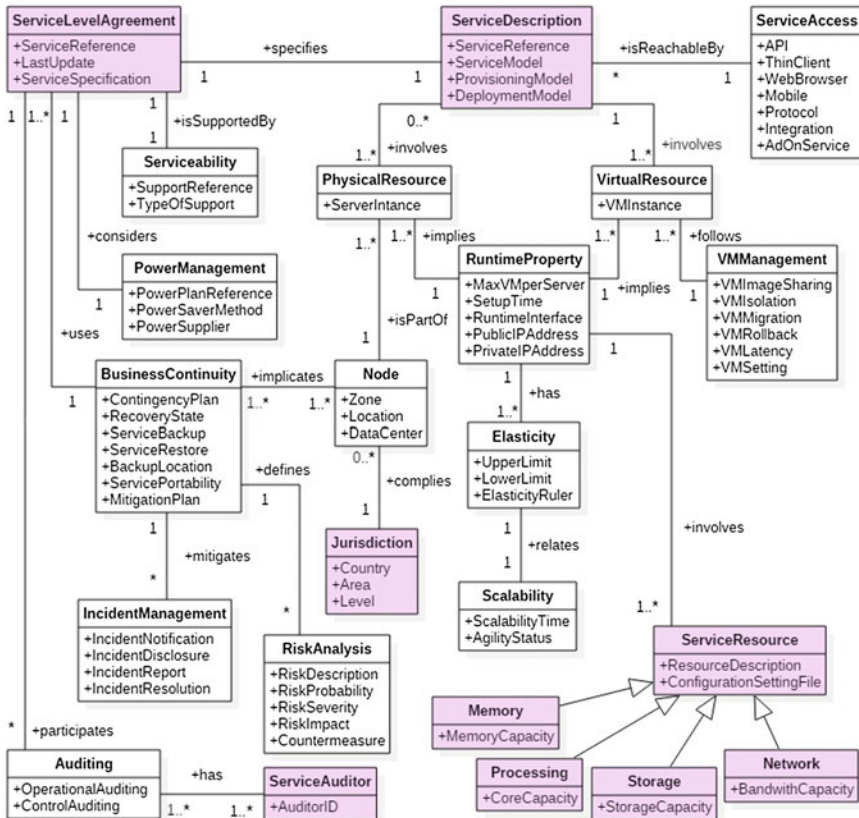


Fig. 2.5 Conceptual model of cloud operational dimension

provisioning of resources). The service is reachable by “*Service Access*” that describes the access mechanisms to use the services.

“*Service Level Agreement*” specifies “*Service Description*” that involves “*Physical Resource*” (i.e., servers, data center) and “*Virtual Resources*” (i.e., virtual machines). The features of those resources are stored in configuration files, and they indicate the setting of each instance. “*VM Management*” covers the information about virtual machines (VM) with the aim of assurance isolation and scalability.

“*Runtime Property*” is the entity that contains information about load balance and service runtime. “*Runtime Property*” manages “*Service Resources*” that are specific service features, such as “*Storage*” (i.e., database, files), “*Processing*” (i.e., CPU, cores), “*Network*” (i.e., bandwidth, switches), and “*Memory*” (i.e., cache and RAM). Load balancer dynamically distributes data and workloads across multiple computing resources for enhancing the overall performance of service.

Operational Dimension cares about growing the number of resource during period of peak demands and resource updating. Resource capacities change over time due to capability demands. Thus, “*Runtime Property*” has “*Elasticity*” properties that are related to “*Scalability*”, and those entities specify the “*Upper Limit*”, “*Lower Limit*”, “*Scalability Time*”, and “*Elasticity Ruler*” (i.e., triggers and events that change service capacity). In case of peak demands, “*Elasticity*” indicates “*Upper Limit*” of provisioning resources to meet the current need. After the peak load, “*Elasticity*” indicates “*Down Limit*” of decreasing unused resources. Unused resources are released and available in the resources pool that keeps resources active and ready to be used anytime.

Operational Dimension aims to keep the service running and available. Thus, disruption, disaster, peak loads, and peak demands have to be resolved. Consequently, “*Service Level Agreement*” is supported by “*Serviceability*” that has all information to technically support tasks and operations in the cloud. “*Power Management*” is also considered and it administrates power energy and saver methods.

Usually, service providers limit their actions and responsibilities in the presence of force majeure, external suspension, or criminal attacks. However, “*Business Continuity*” is attached to “*Service Level Agreement*” and it considers a contingency plan and evaluation of threats and risks. It also implies “*Node*” and “*Jurisdiction*”, because those have impact into “*Risk Analysis*” and “*Incident Management*”. Moreover, services can be allocated in places where natural disasters or cybercrimes often occur, so those location statistics impact risks and threats analysis (e.g., accidents, security attacks, restrictions imposed by public authorities). Finally, “*Auditing*” driven by “*Auditor*” verifies that services and resources are appropriate and adequately controlled to ensure the service level presented in the agreements.

2.3.5 Technical Dimension

Technical Dimension is about technical metrics and measurements. It aims to verify that the results of measurements are over the acceptance values and service level objectives are met, consequently the promised quality of service has been achieved. Figure 2.6 presents the proposed conceptual model for *Technical Dimension*.

In the conceptual model, “*Service Level Agreement*” specifies “*Service Description*” that involves several “*Service Resources*” (cardinality is “1..*” and means “one or more”). “*Service Resource*” has a “*Configuration Setting File*” that indicates all features and configurations of the resources. This service configuration file can be thought of as “web.config” or “app.config” or “config”.

“*Service Level Agreement*” is associated to “*Service Level Objective*” that contains “*Service Level Target*” of the deployed service. “*Indicator*” is about “*Service Resource*” and it utilizes “*Metric*” to calculate “*Actual Value*”. “*Metric*” has a measurement method and measurement scale, which is used in relation to a quantitative service level objective and it can be composed with other metrics, similar to

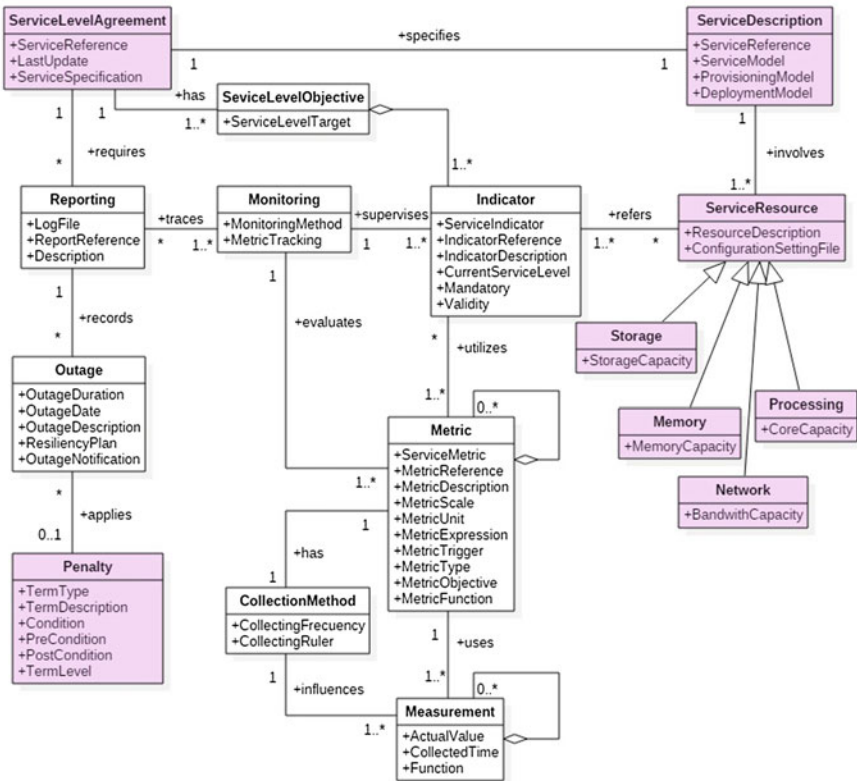


Fig. 2.6 Conceptual model of cloud technical dimension

“*Measurement*”. “*Collection Method*” specifies the “*Collection Frequency*” (e.g., every day, after processing data, etc.) and “*Collection Ruler*” (e.g., when an external event occurs, metric collects value). Each service can have associated one or more metrics, and metrics can be associated to a simple value or a collection of values.

“*Monitoring*” supervises “*Indicator*” instances of the measured service, and “*Reporting*” records “*Outage*”. When “*Outage Notification*” is critical, “*Penalty*” is applied, because service is under the “*Service Level Objective*” and the “*Service Contract*” is violated. Service provider should offer adequate access to carry on measuring and monitoring of services deployed into his infrastructure. There are many service key indicators (e.g., performance, availability, reliability, agility, etc.) and diverse metrics for measuring indicator values (e.g., processing throughput, network throughput, bandwidth speed, instance speed, computing speed, response time, recovery time, resolution time, upload time, download time, connecting time, boot time, reboot time, scale up time, scale down time, request per minute, uptime, downtime, etc.). Metrics provide knowledge about capabilities of a cloud service and it is very important to support decisions in order to satisfy service level requirements.

Key indicators are not explicitly defined in the model, because they mostly depend on service level agreements. Moreover, some authors point out that the indicator “*Performance*” is only measured by the metric “*Service Response Time*” [11] and others specify that the indicator “*Performance*” is calculated by the metric “*Page Down Load Rate*” [5]. Moreover, there are many attributes regarding to quality of service and key performance indicators in cloud computing that express almost same requirements but using different expressions, metrics, and restrictions (e.g., availability and reliability). The list below explains the most common indicators and their associated metrics.

- *Accountability* is a group of quality attributes used to evaluate whether data is handled according to service consumer requirements and is protected in the cloud. It is associated to measure and score services, and it is related to compliance, transparency, control, and auditability of the services [11].
- *Agility* represents how quickly new capabilities are added to adjust the amount of demands and also resources scale. It is related to elasticity, portability, adaptability, and flexibility [11]. It can be measured considering capacity of CPU, memory, and time to scale up and scale down service resources.
- *Assurance* indicates that service is securely delivered in accordance to the SLA and service consumer expectations. It involves availability, stability, serviceability, reliability, and resiliency [11].
- *Availability* is typically measured by the probability that service is active when needed. It is used as an indicator of the percentage uptime, considering the downtime due to faults and other causes, such as planned maintenance and upgrading. It can be also presented as a redundancy method for masking errors and faults. It is measured considering uptime of the service in specific time (e.g., 99.99% uptime per month) [2].

- *Performance* is probably the most common indicator in cloud computing, and there are many solutions to calculate in terms of functionality, time, and resource processing. Depending on the context, performance can be metering by time to complete and receive the process request (service response time), amount of data that can be recuperated from the system in specific unit of time (throughput), or capability to meet deadlines (timeliness) [2].
- *Scalability* describes the aptitude and the time to increase or decrease storage space, and growth or reduction of workloads. It is associated to Elasticity that is the illusion of unlimited resources. Scalability can also be measured by considering maximum of virtual machines for account (scale up), minimum of virtual machines for account (scale down), time to increase a specific number of resources, and time to decrease a specific number of resources, boot time, suspend time, delete time, and provisioning time [2].
- *Usability* is complex to measure because it indicates how practical is to use and consume cloud services. So it depends of cloud users and subjectivism. It is related to accessibility, learnability, and operability [11].

In summary, the proposed conceptual model is useful to identify relevant information about cloud service, but service provider and consumer should clearly indicate what to consider an indicator and what metrics are relevant to measure it.

2.4 Sample Scenario: The Security Guard Company

The sample scenario about the Security Guard Company was introduced for the first time in this project in the approach about dynamic requirements of cloud computing [27], and it is extended in this contribution for explaining cloud dimensions. The Security Guard Company offers a catalog of real-time security modules to its clients in South America, in order to solve the weakness and vulnerabilities of the local public security services. Moreover, the company significantly reduces clients' on-site staff costs by automating security controls in small and large-scale installations.

The Security Guard Company has deployed an integrated system that enables entrances and exits monitoring of buildings, rooms, and parking lots. The system integrates sophisticated digital video cameras, smoke sensors, motion sensors, temperature sensors, and algorithms of face recognition and car patent recognition. The video cameras and sensors are strategically installed in spots of the client facilities, and the incoming data of those devices are recording in the company data center. The company remotely monitors multiple buildings, and some triggers are executed to send notification to clients, local police office, fire station, and emergency medical services. Additionally, the clients can visualize multiple cameras and sensor status in a single interface. The system notifies relevant events to clients using mobile apps, text messages, and email notifications.

The company has grown exponentially in the last months, and it decides to reduce costs by moving all video records and control data older than 6 months to a cloud server, because those videos are not regularly consulted. It also decides to keep the complex security system on premise into the company data center in order to avoid security threats and to regularly update software modules.

Finally, Amazon Simple Storage Service (Amazon S3) is picked after comparing multiple services to find the best one in regard to cloud dimension in South America. Amazon S3 provides secure, durable, highly scalable cloud storage, and it also takes account of backup, recovery, near-line archive, big data analytics, disaster recovery, and content distribution. The relevant terms are extracted from requirements document file and service offers, in order to pick the best service for the given scenario. Some terms of the cloud dimension are completed during the service specification (e.g., pricing method, price currency, term description) and others, during the service runtime (e.g., storage cost, cost reference, capacity).

In the service specification, some entities of *Contractual Dimension* explained in Fig. 2.2 are clearly identified in Amazon Web Service Agreement (AWS Agreement), Amazon S3 agreement and the consumer requirements. The “*Subject*” of the contract is storage capacity, the “*Service Reference*” is named “*Amazon S3 Standard*” and it is based on the “*Service Level Agreement*” updated on “*September 16, 2015*”, in the provider’s website. The information of service provider is “*Amazon Web Services, Inc.*,” and its address is “*410 Terry Avenue North, Seattle, WA 98109-5210, USA*”. Some of the “*Contractual Term*” detected in the SLA are mostly about suspension or termination when maintenance, force majeure events, unavailable internet access, demarcation point, action or inaction of third part and failure of equipments, software or other technology under control of consumer or third part take place. “*Penalty*” is only considered when a claim of outage is sent from the consumer to Amazon Web Service, Inc. Finally, other “*Contractual Term*” specifies the right of the service provider to change any term with no less than 90 days advance notice. It is required 30 days advance notice prior to service termination, and 30 days are required not to erase any content after termination date.

About *Financial Dimension* showed in Fig. 2.3, it is clear that payment method is “*pay-per-use*” and the billing is released “*monthly*”. Penalty terms take places when “*monthly update percent (MUP)*” is less than “*99.95%*” and the refund is about “*10–30% in credit*” to the service consumer. One “*Credit*” is equivalent to “*1 USD*” and the “*Credit Amount*” can only be used in the next payments. All money transactions use credit card accounts in Amazon Web Service, Inc., so the Security Guard Company should indicate a credit card number in the “*Billing Account*” and “*Payment*”. The company credit card will automatically be charged for that month’s usage. The service pricing is complex, because it depends on service reference (e.g., Amazon S3 standard, Glacier), region (e.g., South America, USA, Europe), gigabytes per months, data transfer (i.e., IN and OUT) and requests type (i.e., put, copy, post, list, get). However, the provider offers an online calculator for billing calculus (e.g., “*cost reference*” for “*data transfer out from Amazon S3*” in “*South America*” is between “*\$0.250 and \$0.230 per GB*”). Delete requests are always free.

Entities of *Compliance Dimension* presented in Fig. 2.4 are often referenced in AWS Agreement in different parts, because the provider offers many mechanisms for “Data Encryption”, “Access Control”, and “Data Specification”. Some available options for “Access Control” are: (a) “AWS identity and Access Management (IAM)” that grant IAM users fine-grained control to bucket or object; (b) “Access Control Lists (ACLs)” that selectively grants certain permissions on individual objects; (c) “Bucket Policy” that grants permission across some or all of the objects within a single bucket, (d) “Query String Authentication” that shares object through URLs on a specified period of time, and (e) “Virtual Private Cloud (VPC)” that uses provider network to transfer data in multiple levels of security control. Some “Data Encryption” methods are: (a) Server-Side Encryption with Amazon S3 Key Management (SSE-S3) using Advanced Encryption Standard (AES) 256-bit symmetric key, (b) Server-Side Encryption with Customer-Provided Keys (SSE-C) using Advanced Encryption Standard (AES), and (c) Server-Side Encryption with AWS Key Management Service (KMS) (SSE-KMS) that provides an audit trail and control to comply with PCI-DSS, HIPAA/HITECH, and FedRAMP industry requirements. For authentication method, the “Multi-Factor Authentication (MFA)” and “Authentication Device” are the alternatives in this service. For data transference, SSL encryption of data is the basic method for data in transit using HTTPS protocol, and Bit Torrent Protocol is also available in the cloud provider environment. In “Multitenancy Protection”, Amazon S3 uses a combination of Content-MD5 checksums and cyclic redundancy checks (CRCs) for assuring data integrity. The service should also comply with Apache Software License or other open source license.

The contract “Jurisdiction” depends on the U.S. government rights respect with federal law. The “Jurisdiction” of the consumer is also part of the *Compliance Dimension*, as it is showed in Fig. 2.4, and tax exemption certificates depend on each consumer jurisdiction. The service “Jurisdiction” depends on the country on where the data is stored and processed, so Brazil is also a “Jurisdiction” implied in the agreements.

In *Operational Dimension* presented in Fig. 2.5, “Service Description” is specified as Infrastructure as a Service. The Amazon S3 instance is allocated in Sao Paulo, Brazil (South America Region), because it is the closest data center to the service consumer’s facilities. The node is called as “sa-east-1 (3)” into Amazon S3 environments. Sao Paulo is closed to the clients and this data center location enables the company to address specific legal and regulatory requirements. However, it is common that available backup is cross-region replication (CRR) and in two provider facilities. Elasticity and scalability are unlimited into this provider offer and “VM Management” uses XEN hypervisor in virtualization settings. Finally, the “Support” is free of charges, and any suggestion is confidential.

The last but not less important characteristics of the services are in the *Technical Dimension* showed in Fig. 2.6, and there are many instances for the attribute “Service Level Target” (e.g., “durability is equal to 99.999999999% in MUP”, “availability is equal to 99.99% in MUP”, “availability SLA is equal to 99.9% in MUP”, “first byte latency is equal to milliseconds”). Storage is measured by “total

byte hour usage”. “*Audit Logs*” are configurable and “*Reporting*” considers event notification and send alerts by Amazon SNS or Amazon SQS.

In conclusion, cloud dimension structure makes requirements specification and service specification more efficient than using other methods. Amazon S3 Standard is considered the best solution to keep copy of files under the pricing model “pay-per-use”, especially when clients can ask for old video records anytime, however the company can define rules to automatically migrate Amazon S3 objects to Amazon S3 Standard—Infrequent Access (Standard—IA) or Amazon Glacier based on the age of the data. The Security Guard Company can save money in infrastructure and its clients can access directly to the data stored in the cloud server.

2.5 Conclusions

In this paper, traditional cloud definition framework is extended and five new dimensions are considered: (a) *Contractual Dimension*: contract trails that specify stakeholders, disclaims, and general agreements between parties; (b) *Financial Dimension*: economic aspects of cloud services that are involved in billing, pricing, and costs; (c) *Compliance Dimension*: regulations that restrict cloud services such as legal, standards, and proceedings; (d) *Operational Dimension*: characteristics that cover specifications about service management, deployment, and access control; and (e) *Technical Dimension*: measurable and technical factors that may need functions, values, constraints, metrics, and units.

Because of the stochastic and dynamic nature of cloud contexts, there is not a simple and standard procedure for managing requirements and matching them with service providers offers. Thus, conceptual models about cloud dimensions are presented in order to analyze requirements and capabilities of cloud services, and they can be used to understand them and negotiate agreements with service providers.

In conclusion, considering cloud service as a multifaceted component is a good starting point for handling the dynamism of cloud environment. Different experts can individually analyze those cloud facets and contribute with the contract negotiation. Moreover, the dimensions are very complete and flexible for adding new features, so they can be the bases for future proposals, models, and ontologies. The dimensions are the bases for defining SLA schemas and ontology to create a consistent SLA in machine readable format.

References

1. Abbasov, B. (2014). Cloud computing: State of the art reseach issues. In Application of Information and Communication Technologies (AICT), 2014 IEEE 8th International Conference on (pp. 1–4). IEEE.
2. Alhamad, M., Dillon, T., Chang, E. (2010). Conceptual SLA framework for cloud computing. In 4th IEEE International Conference on Digital Ecosystems and Technologies (pp. 606–610). IEEE.

3. Andrikopoulos, V., Binz, T., Leymann, F., Strauch, S. (2013). How to adapt applications for the Cloud environment. *Computing*, 95(6), 493–535.
4. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50–58.
5. Bao, D., Xiao, Z., Sun, Y., Zhao, J. (2010). A method and framework for quality of cloud services measurement. In 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE) (Vol. 5, pp. V5–358). IEEE.
6. Boampong, P. A., Wahsheh, L. A. (2012). Different facets of security in the cloud. In *Proceedings of the 15th Communications and Networking Simulation Symposium* (p. 5). Society for Computer Simulation International.
7. Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., and Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation computer systems*, 25(6), 599–616.
8. Carroll, M., Van Der Merwe, A., Kotze, P. (2011). Secure cloud computing: Benefits, risks and controls. In 2011 Information Security for South Africa (pp. 1–9). IEEE.
9. Copie, A., Fortiș, T. F., Munteanu, V. I. (2012, August). Data security perspectives in the framework of cloud governance. In *European Conference on Parallel Processing* (pp. 24–33). Springer.
10. Fabian, B., Gürses, S., Heisel, M., Santen, T., Schmidt, H. (2010). A comparison of security requirements engineering methods. *Requirements engineering*, 15(1), 7–40.
11. Garg, S. K., Versteeg, S., Buyya, R. (2013). A framework for ranking of cloud computing services. *Future Generation Computer Systems*, 29(4), 1012–1023.
12. Greenwell, R., Liu, X., Chalmers, K. (2015). Semantic description of cloud service agreements. In *Science and Information Conference (SAI)* (pp. 823–831). IEEE.
13. Heilig, L., Voß, S. (2014). Decision analytics for cloud computing: a classification and literature review. *Tutorials in Operations Research—Bridging Data and Decisions*, 1–26.
14. Karunakaran, S., Krishnaswamy, V., Sundarraj, R. P. (2013). Decisions, models and opportunities in cloud computing economics: a review of research on pricing and markets. In *Australian Symposium on Service Research and Innovation* (pp. 85–99). Springer.
15. Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., Leaf, D. (2011). NIST cloud computing reference architecture. NIST special publication 500–292.
16. Martens, B., Walterbusch, M., Teuteberg, F. (2012, January). Costing of cloud computing services: A total cost of ownership approach. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 1563–1572). IEEE.
17. Mell, P., Grance, T. (2011). The NIST Definition of Cloud Computing (Draft). NIST Special Publication 800–145.
18. Mouratidis, H., Islam, S., Kalloniatis, C., Gritzalis, S. (2013). A framework to support selection of cloud providers based on security and privacy requirements. *Journal of Systems and Software*, 86(9), 2276–2293.
19. Naveed, R., Abbas, H. (2014). Security Requirements Specification Framework for Cloud Users. In *Future Information Technology* (pp. 297–305). Springer Berlin Heidelberg.
20. Patel, P., Ranabahu, A. H., Sheth, A. P. (2009). Service level agreement in cloud computing.
21. Pichan, A., Lazarescu, M., Soh, S. T. (2015). Cloud forensics: technical challenges, solutions and comparative analysis. *Digital Investigation*, 13, 38–57.
22. Repschlaeger, J., Wind, S., Zarnekow, R., Turowski, K. (2012, January). A reference guide to cloud computing dimensions: infrastructure as a service classification framework. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 2178–2188). IEEE.
23. Rimal, B. P., Choi, E., Lumb, I. (2010). A taxonomy, survey, and issues of cloud computing ecosystems. In *Cloud Computing* (pp. 21–46). Springer London.
24. Suleiman, B. (2012). Elasticity economics of cloud-based applications. In *Services Computing (SCC), 2012 IEEE Ninth International Conference on* (pp. 694–695). IEEE.

25. Vaquero, L. M., Rodero-Merino, L., Caceres, J., and Lindner, M. (2008). A break in the clouds: towards a cloud definition. *ACM SIGCOMM Computer Communication Review*, 39 (1), 50–55.
26. Youseff, L., Butrico, M., Da Silva, D. (2008). Toward a unified ontology of cloud computing. In *2008 Grid Computing Environments Workshop* (pp. 1–10). IEEE.
27. Zalazar, A. S., Rodriguez, S., Ballejos, L. (2015). Handling Dynamic Requirements in Cloud Computing. In *Simposio Argentino de Ingeniería de Software (ASSE 2015)-JAIIO 44* (pp. 21–46). SADIO.

Requirements Engineering for Service and Cloud
Computing

Ramachandran, M.; Mahmood, Z. (Eds.)

2017, XVIII, 320 p. 80 illus., Hardcover

ISBN: 978-3-319-51309-6