J Supercomput (2014) 68:1321–1346
DOI 10.1007/s11227-014-1089-x

A systematic review on cloud computing

Frederico Durao · Jose Fernando S. Carvalho · Anderson Fonseka · Vinicius Cardoso Garcia

Published online: 31 January 2014

Abstract Cloud computing is an ascending technology that has introduced a new paradigm by rendering a rational computational model possible. It has changed the dynamics of IT consumption by means of a model that provides on-demand services over the Internet. Unlike the traditional hosting service, cloud computing services are paid for per usage and may expand or shrink based on demand. Such services are, in general, fully managed by cloud providers that require users nothing but a personal computer and an Internet access. In recent years, this model has attracted the attention of researchers, investors and practitioners, many of whom have proposed a number of applications, structures and fundamentals of cloud computing, resulting in various definitions, requirements and models. Despite the interest and advances in the field, issues such as security and privacy, service layer agreement, resource sharing, and billing have opened up new questions about the real gains of the model. Although cloud computing is based on a 50-year-old business model, evidence from this study indicates that cloud computing still needs to expand and overcome present limitations that prevent the full use of its potential. In this study, we critically review the state of the art in cloud computing with the aim of identifying advances, gaps and new challenges.

F. Durao (✉)
Computer Science Department, Federal University of Bahia, Salvador, BA, Brazil
e-mail: freddurao@dcc.ufba.br

J. F. S. Carvalho · A. Fonseka · V. C. Garcia
Informatic Center, Federal University of Pernambuco, Recife, PE, Brazil
e-mail: jfsc@cin.ufpe.br

A. Fonseka
e-mail: afs8@cin.ufpe.br

V. C. Garcia
e-mail: vcg@cin.ufpe.br

Keywords Cloud computing · Service layer agreement · Virtualization · On-demand business model

1 Introduction

Since the 1960s, researchers such as Douglas Parkhill and John McCarthy have focused their efforts on the development of a computing model named Utility Computing. The aim of this model is to provide users with services on the Internet that are similar to traditional utilities such as water, gas and electricity. In other words, users only need to have an Internet access so as to benefit from a variety of services such as file storage, deployment servers and online applications hosted by the organization's computers and devices over the Internet [53,55,63]. Moreover, this model has been adopted for several computing paradigms [10,49] and has also resisted harmful scenarios [13] such as information decentralization through Personal Computers (PCs) in the 1980s [2,5,29,66,82].

Nowadays, Utility Computing is named Cloud Computing [18] which has rapidly changed the dynamics of IT consumption through a model that provides on-demand services over the Internet to many users at any one time. As a key feature, consumers only pay for the services used and as offered by cloud providers that intelligently provide computing capabilities to quickly increase or decrease computing power as business needs change. Of late, this model has caught the attention of investors [22], researchers and practitioners due to its greater flexibility and availability at a lower cost [86]. Buyya at al. [10], for instance, envision that this computing model will one day be the 5th utility (after water, electricity, gas, and telephony) because it will provide users with the elementary level of computing service essential for meeting the everyday needs of the general population.

Although this scenario looks promising, there exist a number of open issues that threaten the very efficiency of Cloud Computing itself: (1) the conception of service contracts [40,51,59]; (2) the real economic benefits [42]; (3) the choice of a suitable software architecture to Software as a Service (SaaS) development [16,43]; (4) data privacy [86,96]; (5) the adoption of an agile process [30]; and last but not least (6) laws [20,24,62,81].

In an effort to investigate and promote advances in Cloud Computing, this study seeks to clarify and synthesize the available evidence as a way to determine key implications for practice as well as identifying research trends and new gaps. The remainder of the paper is structured as follows: Sect. 2 describes the research method used; Sect. 3 presents the main findings; Sect. 4 analyzes the results; Sect. 5 presents a discussion; Sect. 6 looks at the threats to validity; and Sect. 7 discusses the main conclusions.

2 Research methodology

The research methodology chosen for this research was a systematic review, for the reason that this is one effective way of identifying, evaluating, interpreting and comparing all available studies that are relevant to a particular question [41]. A process as

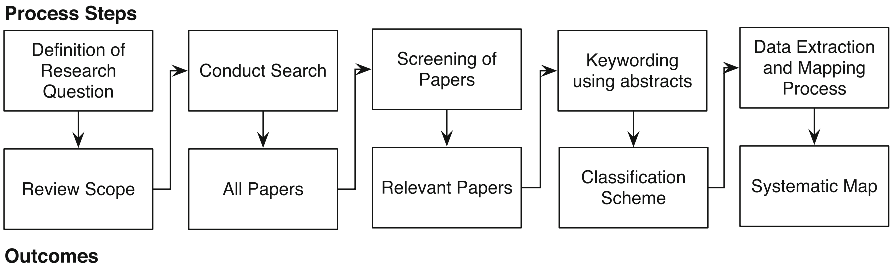


Fig. 1 The systematic mapping process [65]

such can lead to detailed answers within a specific scope. In this sense, we developed eight research questions to address the key concerns of Cloud Computing including economic aspects, service agreements, social impacts, architecture, scalability, storage, monitoring and security (Fig. 1).

2.1 Research questions

In the following, we will introduce the eight aforementioned research questions in order to address the most raised and considered open issues in the area of Cloud Computing.

- RQ1. Which challenges were identified with regard to economic problems?
  This aims at identifying factors that influence the adoption of Cloud Computing and Grid Computing, as well as the challenges faced by Service Providers (Cloud Providers) and Customers.
- RQ2. Which problems and solutions were identified with regard to SLA?
  The objective of this question is to understand the role of SLA in Cloud Computing, identifying its challenges and techniques used to ensure Quality-of-Service (QoS) in the environment.
- RQ3. What is the social impact of Cloud Computing?
  This question seeks to address issues such as possible government Cloud Computing usage, conflicts in laws, and impacts on citizens.
- RQ4. What are the challenges to service conception in Cloud Computing environments?
  This question is aimed at identifying the requirements and challenges towards the development of infrastructure and data center software (SaaS).
- RQ5. What are the main challenges regarding elastic property?
  At this point, the objective is to address techniques that refer to resource allocation in Cloud Computing.
- RQ6. What are the problems and solutions regarding data storage?
  The objective of this question is to address both the problems and techniques used to solve them.
- RQ7. How is resource usage monitoring carried out in Cloud Computing?
  This aims at understanding how resource usage monitoring is implemented in Cloud Computing as well as how it obtains tools and techniques.

– RQ8. What are the main security challenges?
  This aims at understanding issues related to data privacy in Cloud Computing environments.

To answer all these questions, an extensive literature review is made. Of the 827 studies reviewed, most of the answers were obtained from 301 publications. We collected information from conference papers, technical reports, journal papers, and books from several repositories such as the ACM Digital library, ScienceDirect, IEEE Xplore, EL COMPENDEX, SCOPUS, and DBLP.

3 Research findings on cloud computing

The outcome of this systematic review is presented in this section. The following subsections will look at the findings triggered by the eight research questions previously introduced.

3.1 RQ1. Which challenges were identified with regard to economic problems?

The economic conditions and the need to reduce costs have forced enterprises to consider the use of Cloud Computing [19]. This is because Cloud Computing promises to deliver all the functionality of existing IT services (and in fact enable new functionalities that are hitherto infeasible) even as it dramatically reduces the upfront costs of computing which used to deter many organizations from deploying many cutting-edge IT services [54,79].

In addition to lowering the upfront costs, organizations can also see that substantial investments have been grossly underutilized. This happens because their servers are only using 10 to 30 % of their available computing power, not to mention that desktop computers have an average capacity utilization of <5 % [54]. This economic issue extends to the science fields as well. In this particular case, the issue is associated with maintainability of scientific projects and prediction of costs at the start of those projects [32,42].

For Marston et al. [54], Cloud Computing opens up the competitive market to small businesses, as it allows for investment that can be made gradually due to the use of cloud facilities [42]. And although while cloud environments attract stakeholders due to the promise of low cost, there are technological alternatives which could be more interesting at least at the initial stage of Cloud Computing. Depending on the technical need, a Grid Computing [28,77] solution may be more appropriate given its maturity and existing solutions such as caBIG[1] and Earth System Grid[2].

A notable and relevant research was conducted by Woitaszek et al. [88], which examines the application of a billing model similar to the one used for cloud computing resources, including computational time, data transfers, and storage charging for their existing supercomputer. In order to generate break-even revenue on the Blue Gene/L,

[1] http://cabig.cancer.gov/.

[2] http://www.earthsystemgrid.org/home.htm.

Table 1 Grid computing vs. Cloud computing [87]

Criteria	Grid computing	Cloud computing
Virtualization	In its beginning	Essential
Type of application	Batch	Interactive
Development of applications	Local	In the cloud
Access	Via Grid middleware	Via standard Web protocols
Organizations	Virtual	Physical
Business model	Sharing	Pricing (utility model)
Control	Decentralized	Centralized (data center)
Switching cost	Low due to standardization	High due to incompatibilities
SLAs/liability	Not yet enforceable	Essential
Openness	High	Low

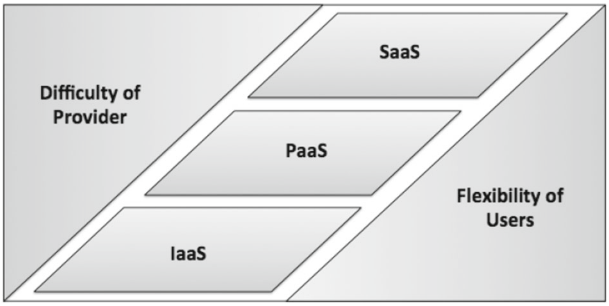


Fig. 2 Flexibility of cloud deployment models [73]

they argue that one would need to charge between 3 and 5 cents per CPU hour, a rate that cannot compete with the performance of current commodity processors available on modern cloud computing resources for applications not requiring a high-performance interconnect. Surprisingly, the analysis demonstrated that for applications run on their Blue Gene/L (supercomputer), charging for data transfers would only produce negligible revenue. The system planned for acquisition in mid-2010 will be substantially more cost-competitive than the outsourced EC2 computational and storage resources.

Needless to say, the choice between Cloud or Grid Computing as a new platform ought to be carefully made. Table 1 outlines some of the properties wherein Grid Computing differs from [87]. Kondo [42] recalls that the scientific project Amazon WS based on VC (Volunteer Computer) can reach 40–95 % saving costs when deployed in the cloud albeit with considerable costs involving bandwidth usage, which means that real savings can only occur when the system works with <10 TB in storage.

The flexibility made possible by cloud deployment models also requires attention. While customers may require a high level of flexibility in terms of a particular service from a Cloud Provider [1,70], enabling this flexibility can be a difficult task depending on the adopted service model: Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS)[3]. Figure 2 illustrates this scenario.

[3] http://searchcloudcomputing.techtarget.com/definition/cloud-computing.

According to Shi et al. [73], from a Cloud Provider's perspective, it is more viable to customize an IaaS because it provides resources such as storage space, processing and bandwidth. On the other hand, customizing SaaS is a more difficult task because the requirements for a customer may not be possible to implement in that software. It is important to remember that choosing a certain degree of customization for a particular service model will modify its original business model for the same service. Otherwise, the provider will not obtain the desired profit from its provided solution. According to Schuff and Altaf [71], due to the lack of techniques for adapting to a specific service, Cloud Providers remove features and other elements of the application in order to reduce costs and to ensure that Small and Medium Enterprises (SMEs) have access to that service. This practice also constitutes a barrier to solutions being adopted in Cloud Computing.

In the context of Private Clouds, choosing the proper technology can be a great ally in the effort to reduce costs in cloud environments. In [20], the Pandora Planning System (People and Networks Moving Data Around) is one such effort to minimize costs over the sending of large datasets among remote servers by providing a way to automatically choose between sending data over the Internet[6] and shipping them in physical hard disks. Thus, if the Pandora algorithms point towards sending the data in a hard disk, the system communicates this to a shipping service (in this particular case, FedEx) which then ships it. Otherwise, the data will be sent via the Internet.

3.2 RQ2. Which problems and solutions were identified with regard to SLA?

Service layer agreement (SLA) is a formal negotiated agreement between a service provider and a customer, and its terms refer to the quality and responsibilities expected from each party. When used properly, the SLA should guarantee the following [38]:

- Identify and define customer needs;
- Provide a model for understanding;
- Simplifying complex issues;
- Reduce conflicts;
- Encourage dialog on any disputes;
- Eliminate unrealistic expectations.

Through the terms of the SLA contract, Cloud Providers declare the level of QoS according to their actual capability [52]. In this way, QoS becomes a decision factor for selecting the best Cloud Providers [80]. In this context, our research has identified considerable attention being devoted by the leading authors towards keeping QoS at an acceptable level [7,17,38,51,59]. The main challenge here is dealing with over-provisioning, so that it does not compromise the profitability of the Cloud Provider. This profitability is called business objective level (BOL) [80]. According to Nae et al. [59], the risk of not achieving the BLOs refers to the inability to keep QoS under control. Nae et al. therefore suggest a model that creates a virtual SLA for delegating tasks to the system elements to ensure QoS (see Fig. 3). Also, in an attempt to ensure QoS, Boloor [7] proposes a model that uses Weighted Round Robin (WRR) and First In First Out (FIFO) algorithms to schedule data that come from geographically-

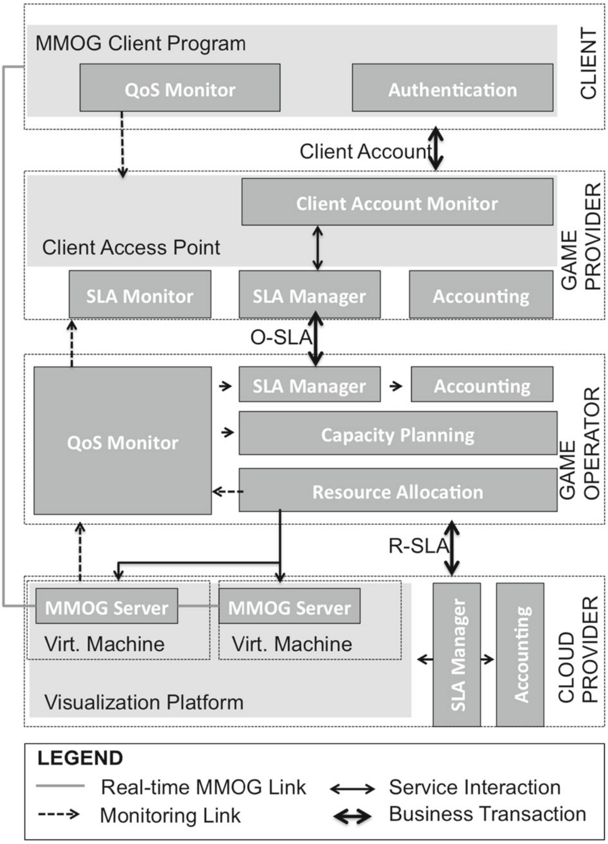


Fig. 3 Virtual SLA among system elements [59]

disposed servers. This approach intends to organize the data requests so as to deliver the respecting limits of SLA terms.

We also identified warnings about bad practices such as submitting false information (better response time, high availability) merely to attract the customer's attention [80]. In addition, some authors argue over the lack of clarity in terms of contracts [7,38]. To cope with such an inconvenience, [38] suggest several questions to be double-checked before agreeing to any contract:

- In terms of availability (99.9 %), can the Cloud Provider sign an SLA?
- What happens when there is a breach of contract?
- How do I get my data at the end of the contract and what kind of data will be returned?

As to data privacy, Kandukuri et al. [38] suggest the following questions:

- What level of data security level is being implemented at the physical layer and network servers?
- What about investigation support?

Table 2 Cloud advantages from interaction perspective for e-Gov [98]

Criteria	Product
Efficiency	Provides uniform access to data and applications
Effectiveness	Improves data quality
	Improves quality of services
Strategic benefits	Provides uniformity of solution
	Introduces new services
	Integrates existing infrastructure deployments
Transparency	Constant evaluation and control of services and application usage, reduction of expenses

– How safe is the data from natural disasters?
– How trustworthy is the encryption scheme of the Service Provider?

The above-mentioned questions are aimed at helping customers avoid entrapments before signing an SLA contract. In the following, we analyze the social impacts of Cloud Computing.

3.3 RQ3. What is the social impact of Cloud Computing?

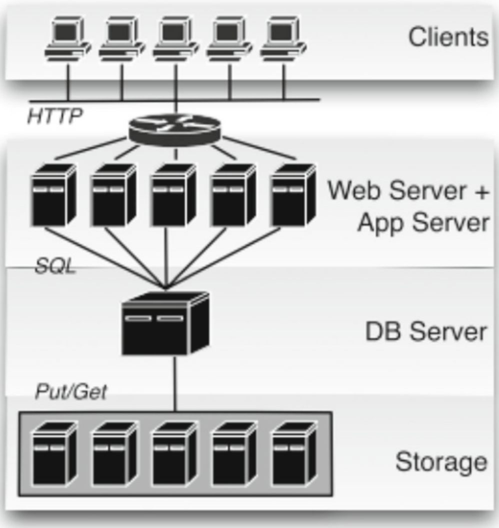
As to its social impacts, [24,81,83] point out that Cloud Computing faces running afoul of governmental laws. In particular, Taylor et al. [81] affirm that data pushed to cloud repositories could be encrypted before entering the cloud environment and could thus be deviated for personal interest. Further, the stored data could be disposed between countries. In Germany, the Federal Data Protection demands that the customer must know the location of his/her data even though cloud providers can store data anywhere [20]. In [96], other conflicting issues are presented such as Health Insurance Portability and Accountability (HIPPA), Electronic Communications Privacy (ECPA), and USA Patriot (UPA). On account of these, some commentators such as [24] and [83] have suggested a number of changes to both country laws and cloud computing security policies.

Zissis and Lekkas [98] affirm that the migration of public datasets to a cloud environment should produce positive results, both for the government and its citizens. In addition to reducing delays in the procedures of a public layer, the authors also outline a number of benefits, as described in Table 2. Besides the advantages presented by Zissis and Lekkas, the adoption of Cloud Computing by governments can foster the creation of a new market geared to such a context. An interesting viewpoint was found with respect to Green IT and Cloud Computing. In Baliga et al. [3], they reported that energy savings do not occur in all cases. The authors relate that under certain circumstances, Cloud Computing can consume more energy than conventional computing. Behind this assertion is the amount of energy spent to maintain the entire cloud infrastructure, from its own servers until the end customer.

3.4 RQ4. What are the challenges being faced by SaaS architectures?

For Cadan et al. [21], SaaS architectures can be classified into four maturity levels in terms of their deployment customization, configurability, multi-tenant efficiency, and

Fig. 4 Classical database architecture [43]

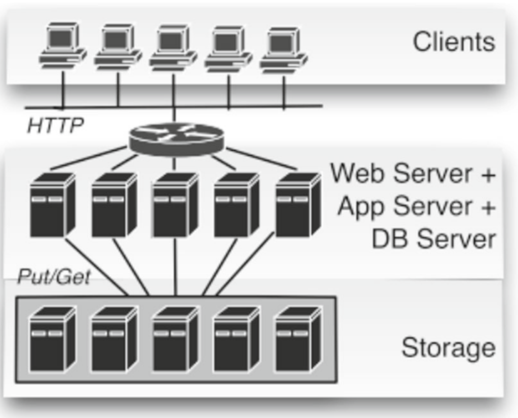


scalability attributes. At the first level of maturity, the customer has his/her own application instance hosted on a cloud server. Customer migration from his/her traditional non-networked or client-server application to this level of SaaS typically requires the least development effort. At the second level, the keyword is metadata. In holding a configurable metadata, it is possible to provide a flexible application instance for each customer. This approach will allow the vendor to meet the different needs of each customer through detailed configuration options, while at the same time simplifying maintenance of the common code base [11]. The third level refers to multi-tenant efficiency. At that point all customers stay on a unique instance of the application, but with each one being treated as a *tenant*. This approach allows for a potentially more efficient use of server resources without any apparent difference to the end user. For [11], at the fourth level, explicit scalability features are added through a multi-tier architecture that support a load-balanced farm of identical application instances, running on a variable number of servers.

According to Bonetta and Pautasso [8], the dynamic nature of Cloud Computing and its virtualized infrastructure pose new challenges in terms of application design, deployment and dynamic reconfiguration. In their work, Bonetta and Pautasso present a novel parallel programming model called Liquid Architecture. This approach builds up application services that can be transparently deployed in multi-core and cloud-execution environments. It also utilizes the fundamentals of Representation State Transfer (REST) and its loosely-coupled components to exchange messages, thereby creating an auto-adaptive environment.

Figure 4 shows the classical architecture, and since the DB Server Layer comprises only one server, it can become a bottleneck in the future. To attenuate this problem, companies tend to acquire expensive servers to replace it. To reach scalability in that model, companies can insert new solid disks into the Storage Layer. As an alternative,

Fig. 5 Distributed control [43]



Kossmann presents other variations of the classical architecture which seem more suitable to cloud environments, as seen in Fig. 5. In this infrastructure, the cloud has high scalability even if there is always a certain cost involved. For instance, with the physical and logical growth of the system, the cloud environment cannot ensure resilience, consistency and availability. Another widespread and often referred to work for guiding stakeholders in the development of cloud architectures is the RESERVOIR framework [16,23,26,50], which consists of a multi-tier model, and the key difference is its ability to treat federate environment across different sites. For Rimal et al. [68], there are additional requirements that should be considered when it comes to developing a cloud environment. The authors break down the requirements into the following three: (1) cloud provider; (2) organizations; and (3) end-user (as shown in Fig. 6).

3.5 RQ5. What are the main challenges regarding elastic property?

A cloud is not much of a cloud if it is not elastic. The elastic property of the cloud, which enables it to expand and shrink based on demand is possible only with the proper planning of resource allocation. To deal with this issue, the load balancing mechanism [25,56] is commonly utilized to manage instances of application servers as shown in Fig. 7.

Another solution for resource allocation is proposed by [49], which uses a feedback mechanism for delivering computing resource. The mechanism analyzes the CPU, I/O and RAM memory usage as shown in Fig. 8. The *Target System* is a computing system deployed in a cloud environment managed by a controller. In order to achieve the desired objective of the Target System (accurate provisioning), the controller dynamically regulates the environment based on feedbacks received due to the difference between *Reference Input* and *Measured Output*. For Nair et al. [60], a *broker system* model can be a feasible way of delivering service according to SLA terms due to the existence of a component on the cloud environment that is responsible for allocating resources according to the contractual terms. In this sense, when a customer throws a request to the cloud provider, a broker system allocates the computing resource from

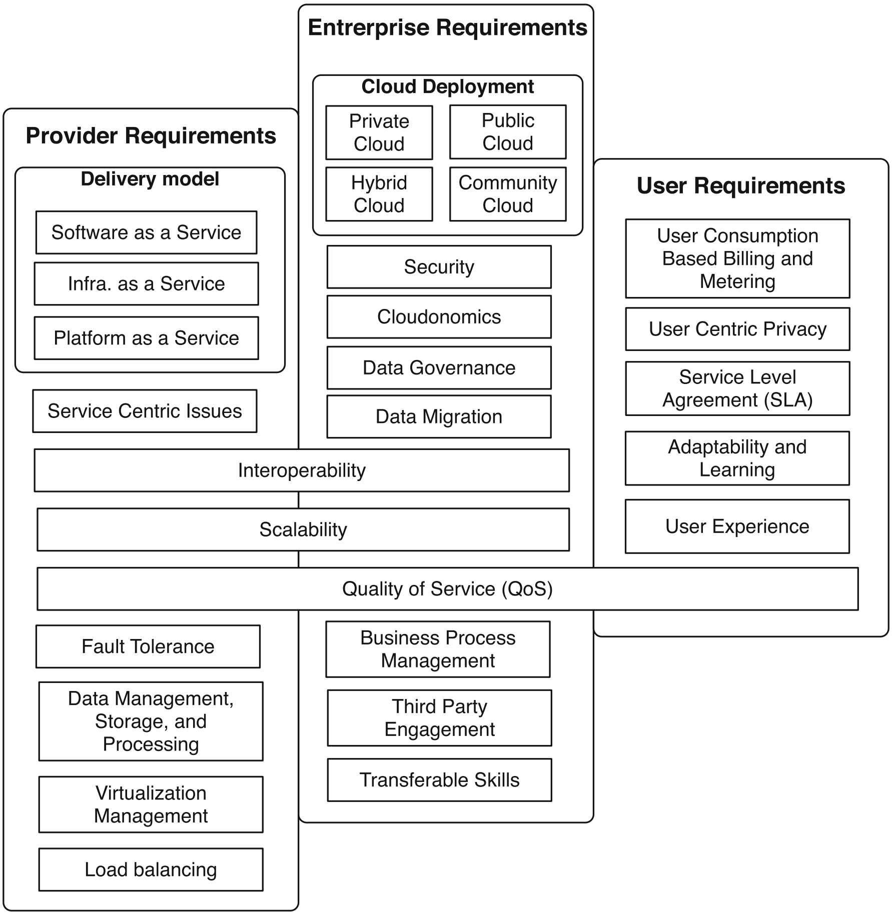


Fig. 6 Requirements for development of cloud environments [68]

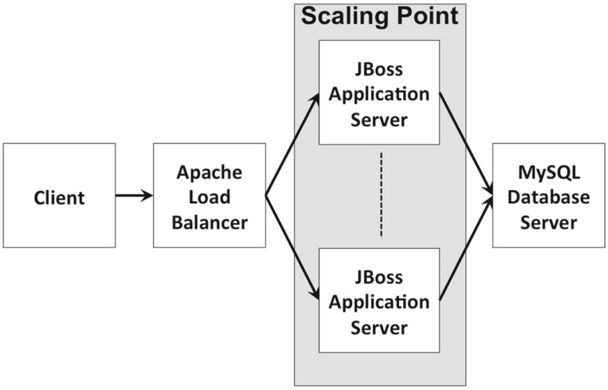


Fig. 7 Load balancer and scaling point [25]

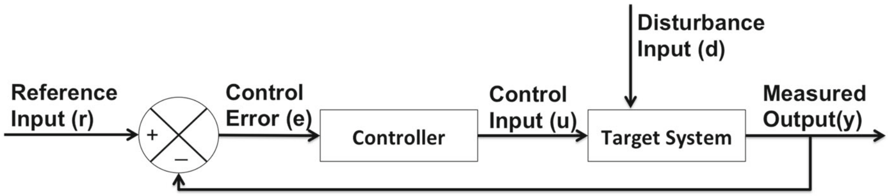


Fig. 8 A standard feedback control system [49]

a local farm. Otherwise, its resource will be allocated from a third company such as Amazon AWS, thereby causing cloud bursting. Similarly, another proposal to assist in resource allocation is *Prediction* [14]. This refers to the allocation of resources based on the future needs of the cloud environment. Besides Prediction, a cloud environment can predict the resource allocation based on similarity of occurred historic. In other words, a mechanism needs to analyze a scene that has already occurred on a cloud environment, and then prepare it to execute allocation at a future opportune moment in time.

3.6 RQ6. What are the problems and solutions regarding data storage?

The high amount of requests made to the storage system is a classic I/O problem of Cloud Computing [76,84]. To overcome this problem [93] suggest the development of an approach based on having a reservation time for requests. Whenever a user accesses the storage system during the reserved time, the requested performance is guaranteed because the storage system allocates the resources according to the reservation, and prioritizes I/O requests for the reserved access. Other alternatives to the data compression have been proposed; these have been intended not only to address the I/O issue but also the use of bandwidth [61].

Due to the huge data generated by people, systems, and companies, Cloud Computing is seen more and more as a solution for storing data. Nevertheless, Kozuch et al. [44] defend the notion that cloud storage systems utilize location-aware mechanism as a data storage technique. Such a proposal refers to the project TASHI which is supported by the Apache incubator. Another solution that has been popularly utilized is Hadoop MapReduce, which is a framework for writing applications that rapidly process vast amounts of data in parallel on large clusters of compute nodes [84,85]. Nevertheless, Kozuch et al. [44] caution that the Hadoop MapReduce framework can also affect software development in cases where some stakeholders intend to migrate their own software to that framework.

In order to guarantee the integrity of data on a cloud system, the environment needs to adopt a proof of integrity (POI) protocol [45,95]. Such a protocol would prevent the cloud storage archives from misrepresenting or modifying the stored data without the consent of the (data) owner through frequent checks on the storage archives. Nonetheless, Kumar and Sexena [45] emphasize that the POI protocol should be used with caution to avoid overhead on the system.

Table 3 Cloud providers monitoring control [78]

Level	SaaS	PaaS	IaaS
Facility (Fisical)	×	×	×
Network	×	×	×
Hardware	×	×	×
O.S.	×	×	?
Application	×	–	–
User	–	–	–

3.7 RQ7. How is resource usage monitoring carried out in Cloud Computing?

For Spring [78], monitoring is a major ally of both SLA and security in cloud environments. Spring also shows in Table 3 what the amplitude of monitoring control for cloud providers should be like.

According to Table 3, the (**x**) mark refers to the control through monitoring, the (**–**) mark represents unreachable elements and the (**?**) mark means that control of the monitoring scheme depends on the type of implementation on the element. For Elmroth and Larsson [26], two approaches can be used in the monitoring context. At first, the machines. The second is charged with observing statistics gathered from application modules such as the quantity of users logged or the life-time of threads. For such monitoring of usage, Table 4 illustrates the tools most commonly mentioned in the literature.

3.8 RQ8. What are the main security challenges?

According to Wayne A. Jansen (NIST) [86], the main challenges regarding security and privacy can be classified into the following sub-categories: trust, architecture, identity management, software isolation, and data protection.

3.8.1 Trust

It is important that both customer and cloud provider understand that by adopting the paradigm of Cloud Computing, the customer thereby delegates control of the security system to the service provider. Thus, to avoid creating gaps in the cloud environment, security policies, monitoring, processes and control techniques must be applied by the cloud provider's side [58].

3.8.2 Architecture

Security architecture challenges are directly linked to the care of elements of which it consists. In general, cloud environments consist of software components and hardware. Virtual Machines (VMs) typically serve as the abstract unit of deployment and are loosely coupled with the cloud storage architecture. Moreover, applications deployed in a cloud environment are usually created by intercommunication among components in the environment. On this issue, we found various proposals for safety models

Table 4 Used tools and frameworks for monitoring on Cloud Computing

Framework/tool	Description
GrenchMark	Framework for performance testing and analysis, system functionality testing, and comparing setting. Initially, the project was used for grid computing although there are evidences of its use in Cloud Computing
C-METER	An extension of the project GrenchMark adapted to Cloud Computing [91]
Monalytics	Framework for monitoring data, taking into account the scalability of the cloud. The author split the cloud environment into zones, allowing the monitoring only on interesting areas [46]
CloudClimate	Monitoring of cloud infra online. Agents are installed in environments cloud and perform tests of performance by sending the report to the project site
Grid monitoring architecture (GMA)	This framework is commonly cited as base to other monitoring extensions [26,33]
Push&pull model (P&P)	An approach based monitoring actions of the type Pushing and Pulling [33]
File system in user space (FUSE)	It is used for monitoring I/O access to the file system
Joulemeter	Monitoring of energy consumption of virtual machines [39]

of cloud architectures addressing efforts against intrusion [37,47], virtual network security models [90], and patching models [97].

3.8.3 Identity management

Data sensitivity, information privacy and unauthorized access to information resources in the cloud have increasingly become a major concern for organizations. One key reason for this issue seems to be a lack of cloud-driven frameworks that are specially focused on security [86]. In this context, Carelo et al. [12] propose an Access Control API for Cloud Federations, where a tuple is adopted for each stakeholder on a federation, as shown in Fig. 9. The approach adopts a RESTfull approach, where each resource on a federated cloud is accessed according to a 5-tuple structure and hierarchy. For example, a 5-tuple as in this next bracket (Paul, Mariah, Read, CloudStorage, /root/) means that Paul informs the system that Mariah has access towards reading the folder /root/of the CloudStorage service.

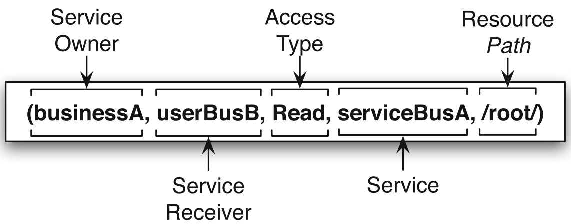


Fig. 9 Cloud federation access control API [12]

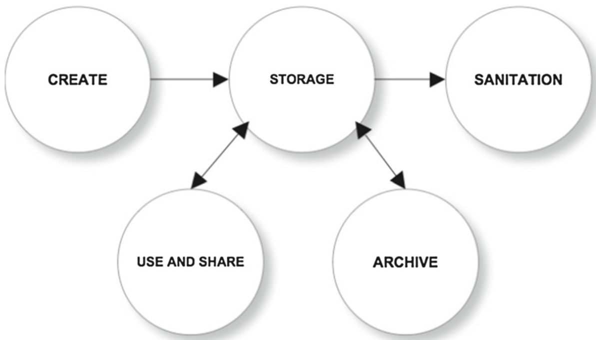


Fig. 10 The life cycle data model in cloud computing [92]

3.8.4 Software isolation

Multi-tenancy in Cloud Computing is typically done by multiplexing the execution of VMs from potentially different users on the same physical server [86]. In case an attack occurs on one user, the cloud provider must provide a security level that isolates only that particular client so that the others can keep working on your transactions without any interference.

3.8.5 Data protection

Data stored in the cloud typically resides in a shared environment, co-allocated with data from other customers. Therefore, organizations that move sensitive and regulated data into the cloud must account for the means by which access to the data is controlled so that it is kept secure [86]. In this sense, Yu and Wen [92] propose a data life cycle model as a way to follow all stages of user data as shown in Fig. 10. Additional efforts to protect data includes the use of cryptography [75], RSA algorithm [36], and kNN queries with cryptography [89].

In the following section, we shall demonstrate several correlations among the various suggestions, ideas and proposals from refereed authors already discussed in terms of addressing this study's research questions.

Table 5 Amount of studies vs. year of publication

2008	2009	2010	2011
5	55	202	39

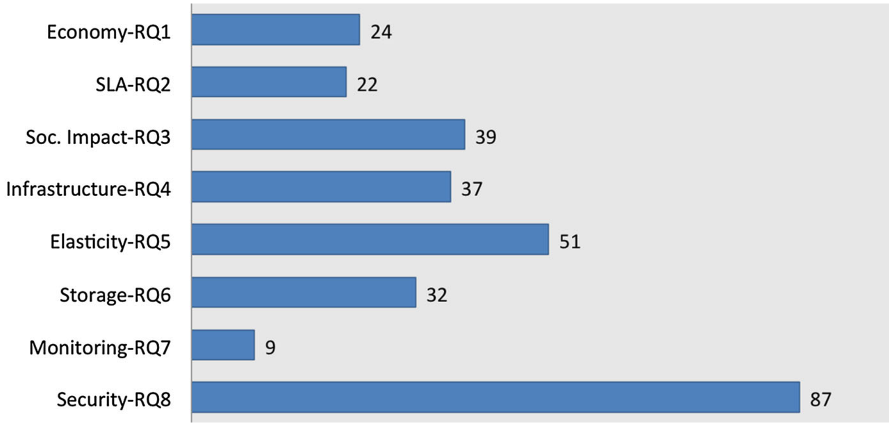


Fig. 11 Number of studies by research question

4 Statistical analysis of the systematic review

In this section, we correlate various studies on diverse topics, and analyze the research results from a broader perspective that is less question-oriented.

Table 5 shows the distribution of relevant papers per year of publication. As can be seen, most of the selected papers were published in 2010, and of these we outline the publications from the IEEE International Conference and Workshops on Cloud Computing Technology and Science (CloudCom), 4th edition, and the International Conference on Cloud Computing (CLOUD), 5th edition. Figure 11 presents the distribution according to the number of studies per research question. In particular, RQ7 (Monitoring) was addressed by the least number of studies, whereas RQ8 (Security) was the most addressed issue. Moreover, motivated by Petersen et al.'s [65] view, we adopted certain *aspects* associated with Cloud Computing, e.g. economy, infra, SLA and security, to classify our research material.

As shown in Fig. 12, all aspects are referenced in the research material with the exception of Cloud Monitoring, which has several occurrences over the observed period. This may have suffered from the influence of topics such as on-demand and elasticity of cloud environments that were smothered by a security "fever" in 2010. We also understand that another cause for the lack of further evidence on flexibility relates to the existence of proprietary standards and business values in such strategy. Concerning Security, as addressed in the RQ8 studies, it was mostly focused on mitigating risks regarding the adoption of Cloud Computing without overlooking its attractive promises. As to RQ2, studies warned about the penalties that Cloud Providers can pay if they do not comply with the proposed terms of SLA contracts such as the Quality Level of Service (QoS) [7]. In this resource management, the architectural aspect of

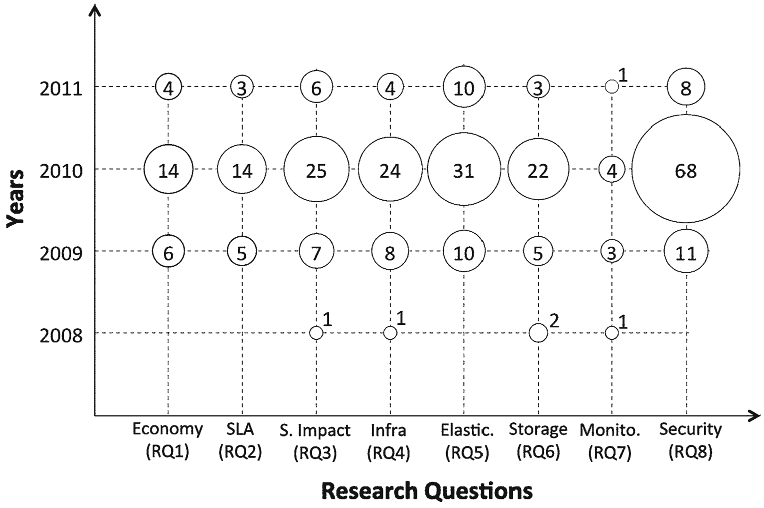


Fig. 12 Number of publication by year of each research question

Cloud Computing was taken into consideration because of its close relationship to that problem. Further, due to the attractive appeal of low-cost and new employment opportunities, the economic aspect was also a dominant factor in RQ3 (Social Impact).

4.1 SWOT analysis

In order to summarize the analysis in these studies, we created a S.W.O.T.[4] frame to evaluate the strengths [31,67,97], weaknesses [64,75], opportunities [3,32,67,98], and threats [24,81] relating to Cloud Computing. Figure 13 shows that multi-tenancy was added to the strengths because of the long-tail effect. In other words, the same infrastructure can meet the requirements for both organization and final user, besides making it profitable to the cloud provider.

5 Discussion

The traditional IT role of maintaining the corporate infrastructure and keeping systems updated as well as providing the first level of support to users, is fast dying out. For Ichak Adizes [35], the main factors in the death of enterprises during the first 5 years are:

– lack of planning;
– uncertainties about customers, suppliers and the market.

[4] http://www.sri.com/sites/default/files/brochures/dec-05.pdf.

STRENGTHS On-demand property [67]; User-Driven System [32]; Multitenancy [97].	**WEAKNESSES** Maturity stage [64]; Lack of a Taxonomy; Control of privacy [75].
OPPORTUNITIES e-Gov instruments [98]; Develop. of Green IT [4]; Science [67]; Diversity of XaaS [33].	**THREATS** Loopholes in laws [81][25]; Indiscriminate use of term; Unclearness of contracts.

Fig. 13 S.W.O.T. analysis of Cloud

According to Gartner[5], IT spends globally–from devices, services and data centers – about \$3.7 trillion in 2013 but this represents a shrinking growth of only 2 % on 2012, as more expensive items like PCs and on-premise software continue to get pushed out by less expensive ones. Cloud Computing is partially guilty once the pay-as-you-go business model enables companies of all sizes to have access to very powerful resources and solutions in a suitable way. Furthermore, the easy scalability of cloud services allows companies to feasibly optimize their costs based on usage levels instead of having to worry about peak demands.

Although some studies defend Cloud Computing for the reason that it can fit in as an element to control expenses, there exist some caveats. The studies of [42] and [72] claim that governmental applications are not yet suitable for the market because of limitations to resource provisioning and the lack of a clear business model being proposed by cloud providers. Additionally, Nae et al. [59] criticize the complexity relating to implementing cloud environments in comparison to conventional data center models. According to [51] and [17], service providers and customers need a good structured SLA contract. Otherwise, stakeholders may end up with serious problems of security, loss of privacy and other conflicts [38].

Moreover, cloud has enabled businesses to focus more on their business, and less on the technology required to run it. By outsourcing their basic infrastructure to cloud providers, companies no longer have to worry about upgrading and maintaining data centers and servers, leaving those to companies who are focused entirely on the technical aspects of such issues. The same goes for cloud applications, which allow companies to worry more about using the software and less about maintaining it and keeping it updated. Furthermore, by moving infrastructure and applications to the cloud, companies set themselves up to take advantage of future economies of scale that will most likely be on the side of cloud providers. For those companies that adopt cloud technologies, such developments mean that the cloud is rapidly making IT departments

[5] http://www.gartner.com/newsroom/id/2537815/.

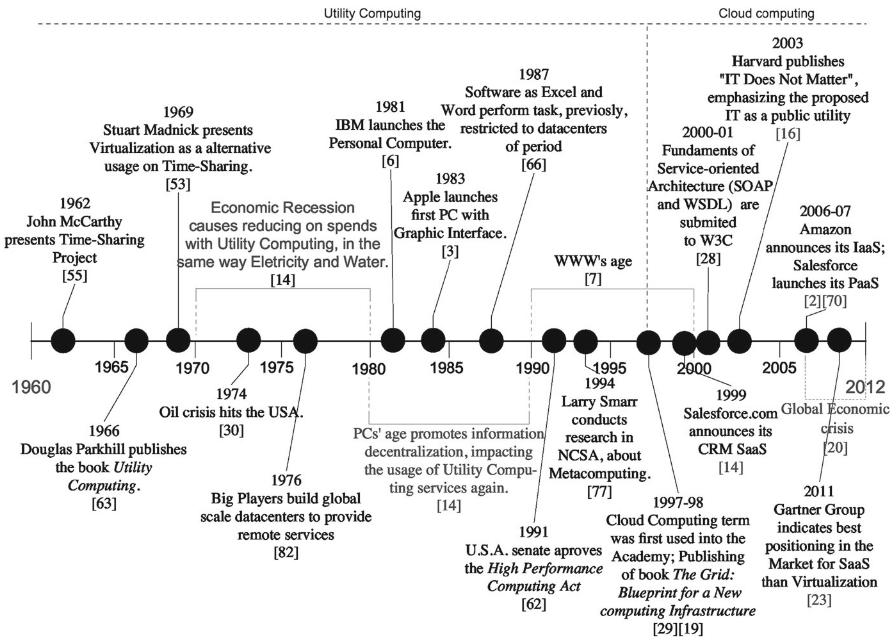


Fig. 14 Relevant computing events before and after the begging of Cloud Computing

obsolete. Based on this premise, we can assert that in 2014, cloud might truly come of age.

More and more organizations are converting their legacy systems to cloud-based ones, whether public, private or hybrid. The personal cloud is also rising fast with applications such as iCloud, Evernote and Dropbox that demonstrate just how easy and reliable it can be for the average user. Meanwhile, moving systems to a cloud infrastructure reduces company costs not only in terms of initial investments, but also through cutting back on the personnel needed to maintain its IT infrastructure. Finally, the cloud itself ensures the compatibility of applications with the company's internal systems and technological platform since applications can basically run on any browser, not to mention the visioning process of applications or security patches that are facilitated by this approach. These trends mean that the conventional IT department of the 1990s and 2000s is fated to disappear [15]. Most of its roles no longer make sense in a cloud-centric world which has, in many ways, developed to overcome the limitations and bottlenecks of this very IT department model. This does not mean, however, that IT departments will simply stop existing; rather, they need to reinvent themselves in the face of change.

As to the conflicts with government regulations, some studies such as [20,24,81,83,96] warn that differences between current cloud business models and contemporary laws inspire new shifts. This is because of scenarios such as the Federal Data Protection Act [20], which says that a customer should know the location of its data even though by definition cloud providers can put the data anywhere. We understand, however, that cloud providers should pay attention to the relevant regulations before deploying their services anywhere (Fig. 14).

Moreover, Cloud Computing inspires rethinking of disaster recovery. Network World's Editor-in-Chief, John Dix, recently discussed the subject of disaster recovery with IBM's distinguished engineer Richard Cocchiara (CTO and managing partner of Consulting for IBM's Business Continuity and Resiliency Services) for his perspective on the subject. Cocchiara leads a worldwide team who work with clients on system availability, disaster recovery planning, business continuity management and IT governance. One of the questions posed, according to an article on NetworkWorld.com[6], was the following: What are the different roles cloud can play in disaster recovery and business continuity? According to Cocchiara, probably, the most basic thing is backing up data offsite. Most large companies have some sort of a backup strategy, but more often than you might think, companies do not send their data offsite or do not send it far enough offsite. When asked if they have checked to see what potential regional issues there might be, he explained that sometimes they find some geological or weather or some other type of potential risk that would affect their ability to recover them locally. Cloud gives them the ability to store data at some place remote, store it online, and to typically recover them faster than from a tape.

Still unclear are all the variables that should be considered for building a system architecture to provide service on Cloud Computing [43]. Some directions are clear, for instance, a suitable development of XaaS must be based on harmony between infrastructure and software applications. This will transform a heterogeneous environment into a homogeneous one, which will allow services to be delivered in a flexible way and meet requirements of all customer categories. As to the conception of SaaS, many architectural styles have been considered such as a model-driven style [57], multi-tenant maturity levels [11], Service-oriented architecture [27,34], and the RESTFull model [12].

Aligned with Ian Foster [74], we believe that cloud interoperability is a big issue because current solutions have been developed over proprietary control. This concern opens up a new perspective of research even though there are interesting ongoing studies on the run [48]. Still, we believe that Cloud Computing will become more popular, suffer less resistance and reach other horizons if open standards are further considered such as the open virtualization format (OVF), security assertion markup language (SAML) of OASI, and cloud data management interface (CDMI) of Storage Networking Industry Association (SNIA).

6 Threats of validity

Although we tried to conduct this systematic review as rigorously as possible, it might have still suffered from several validity threats. Future efforts should therefore take into account these limitations when interpreting or directly using the findings or conclusions in this report:

- *Research scope* The practices of Cloud Computing are being reported in various sources such as academic publications, technical reports, magazines and blogs, etc. In particular, academic publications are normally formal, following a rigorous

[6] http://www.networkworld.com/news/2013/073013/cloud-computing-disaster-recovery-272370.html.

peer-reviewing process. Having considered the generally specific and precise documentation of Cloud Computing in formal publications, we limited this review to academic studies only. There is no doubt that informal descriptions in the Cloud Computing area, relevant experiences and projects in blogs and technical reports can also provide highly relevant information. However, it is impossible to explore and collect useful data from different sources all at once. Moreover, the published studies can be viewed as typical of the existing ad hoc documentation practices. In fact, we proposed using first the result of this review to construct a knowledge-base which can gradually be extended and enriched by other informal and empirical studies in the Cloud Computing area.

- *Research questions* The set of questions that we defined might not have covered the whole Cloud Computing area, which implies that one can still find other relevant questions of interest. Having considered this as a viable threat, we had several meetings with members of the ASSERT research group [7] in order to calibrate the relevant importance of the posed questions. In this way, even if we had not selected the most optimum set of questions, we have at least attempted to address the most raised and considered open issues in the field.
- *Publication bias* We could not guarantee that all relevant primary studies were selected. It is possible that some relevant studies were not chosen (or rather overlooked) throughout the research process. As much as possible, we did try to avoid this by following the references in the most significant primary studies.
- *Comprehensiveness* Given the increasing number of studies in this area, we have admitted that some relevant studies might have been ignored or overlooked. The underlying reasons could be various, ranging from the search engines to the search query. Firstly, we did not look into every possible search resource. To balance between the estimated workload and coverage, five electronic libraries were selected, based on previous review experiences. In fact, the statistics suggest that these five library search engines would have given us a broad-enough repertoire of the relevant studies [94].
- *Conducting the search* The digital databases do not have compatible search rules; hence, only a few search engines allowed us to search by authors while others only allowed it by content. We adapted our own search strategy for each digital database. We also tried to the best of our ability to reduce any possible bias in the manner of conducting the review, including workshop discussion with members of the ASSERT research group. However, when it comes to the data analysis, there might still have been the possibility for incomplete findings or conclusions based on personal interest and/or opinions.
- *Data extraction* During the process of data extraction from the reviewed studies, we found that not many of these papers have specified sufficient details about the evaluation background, environment, and procedure, which could be partially reflected in the quality assessment. As a result, sometimes we had to infer certain information from some rather ambiguous clues, particularly when we tried to ascertain the study's purpose or key challenges. Therefore, there may be some inaccuracies

[7] http://assertlab.com/.

in the inferred data. However, this point can be considered as a limitation not so much on this review as the primary studies consulted. Since empirical research in Cloud Computing falls under the domain of experimental computer science [4], we suggest that researchers could consider employing a structural abstract [9] and/or guidelines for conducting and reporting experiments or case studies [69] to regulate future attempt at evaluation. Moreover, the studies were classified based on our judgment. However, despite double-checking, some studies could still have been classified incorrectly. To mitigate this, the entire classification process was validated by the ASSERT research group members.

7 Conclusion

This study presented a Systematic Review of Cloud Computing. Along this vein, we reviewed several state-of-the-art cloud applications, clarifying and discussing open issues via an in-depth analysis of over 301 primary studies. Through answers provoked by eight exploratory research questions, we found evidence confirming Cloud Computing as an ascending technology that introduces a new paradigm by enabling a rational computational model. In general, Cloud Computing still needs improvements in terms of managing the heterogeneity of its elements in order to become a truly on-demand environment.

The overall data collected in this study should help familiarize the curious with the state-of-the-art and state-of-the-practice in the Cloud Computing area. In particular, the answers to the aforesaid research questions summarized Cloud Computing's current challenges, open issues, main use, approaches and strategies. As a result of this research, we built a Cloud Computing timeline ranging from the 1960's to 2012 which pointed out the market behaviors over the last 50 years and the close relation between Utility Computing and Cloud Computing models, thereby characterizing Cloud Computing as a viable option to today's IT challenges.

In particular, we noted that security and privacy are key issues relating to the adoption of cloud solutions. Nevertheless, we also identified ongoing efforts by the IT community to mitigate current problems around these issues. We also found that Cloud Computing requires efforts regarding the deployment of parallel applications in enterprise environments. Another identified problem was the inadequacy of current business models. Based on this research, it remains unclear how Cloud Providers ought to charge usage. While some providers strongly defend the pay-per-use model, others charge according to time of usage. We understand that service diversity, being proposed by Cloud Computing (XaaS), is one of the most attractive elements of the model. Based on the evidence gathered, we may highlight the following suggestions about services on cloud: (1) make sure the service really needs a cloud environment; (2) the whole cloud environment must be implemented with the focus being on green IT and dealing with power energy factors beyond the datacenters; (3) by distributing the datacenters among various countries, the cloud provider must pay attention to local regulations so as to avoid potential legal complications; and (4) adapt the service model and cloud environment according to the customer's needs.

Last but not least, we sincerely hope that the results of this study will help research groups develop new research fronts that further contribute to the maturity and adoption of Cloud Computing.

Acknowledgments The authors would like to thank the ASSERT Research Group for the feedback on meetings and support during the execution of this research. This work was partially supported by the National Institute of Science and Technology for Software Engineering (INES), funded by CNPq and FACEPE, grants 573964/2008-4 and APQ-1037-1.03/08.

References

1. Amazon (2012) Amazon web services. URL: http://aws.amazon.com/. Retrieved 24 Oct 2013
2. Apple (1983) Apple invents the personal computer. URL: http://archive.computerhistory.org/resources/text/Apple/Apple.Lisa.1983.102634506.pdf. Retrieved 24 Oct 2013
3. Baliga J, Ayre RWA, Hinton K, Tucker RS (2010) Green cloud computing: balancing energy in processing, storage and transport. J Proc IEEE 99
4. Basili VR, Zelkowitz MV (2007) Empirical studies to build a science of computer science. Commun ACM 50(11):33–37
5. Bellis M (1997) The history of computers. URL: http://inventors.about.com/library/blcoindex.htm. Retrieved 24 Oct 2013
6. Berners-Lee T (1998) The world wide web: a very short personal history
7. Boloor K, Chirkova R, Viniotis Y, Salo T (2010) Dynamic request allocation and scheduling for context aware applications subject to a percentile response time sla in a distributed cloud. In: IEEE International Conference and Workshops on Cloud Computing Technology and Science (CLOUDCOM'10)
8. Bonetta D, Pautasso C (2011) Towards liquid service oriented architectures. In: International conference on World Wide Web, Hyderabad, India
9. Budgen D, Kitchenham BA, Charters SM, Turner M, Brereton P, Linkman SG (2008) Presenting software engineering results using structured abstracts: a randomised experiment. Empirical Softw Eng 13(4):435–468
10. Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I (2009) Cloud computing and emerging it platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Comput Syst 25(6):599–616
11. Cadan KS, Li WS, Phan T, Zhou M (2009) Frontiers in information and software as services. In: International Conference on Data, Engineering (ICDE'09)
12. Calero JMA, Edwards N, Kirschnick J, Wilcock L, Wray M (2010) Toward a multi-tenancy authorization system for cloud services. J Secur Priv 8:48–55
13. Campbell-Kelly M (2009) Historical reflections the rise, fall, and resurrection of software as a service. J CACM 52
14. Caron E, Desprez F, Muresan A (2011) Pattern matching based forecast of non-periodic repetitive behavior for cloud clients. J Grid Comput 9:49–64
15. Carr NG (2003) It doesn't matter. In: Harvard Business School
16. Chapman C, Emmerich W, Márquez FG, Clayman S, Galis A (2011) Software architecture definition for on-demand cloud provisioning. J Cluster Comput 14:1–22
17. Chaves SA, Westphall CB, Lamin FR (2010) Sla perspective in security management for cloud computing. In: International Conference on Networking and Services (ICNS'10)
18. Chellappa RK (1997) Intermediaries in cloud-computing: A new computing paradigm. In INFORMS Annual Meeting, Dallas
19. Chieu T, Kapoor S, Mohindra A, Shaikh A (2010) Cross enterprise improvements delivered via a cloud platform: a game changer for the consumer product and retail industry. In: International Conference on Services, Computing (SCC'10)
20. Cho B, Gupta I (2010) New algorithms for planning bulk transfer via internet and shipping networks. In: International Conference on Distributed, Computing Systems (ICDCS'10)
21. Chong F, Carraro G (2006) Architecture strategies for catching the long tail. MSDN Library, Microsoft Corporation, pp 9–10
22. Columbus L (2011) Gartner releases their hype cycle for cloud computing, 2011. URL: http://goo.gl/pqrDC, 2011. Retrieved 24 Oct 2013

23. Costa R, Brasileiro F, Filho GL, Souza DM (2009) Oddci: on-demand distributed computing infrastructure. In: Workshop on Many-Task Computing on Grids and Supercomputers (MTAGS'09)
24. Doelitzscher F, Reich C, Sulistio A (2010) Designing cloud services adhering to government privacy laws. In: Complex, Intelligent and Software Intensive Systems (CIT'10)
25. Dutreilh X, Moreau A, Malenfant J, Rivierre N, Truck I (2010) Data center resource allocation to control theory and back. In: International Conference on Cloud, Computing (CLOUD'10)
26. Elmroth E, Larsson L (2009) Interfaces for placement, migration, and monitoring of virtual machines in federated clouds. In: International Conference on Grid and Cooperative, Computing (GCC'09)
27. Erl T (2005) Service-oriented architecture (SOA): concepts, technology, and design. Prentice Hall
28. Foster I (1998) The grid: blueprint for a new computing infrastructure. Morgan Kaufmann Publishers Inc, Burlington
29. Gill K (2008) Remember the oil crisis? URL: http://uspolitics.about.com/b/2008/01/02/remember-the-oil-crisis.htm. Retrieved 24 Oct 2013
30. Guha R, Al-Dabass D (2010) Impact of web 2.0 and cloud computing platform on software engineering. In: Proceedings of the 2010 International Symposium on Electronic System Design (ISED'10), pp 213–218
31. Hassan MM, Song B, Huh EN (2009) A framework of sensor, cloud integration opportunities and challenges. In: International Conference on Ubiquitous Information Management and Communication (ICUIMC'09)
32. Hou Z, Zhou X (2010) Asaas: application software as a service for high performance cloud computing. In: International Conference on High Performance Computing and Communications (HPCC'10)
33. Huang H, Wang L (2010) P&p: a combined push-pull model for resource monitoring in cloud computing environment. In: International Conference on Cloud, Computing (CLOUD'10)
34. Hutchinson C, Ward J, Castilon K (2009) Navigating the application architecture. J IT Prof 11:18–22
35. Ichak A (1996) The pursuit of prime: maximize your company's success with the Adizes Program. Knowledge Exchange
36. Jianhong Z, Hua C (2010) Secuirty storage in the cloud computing: a rsa-based assumption data integrity check without original data. In: International Conference on Educational and Information Technology (ICEIT'10)
37. Jin H, Xiang G, Zou D, Wu S, Zhao F, Li M, Zheng W (2011) A vmm-based intrusion prevention system in cloud computing environment. J Supercomput 66:1133–1151
38. Kandukuri BP, Paturi VR (2009) Cloud security issues. In: International Conference on Services, Computing (SCC'09)
39. Kansal A, Zhao F, Liu J, Kothari N, Bhattacharya AA (2010) Virtual machine power metering and provisioning. In: ACM symposium on Cloud computing (SoCC'10)
40. Kertész A, Kecskeméti G, Brandic I (2011) Autonomic sla-aware service virtualization for distributed systems. In: Euromicro Conference on Parallel, Distributed and Network-based (PDP'11)
41. Kitchenham B, Charters S (2007) Guidelines for performing systematic literature reviews in software engineering. Technical Report EBSE 2007–001, Keele University and Durham University Joint, Report
42. Kondo D, Javadi B, Malecot P, Cappello F, Anderson DP (2009) Cost-benefit analysis of cloud computing versus desktop grids. In: IEEE International Symposium on Parallel and Distributed Processing with Applications (IPDPS'09)
43. Kossmann D, Kraska T, Loesing S (2010) An avaluation of alternative architectures for transaction processing in the cloud. In: International conference on Management of data (SIGMOD'10)
44. Kozuch MA, Ryan MP, Gass R, Schlosser SW, O'Hallaron, Cipar J, Krevat E, ópez JL, Stroucken M, Ganger GR (2009) Tashi: location-aware cluster management. In: International Conference on AC and DC Power Transmission (ACDC'09)
45. Kumar SR, Saxena A (2011) Data integrity proofs in cloud storage. In: International Conference on COMmunication Systems and NETworkS (COMSNETS'11)
46. Kutare M, Eisenhauer G, Wang C, Schwan K, Talwar V, Wolf M (2010) Monalytics: Online monitoring and analytics for managing large scale data centers. In: International Conference on Autonomic Computing (ICAC'10), Washington
47. Lee JH, Park MW, Eom JH, Chung TM (2011) Multi-level intrusion detection system and log management in cloud computing. In: International Conference on Advanced Communication Technology (ICACT'11)

48. Li J, Zhao G, Chen X, Xie D, Rong C, Li W, Tang L, Tang Y (2010) Fine-grained data access control systems with user accountability in cloud computin. In: IEEE International Conference and Workshops on Cloud Computing Technology and Science (CLOUDCOM'10)
49. Li Q, Hao Q, Xiao L, Li Z (2009) Adaptive management of virtualized resources in cloud computing using feedback control. In: International Conference on Information Science and Engineering (ICISE'09)
50. Lin FT, Shih TS (2010) Cloud computing: the emerging computing technology. J ICIC Int 1:33–38
51. Luo M, Zhang LJ, Lei F (2010) An insuanrance model for guranteeing service assurance, integrity and qos in cloud computing. In: International Conference on Web Services (ICWS'10)
52. Macías M, Fitó JO, Guitart J (2010) Rule-based sla management for revenue maximisation in cloud computing markets. In: International Conference on network and Service Management (CNSM'10)
53. Madnick S (1969) Time-sharing systems: virtual machine conept vs. conventional approach. J Modern Data Sys 2:34–36
54. Marston S, Li Z, Bandyopadhyay S, Zhang J, Ghalsasi A (2010) Cloud computing-the business perspective. J Decis Support Syst 51:176–189
55. McCarthy J (1983) Reminiscences on the history of time-sharing. URL: http://www-formal.stanford.edu/jmc/history/timesharing.dvi, 1983. Retrieved 02 June 2012
56. Mehta HK, Kanungo P, Chandwani M (2011) Performance enhancement of scheduling algorithms in clusters and grids using improved dynamic load balancing techniques. In: International conference on World Wide Web (WWW'11)
57. Menzel M, Warschofsky R, Thomas I, Willems C, Meinel C (2010) The service security lab: A model-driven platform to compose and explore service security in the cloud. In: World Congress on Services (SERVICES-I'10)
58. Mounzer J, Bambos N (2010) Integrated security risk management for it-intensive organizations. In: International Conference on Information Assurance and Security (IAS'10)
59. Nae V, Prodan R, Losup A (2011) A new business model for massively multiplayer online games. In: International conference on Performance, engineering (ICPE'11)
60. Nair SK, Porwal S, Dimitrakos T, Ferrer AJ, Tordsson J, Sharif T, Sheridan C, Rajarajan M, Khan AU (2010) Towards secure cloud bursting, brokerage and aggregation. In: International Conference on Web Services
61. Nicolae B (2010) High throughput data-compression for cloud storage. Lect Notes Comput Sci 6265(2010):1–12
62. NITRD (1991) High performance computing act of 1991. URL: http://www.nitrd.gov/Congressional/Laws/pl_102-194.html, 1991. Retrieved 24 Oct 2013
63. Parkhill DF (1966) The challenge of the computer utility. Addison-Wesley Publishing Company, Boston
64. Pervez Z, Khattak AM, Lee S, Lee YK (2010) Dual validation framework for multi-tenant saas architecture. In: Future Information Technology (FutureTech'10)
65. Petersen K, Feldt R, Mujtaba S, Mattsson M (2008) Systematic mapping studies in software engineering. In: Evaluation and Assessment in Software Engineering (EASE'08), Italy. University of Bari
66. Polsson K (2012) Chronology of personal computers. URL: http://www.islandnet.com/kpolsson/comphist/comp1988.htm, 2012. Retrieved 24 Oct 2013
67. Ramakrishman L, Jackson KR, Canon S, Cholia S, Shalf J (2010) Defining future platform requirements for e-science clouds. In: ACM symposium on Cloud, computing (SoCC'10)
68. Rimal BR, Jukan A, Katsaros D, Goeleven Y (2010) Architectural requirements for cloud computing systems: an enterprise cloud approach. J Grid Comput 9:3–26
69. Per R, Martin H (2009) Guidelines for conducting and reporting case study research in software engineering. Empirical Softw Engg 14(2):131–164
70. Salesforce.com (2013) Salesforce.com. last checked oct/2013. URL: www.salesforce.com, 2013. Retrieved 24 Oct 2013
71. David S, Farheen A (2010) Taking a flexible approach to asps. J CACM 53:139–143
72. Sevior M, Fifield T, Katayama N (2010) Belle monte-carlo production on the amazon ec2 cloud. J Phys Conf Ser 219 012003. doi:10.1088/1742-6596/219/1/012003
73. Shi A, Xia Y, Zhan H (2010) Applying cloud computing in financial service industry. In: International Conference on Intelligent Control and Information Processing (ICICIP'10)
74. Foster I, Zhao Y, Raicu L, Shiyong L (2008) Cloud computing and grid computing 360-degree compared. URL: http://arxiv.org/ftp/arxiv/papers/0901/0901.0131.pdf, 2008. Retrived 24 Oct 2013

75. Sigh MD, Krishna PR, Saxena A (2010) A cryptography based privacy preserving solution to mine cloud data. In: Proceedings of the Annual ACM Bangalore Conference (COMPUTE'10)
76. Sivathanu S, Liu L, Yiduo M, Pu X (2010) Storage management in virtualized cloud environment. In: International Conference on Cloud, Computing (CLOUD'10)
77. Smarr L (2008) Metacomputer architecture of the global lambdagrid: How personal light paths are transforming e-science. URL: http://goo.gl/ohpfMR, 2008. Retrieved 24 Oct 2013
78. Spring J (2011) Monitoring cloud computing by layer, part 1. J IEEE Secur Priv 9:66–68
79. Staten J (2009) Hollow out the moose: reducing cost with strategic rightsourcing. Forrester Research Inc, Cambridge
80. Tao Q, Chang H, Yi Y, Gu C (2010) A trustworthy management approach for cloud services qos data. In: International Conference on Machine Learning and Cybernetics (ICMLC'10)
81. Taylor M, Haggerty J, Gresty D, Hegarty R (2010) Digital evidence in cloud computing systems. J Comput Law Secur Rep Rev 26:204–208
82. Thelen E (2010) General electric computer department from the bottom up 1961 through 1965. URL: http://www.ed-thelen.org/EarlyGE-Computers.html, 2010. Retrieved 24 Oct 2013
83. Udo H (2010) Data protection and legal compliance in cloud computing. J DuD 34:554–556
84. Wang J, Varman P (2010) Avoiding performance fluctuation in cloud storage. In: International Conference on High, Performance Computing (HiPC'10)
85. Wang Y, Song A, Luo J (2010) A mapreducemerge-based data cube construction method. In: International Conference on Grid and Cooperative, Computing (GCC'10)
86. Wayne NIST, Jansen A (2011) Cloud hooks: security and privacy issues in cloud computing. In: Hawaii International Conference on System Sciences (HICSS'11)
87. Christof W, Arun A, Benjamin B, Nikolay B, Thomas M, Wibke M, Jochen S (2009) Cloud computing: a classification, business models, and research directions. J Bus Inform Syst Eng 1:391–399
88. Woitaszek M, Tufo HM (2010) Developing a cloud computing charging model for high-performance computing resources. In: CIT, IEEE Computer Society, pp 210–217
89. Wong WK, Cheung DW, Kao B, Mamoulis N (2009) Secure knn computation on encrypted databases. In: International conference on Management of data (SIGMOD'09)
90. Wu H, Winer C (2009) Network security for virtual machine in cloud computing? In: International Conference on Computer Sciences and Convergence Information Technology (ICCIT'09)
91. Yigitbasi N, Iosup A, Epema D, Ostermann S (2009) C-meter: a framework for performance analysis of computing clouds. In: IEEE/ACM International Symposium on Cluster, Cloud and Grid, Computing (CCGrid'09)
92. Yu X, Wen Q (2010) A view about cloud data security from data life cycle. In: International Conference on Computational Intelligence and Software Engineering (CiSE'10)
93. Yusuke T, Koie H, Tomohiro K, Isao K, Yoshio T (2010) A distributed storage system allowing application users to reserve i/o performance in advance for achieving sla. In: International Workshop on Middleware for Grids, Clouds and e-Science (MGC'10)
94. Zhang Q, Cheng L, Boutaba R (2010) Cloud computing: state-of-the-art and research challenges. J Internet Serv Appl 1(1):7–18
95. Zheng Q, Xu S (2010) Fail and dynamic proofs of retrievability. In: ACM Conference on Data and Application Security and Privacy (CODASPY'10)
96. Zhou M, Zhang R, Xie W, Qian W, Zhou A (2010) Security and privacy in cloud computing: a survey. In: International Conference on Semantics Knowledge and Grid (SKG'10)
97. Zhou W, Ning P, Wang R, Zhang X, Ammons G, Bala V (2010) Always up-to-date -slacalable offline patching of vm images in a compute cloud. In: Annual Computer Security Applications Conference (ACSAC'10)
98. Zissis D, Lekkas D (2011) Securing e-government and e-voting with an open cloud computing architecture. J Gov Inform Quart 28:239–251