2010 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing

Cloud Computing Landscape and Research Challenges regarding Trust and Reputation

Sheikh Mahbub Habib*, Sebastian Ries†, Max Mühlhäuser‡
Center for Advanced Security Research Darmstadt(CASED)
Technische Universität Darmstadt
Mornewegstr. 32, DE-64293, Germany
Email: *sheikh.habib@cased.de,†ries@cased.de,‡max@tk.informatik.tu-darmstadt.de

***Abstract*—Cloud Computing is an emerging computing paradigm. It shares massively scalable, elastic resources (e.g., data, calculations, and services) transparently among the users over a massive network. The Cloud market is growing rapidly and bringing up numerous research challenges. This paper provides a landscape of Cloud Computing and its research challenges, especially considering the areas of service selection, quality assurance of Cloud services, and trust establishment in Cloud environments. As the latter is known to be one of the major challenges of Cloud Computing, We also provide an overview of the important aspects that need to be considered when integrating trust and reputation concepts into Cloud Computing.**

***Index Terms*—Cloud Computing, Trust models, Reputation, QoS**

I. Introduction

Cloud Computing is a new paradigm that uses dynamically scalable shared resources over the scalable network of nodes. Data centers, web services, and low-end devices can be examples of such nodes. The network of such nodes can be termed as the *Cloud* and several networks of such nodes can be called the *Internet-of-Clouds*. The Internet-of-Clouds involves four major participants which are Cloud providers, brokers, resellers, and end consumers.

The business market that establishes around Cloud Computing is growing rapidly to fulfill the users' demands in the near future. Gartner Inc. predicts that Cloud Computing revenue will exceed $150 Billion by 2013 [1].As the market is growing faster, there will be a need to reliably identify the quality level of the service providers. This will establish the customers' confidence in adopting Cloud-based services and support them in selecting the appropriate service providers.

These issues are already known from the Internet of Services (as well as from P2P and eCommerce). There, trust and reputation systems [2] have been proposed to differentiate the service providers based on the quality of their services and to identify high quality services. The Internet-of-Clouds needs a similar concept to support customers in selecting appropriate providers. Some industry experts have already stated the need of regulation and monitoring in the Cloud Computing world which are mentioned as follows. The need of third party assurance body to accredit the Cloud vendors is mentioned in [3]. In a recent article [4], the author has discussed some ways to evaluate the service quality of the Cloud vendors based on parameters like response time, availability and elasticity. Also, a few numbers of research articles have targeted to reveal the security weaknesses [5], identify research issues [6], provide security guidance [7], and recommendations [8] regarding Cloud Computing.

To the best of our knowledge, there are only few research articles in the field of Cloud Computing that focus on the evaluation of the Cloud vendors or on finding appropriate solutions to establish confidence between the customers' and the Cloud vendors' community. We focus on this particular issue in this paper.

This paper proposes a new research direction in the field of Cloud Computing: how to support users in selecting trustworthy Cloud providers using trust and reputation concepts. We identified a set with the most important parameters required to support the consumers in selecting Cloud providers based on a broad survey of the current state-of-the-art literatures. The remainder of the paper is organised as follows: Section II describes the building blocks of Cloud Computing. Section III lists some key benefits of and possible threats to Cloud Computing. Section IV introduces the trust and reputation concepts and a set of QoS+ (beyond QoS) parameters that are relevant while selecting a Cloud provider. We present two sets of research challenges in section V: one around Cloud Computing in general and another one regarding service provider selection in particular. In Section VI, We draw our conclusions and discuss the future work.

II. Cloud Computing Building Blocks

This section describes the landscape of Cloud Computing from our perspective; in particular including service delivery, deployment models, and involved entities. Regarding a definition of Cloud Computing We refer to [7]–[9], where IBM, Forrester Research, NIST and ENISA come up with concrete definitions.

A. Service Delivery and Deployment Models

According to [7], Cloud service delivery models are divided into three categories. However, three more categories are discussed in a recent talk [10]. Adopting all

978-0-7695-4272-0/10 $26.00 © 2010 IEEE
DOI 10.1109/UIC-ATC.2010.48

these, service delivery models are categorized into six types which are Software as a Service(SaaS), Data as a Service (DaaS), Network as a Service (NaaS), Platform as a Service (PaaS), Identity and Policy Management as a Service (IPMaaS), and Infrastructure as a Service (IaaS). For further details regarding specific delivery models We refer to [7], [10].

Cloud deployment models are categorized into four different types [7] which are Public Cloud, Private Cloud, Community Cloud, and Hybrid Cloud.

B. Cloud Entities

Cloud providers and consumers (which We also refer to as customers) are the two main entities in the business market. But, service brokers and resellers are the two more emerging service level entities in the Cloud world. These are discussed as follows:

Cloud Providers: The providers host and manage the underlying infrastructure and offer different services (e.g., SaaS, PaaS, IaaS, and etc.) to the consumers, the service brokers or resellers. Cloud brokers and resellers plays the same role as "Cloud providers" in certain contexts which are discussed as follows:

Cloud Service Brokers: Service brokers concentrate on the negotiation of the relationships between consumers and providers without owning or managing the whole Cloud infrastructure. Moreover, they add extra services on top of a Cloud provider's infrastructure to make up the user's Cloud environment.

Cloud Resellers: Resellers can become an important factor of the Cloud market when the Cloud providers will expand their business across continents. Cloud providers may choose local IT consultancy firms or resellers of their existing products to act as "resellers" for their Cloud-based products in a particular region.

Cloud Consumers: End users belong to the category of Cloud consumers. However, also Cloud service brokers and resellers can belong to this category as soon as they are customers of another Cloud provider, broker or reseller.

In the next section, key benefits of and possible threats and risks for Cloud Computing are listed.

III. Key Benefits, Possible Threats and Risks of Cloud Computing

Cloud Computing has several benefits compared to traditional datacenter-based computing. However, a number of risks and obstacles(e.g., data lock-in, data confidentiality and auditability, data transfer bottlenecks, and etc.) to adopt Cloud Computing in enterprises are mentioned in [11].

A. Key Benefits

Small and medium enterprises (SMEs) and large organizations are outsourcing IT resources in the Cloud for the following key benefits:

Reduced Costs: Consumers are embracing [10] the concept of Cloud Computing to reduce costs by outsourcing the IT management. A good example is the outsourcing of Rentokil Initial's mail systems and other communication tools (i.e. calendars, instant messaging, video communication etc.) to Google's cloud in 2010 [12].

Dynamic Resource Sharing: This particular characteristic is helping Cloud vendors to offer cheap prices to Cloud consumers when it comes to leasing the virtual machines (VMs), virtual storages and compute cycles.

Pay-per-Use: The concept comes from the Utility Computing where customers have to pay according to time, cycles or volumes. No upfront cost has to be paid by the customers.

Faster Time to Roll Out New Services: Another key advantage of using Cloud Computing infrastructure and services by the enterprises is being able to roll out new services faster than the usual time using on-premises data center.

Dynamic Resource Availability: Using the Cloud Computing infrastructure, enterprises ensure resource availability during crunch periods. An ideal example is, a large number of users were able to easily render their photos into DVD quality videos by using a Cloud-based application [10].

B. Possible Threats and Risks

Security, privacy and trust are the main concerns for the consumers to adopt Cloud computing [13]. Beside these, there are some other risks which are discussed in the remainder of this section.

Threats to Security: According to standard computing literature [14], the "IT Security " can be split into three subgoals: *Confidentiality, Integrity and Availability.* Apart from known general threats to these three security subgoals, Cloud Computing poses specific threats to each one of them as follows. *Confidentiality* is often achieved by encryption. However, when a company's data is stored in a Cloud environment, one has to consider the problem of long-term confidentiality, meaning that past and present encryption schemes are expected to be insecure in a long run (e.g. 30 years). Moreover, if one is going to process data in the Cloud, this data will usually be decrypted which also poses threat to *Confidentiality.* Furthermore, information leakage vulnerability [5] in third-party compute Clouds pose threats to *Confidentiality* too. As the data is outsourced, there is no trivial way to know about the data having been tampered with, unless the Cloud providers let the consumers know about the incident which poses threat to the *Integrity* aspect. *Availability* will be discussed later in the "Reliability" section.

Threats to Privacy: Privacy is an important concern in Cloud Computing from the perspective of Cloud consumers, regarding legal compliance and consumers' trust. Sharing an infrastructure with other organizations off-premise is not the only aspect of Cloud Computing, but it enables new services to be made available in the cloud by combining other services: e.g. a "print on demand" service

could be provided by combining a printing service with a storage service [15]. In this type of scenario, threats to privacy arises as the information regarding the services might need to flow across service providers' boundaries. More detailed description regarding privacy issues and risks for Cloud Computing is given in [15].

Lack of Trust: Trust issues become important when the data centers are decentralized and the resources are distributed beyond the perimeter, which is especially true in the Cloud Computing scenario. With the growing number of Cloud service providers, the customers are facing a challenge to select the best and most appropriate providers from numerous offers. In [3], the author points out a typical scenario, where a Cloud provider can offer a "wonderfully" secure service while another may not, if the latter charges half the price, the majority of organisations will opt for the latter one as there is no real way to explore the difference.

Lack of Identity Management Solutions for Federated Clouds: (Federated) Identity Management (FIM) becomes important when thinking about federated Clouds. For example, an employee from Enterprise A is allowed to access certain resources in the Cloud environment of Enterprise B. Here, FIM provides means for sharing resources and services between enterprises without adopting the same technologies for directory services, authentication, and authorization. However, existing FIM solutions usually force the enterprises to share a common trusted third party as identity management provider (also known as authentication broker) like myOneLogin(http://www.myonelogin.com/). This kind of application may introduce a single point of failure as well as a single point where the security of an entire service inventory can be breached.

Lack of Latency and Bandwidth Guarantees: There are two essential characteristics that customers want to be ensured by the service providers: latency and bandwidth guarantees. Latency depends on the geographical placement of servers and content delivery network (CDN) services. Gomez Inc. has shown the test results where geographical location of the data centers is the main reason for lower or higher latency in the Cloud [4]. CDN services can be a solution of higher latency, but latency problems exist in certain cases [4]. High price, and variable throughput (e.g., in the case of sharing a VM with a bittorrent server) are the main factors behind offering less guarantees regarding bandwidth by the Cloud providers to their customers.

Weak Service Level Agreements (SLAs): Standard service level agreements (SLAs) in the present Cloud market are also one of the obstacles that the consumers face while adopting the services offered by the Cloud providers. Consumers might face problems that occur from vendor lock-in, insufficient security measures, data unavailability, hidden costs, and non-transparent infrastructure. In most cases, SLAs are created to protect the vendors/providers and not the customers. Most of the above mentioned problems are overlooked in current SLAs offered by the Cloud providers [16].

Lack of Standards and Interoperability: Cloud providers are not using any kind of common open standards yet which can lead the customers into problems like vendor lock-in and data portability. Even, there is no independent accreditation body to accredit the Cloud providers [3]. Some providers are offering portability features but within a limited boundary.

Lack of Customer Support: Providers, such as, Rackspace Inc., GoGrid or ZOHO are offering 24/7 customer support for free. However, Microsoft or Amazon is more inclined to provide paid customer support. Google's attitude is more likely: "Cloud it on your own" towards customers [17].

Perceived Lack of Reliability: *Availability* of resources in Cloud Computing is one of the biggest concerns for the consumers [11], [18]. Here, availability does not only refer to the reachability of the Cloud service, but also the success rate of the transaction. Most Cloud providers do not define the availability in this way. Cloud providers use the "availability" term to show their customers the level of reliability they would get regarding the Cloud services. Most cloud providers offer 99.99% availability for their servers, but it is not clear whether the availability is for a single server where the virtual instance of particular customer resides or for all the servers placed in data centers in different locations of the world. There have already been numerous reported outage incidents in the data centers of the Cloud providers [11] which conveys a negative message to the Cloud consumers about the providers regarding reliability.

Absence of Independent Quality Assurance Body: Cloud providers, e.g., Amazon, ZOHO, Rightscale are offering monitoring tools for the consumers to monitor their service availability and performance in real-time with extra charges. Yet, most of the Cloud providers are not offering these kind of solutions and if they do, they do not really monitor the SLA compliance. Alternatively, companies, such as, Gomez Inc. and Hyperic Inc. is offering monitoring services to evaluate the Cloud providers based on specific characteristics (e.g., SLA compliance, elasticity or cloud bursting, and etc.), which cannot be monitored from the proprietary tools offered by the providers. All in all, independent quality assurance bodies for monitoring the performance or quality of the Cloud services (besides Gomez Inc. and Hyperic Inc.) are still missing. Thus, Cloud customers are often let alone presently.

C. Recommendations Towards Trustworthy Cloud Service Environments

A number of threats and risks are listed regarding Cloud Computing paradigm in the previous section. However, Cloud providers are coming up with new ideas (e.g. 24/7 free customer support, publishing case studies of end

customers in web portal, offering trial periods, and etc.) to increase the customers' confidence towards Cloud-based services. But, the new initiatives are still far away from mitigating the threats and risks introduced by Cloud providers. Thus, Cloud service environments are still perceived as not sufficiently trustworthy from customers' perspective. A set of recommendations to increase Cloud providers' trustworthiness is given below:

- An independent mediation layer is needed to evaluate the service providers.
- Evaluation framework should be trusted enough so that malicious providers cannot manipulate the evaluation process.
- Cloud service providers should be evaluated based on fine-grained QoS parameters together with consumers' feedbacks, recommendations, and further specific parameters related to the Cloud Computing environment.

IV. Trust and Reputation in Cloud Environments

We see that support for customers in selecting Cloud providers is important and We believe that trust and reputation models which are successfully used in eCommerce, product reviews, P2P, online social networks, wireless sensor and adhoc networks will come into play here.

A. Definitions and Related Work

Trust and reputation are two essential concepts facilitating the decision making in many fields, from ancient fish market to the eCommerce. Trust is the subjective expectation of one entity about another within a specific context at a given time [2], [19], [20]. Reputation, on the other hand, is what is believed about an entity's standing by the community [2]. This belief can be derived from direct or indirect experiences collected in previous interactions between entities. It is important to note that trust can be used to determine the reputation of an entity, and vice versa [21].

We aim to explore the trust and reputation based approaches for supporting customers in selecting service providers in the Cloud environment. In online service environments, trust and reputation models have been proven useful in decision making [2], [21]. The concepts have also been adapted to wireless sensor and adhoc networks to solve problems such as, in choosing relay nodes to forward packets or for accepting location information from beacon nodes [22]. Furthermore, the integration of trust management systems in Grid computing has already received attention [23].

Recently, a trust-based reputation system is proposed to determine service trustworthiness in Intercloud computing envionments [23]. But, this system does not take account of different QoS parameters and contextual parameters (e.g., different service delivery models and service deployment models) which are important means to evaluate the Cloud providers; especially We see the need for identifying the parameters that are relevant for the customers as a basis for the trust establishment. Therefore, as a first step to integrate trust and reputation system in Cloud environment, a set of QoS+ (beyond QoS) parameters are presented in the next section.

B. QoS+ Parameters for Cloud Computing Environment

In section III-B, a number of shortcomings are identified in Cloud Computing environment showing which aspects in particular need to be improved to make the Cloud market more trustworthy for the consumers. This brings up new challenges in the area of trusted computing, Cloud service computing, attestation, and trust and reputation. When selecting a Cloud provider multiple parameters are important, which need to be identified properly. Also, there is need for mechanisms to measure those parameters and aggregate these measurements based on the customers' preference regarding the importance of the parameters. Based on the state-of-the-art survey presented in section III We have identified the following parameters:

i) Service Level Agreement (SLA), *ii)* Compliance or accreditation or certification, *iii)* Portability feature, *iv)* Interoperability feature, *v)* Geographical location of the data center (Cloud), *vi)* Customer support facilities, *vii)* Performance test, *viii)* Deployment models(e.g., private, public, and hybrid clouds) *ix)* Federated identity management solution, *x)* Security measures, and *xi)* User recommendation, feedback and publicly available reviews.

There are two parameters (i.e. Performance test, and Security measures) which can be further explored as follows:
i) Performance test: *a)* Latency, *b)* Bandwidth, *c)* Availability, *d)* Reliability, *e)* Elasticity.
ii) Security measures: *a)* Crypto algorithms and key management, *b)* Physical security support, *c)* Network security support, *d)* Data security support.

V. Shaping the Research Challenges

There are number of challenges around each of the parameters mentioned in section IV-B. We will discuss those as follows:

Specification and Evaluation of SLAs: A big challenge for the Cloud customers is to evaluate SLAs of Cloud vendors. Most vendors create SLAs to make a defensive shield against legal action, while offering minimal assurances to customers [24]. So, there are some important issues [24], e.g., data protection, outages,and price structures, that need to be taken into account by the customers before signing a contract with a provider. The specification of SLAs will better reflect the customers' needs if they address the required issues at the right time.

Common Standards and Unified Accreditation: Security-based accreditation for Cloud Computing would cover three main areas which are technology, personnel and operations [3]. Technical standards are likely to be driven

by organizations, such as, Jericho Forum[1] before being ratified by established bodies, e.g., ISO[2] (International Standard Organisation). On the personnel side, the Institute for Information Security Professionals[3] (IISP) is already offering formal accreditation for the security professionals. For the operational elements, there are some workable solutions such as tweaking the ISO 27001 and using it as the default measurement standard within the framework of the SAS 70[4]. Currently, one of the main problems is that there are many fragmented activities going in the direction of Cloud accreditation, but a common body for the coordination of those activities is missing. The creation of a unified accreditation body to certify the Cloud services would also be a big challenge.

Establishing Common Security Measures for Cloud Computing: This is a broad area which spans from ensuring the trustworthiness of services (i.e. they behave as expected) to provide guarantees about the security of infrastructure at the service provider side. In section III-B, We have listed some issues regarding information leakage, data protection, and privacy. This brings up new challenges in the area of privacy-enhancing technologies and trusted computing including trusted computing platforms and trusted platform modules.

Supporting Customers in Selecting Service Providers: The current initiatives mentioned in section III-C are offered by the service providers to gain more trust from and show transparency to their potential customers which seems still to be insufficient. There is no third-party assurance body yet to evaluate the vendors. The novel prize winning economist George Akerlof has already described the risk and consequences of not having an independent assurance body in a typical eCommerce environment in his famous paper [25]. Similar problems may arise in the Cloud environment which can affect the economical aspect of Cloud Computing and decrease the level of trust of customers towards Cloud providers.

The focus of our research is to support the customers in selecting the Cloud service providers using trust and reputation concepts. In this field, We still see numerous challenges and list the most important ones below:

Computation of Trust: Trust computation should consider the parameters listed in section IV-B, which represent the competencies and capabilities of a service provider in certain contexts, e.g., providing security measures, accreditation, bandwidth, customer support, and etc. The consideration of these different contexts brings up challenges regarding: *a)* aggregation of objective trust parameters, such as, expert ratings or real time measurements of elasticity, response time, and subjective trust parameters, such as, recommendations by other customers, *b)* combining hard trust, e.g., certificate and hardware based trust with soft trust, e.g., user feedback, *c)* aggregation of parameters from different rating domains, e.g., binary, discrete, and continuous, and *d)* reasoning about competencies: e.g., service providers might highlight competencies such as supporting TPM (Trusted Platform Module)-based servers and following a reliable external auditing standard (e.g., SAS 70 Type II) providing good evidence that the bookstore is less exposed to VM and hypervisor attacks and has the ability to safeguard the customers' data. However, those measures cannot ensure timely delivery of an ordered book.

Customization vs. "One Size Fits All": When trust is derived from different parameters, it is possible to consider subjective interests and requirements *depending* on the entity evaluating the trustworthiness of a service provider or to provide only a single "objective" trust (or reputation) value per service *independent* from the entity evaluating the trustworthiness. The subjective trust values provide means for considering the preference of each user in detail, while service providers might be more interested in the calculation of a single trust (or reputation) value, as this might be more directly influenced and observed by the companies. Customization allows users to define the parameters relevant for trust establishment from their point of view and supporting the user in weighting those parameters. For example, one customer might give a higher weight to security measures whereas for another customer a high-quality customer support is more important for the trust establishment.

Whom to Trust in Trust Establishment?: Establishing trust between the service providers and consumers has always been a challenge in service environments. Trust can be established in two ways: one way is to hosting trust models in centralized repository and other way is to use decentralized trust models. Both have advantages and disadvantages. In centralized trust models, requiring a trusted third party, users cannot manipulate the data except the ratings they provide themselves. The aggregation methodology can be kept secret and the individual ratings of an entity are not necessarily not published. However, the trusted authority hosting the centralized repository may manipulate the results and represents a single point for attacks. Decentralized trust models do not require a trusted third party, however, one has to trust in the mechanisms which are used for distributing the ratings and to consider the costs for distributing the ratings among the entities. The latter can be solved by applying algorithms that aggregate the individual ratings by only communicating with an entity's local neighborhood. A disadvantage of decentralized models is that preserving privacy can become harder as more information is distributed between the participating entities. However, entities are usually free to decide to whom they offer information.

Transferring Trust between Contexts: The customers' trust towards a service provider depends on application context or the scope of the interaction. The transfer

[1]https://www.opengroup.org/jericho/
[2]http://www.iso.org/iso/home.htm
[3]https://www.instisp.org/SSLPage.aspx
[4]http://www.sas70.us.com/what-is/what-is-sas70.php

of trust across those contexts is a big challenge for trust and reputation systems. For example, a service provider offers an email service and a video rendering service, both belonging to SaaS. Both application contexts require different competencies, e.g., spam protection issues and storage in the email context whereas for video rendering context latency, bandwidth, and parameters dealing with performance issues (e.g., response time, CDN facilities, and etc.) are important. Here, transferring trust, established in one context (email) to the other one (video rendering) is not a trivial task.

Attack Resistance: As soon as the influence of trust and reputation models on the decision of customers will grow, the interests in manipulating those values might grow, as seen in service environments earlier. A number of different attacks (e.g., Playbooks, Proliferation attacks, Reputation lag attacks, and etc.) against trust and reputation systems have been discussed [26], [27]. These types of attacks will also be of concern when designing trust and reputation systems for Cloud Computing environment. Thus, attack resiliency is the central design goal for the developers of these kind of systems.

Making Trust Information Transparent to the User: Derived trust values or reputation score should be transparent to the consumers so that they can easily take trust-based decision. To make the trust values transparent, users need an intuitive representation of trust supporting the relevant parameters.

VI. Conclusions and Future Work

In this paper, We have portrayed the landscape of Cloud Computing, describing what Cloud Computing is about, and what kind of services are offered by the Cloud providers at present. We have also listed the key benefits and identified possible threats and risks that come with Cloud Computing from the customers' perspective. These obstacles lead us to identify a set of QoS+ parameters (mentioned in section IV-B), which are important to assess the service providers and support customers in selecting among them. We have pointed out a number of research challenges regarding SLA specifications, open standards and accreditations, security measures, and service selection in Cloud Computing. Especially, We believe that the establishment of trust in the Cloud environment is a major issue for the success of Cloud Computing. Therefore, We have outlined a set of research challenges regarding trust and reputation models in Cloud environment in the previous section.

State-of-the-art trust and reputation models, as mentioned in section IV-A, have been proven promising to support customers in diverse areas. But, those models do not address most of the research challenges outlined in the last section. Thus, in the future, We will continue along the direction of supporting customers in selecting service providers in Cloud environment.

References

[1] Pring et al., "Forecast: Sizing the cloud; understanding the oppurtunities in cloud services," Gartner Inc., Tech. Rep. G00166525, March 2009.

[2] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43(2), pp. 618–644, 2007.

[3] C. Everett, "Cloud computing - a question of trust," *Computer Fraud & Security*, vol. 2009, no. 6, pp. 5 – 7, 2009.

[4] I. Mouline, "Why assumptions about cloud performance can be dangerous to your business," *Cloud Comp. J.*, vol. 2, no. 3, pp. 24–28, 2009.

[5] Ristenpart et al., "Hey, you, get off of my cloud! exploring information leakage in third-party compute clouds," in *Proceedings of the 16th ACM CCS 2009*. ACM Press, 2009, pp. 199–212.

[6] T. T. Mei L., Chan W.K, "A tale of clouds: Paradigm comparisons and some thoughts on research issues," in *Proceedings of the IEEE Asia-Pacific Services Computing Conference*. Washington D.C.: IEEE Computer Society Press, 2008, pp. 464–469.

[7] CSA, "Security guidance for critical areas of focus in cloud computing v2.1," Cloud Security Alliance, Tech. Rep., 2009.

[8] ENISA, "Cloud computing- benefits, risks and recommendations for information security," ENISA, Tech. Rep., 2009.

[9] R. Bias. Challenges embracing cloud storage. SNIA Cloud Storage Summit- Winter Symposium 2009. SNIA.

[10] S. Hanna. Cloud computing: Finding the silver lining. Distinguished Lecture in Inst. For Security, Technology, and Society, 2009. Darmouth College,USA.

[11] Armbrust et al., "Above the clouds: A berkeley view of cloud computing," EECS Department, University of California, Berkeley, Tech. Rep., 2009.

[12] Computing UK, "Why Rentokil opted to use Google Apps," Oct 13 2009.

[13] Aitenbichler et al., "Shaping the future internet," in *Proceedings of the 3rd International CompanionAble Workshop IoPTS*, 2009.

[14] C. P. Pfleeger and S. L. Pfleeger, *Security in Computing (4th Edition)*. Prentice Hall PTR, 2006.

[15] S. Person, "Taking account of privacy when designing cloud computing services," HP Laboratories, Tech. Rep. HPL-2009-54, 2009.

[16] SearchCIO, "Beware these risks of cloud computing, from no SLAs to vendor lock-in," Aug 6 2009.

[17] A. Williamson, "Comparing cloud computing providers," *Cloud Comp. J.*, vol. 2, no. 3, pp. 3–5, 2009.

[18] ENISA, "An sme perspective on cloud computing-survey," ENISA, Tech. Rep., 2009.

[19] D. Gambetta, "Can We Trust Trust?" in *Trust: Making and Breaking Cooperative Relations*. Department of Sociology, University of Oxford, 2000, ch. 13, pp. 213–237.

[20] S. Ries, "Extending bayesian trust models regarding context-dependence and user friendly representation," in *Proceedings of the 2009 ACM Symposium on Applied Computing*. New York, NY, USA: ACM, 2009, pp. 1294–1301.

[21] S. Ries, "Trust in ubiquitous computing," Ph.D. dissertation, Technische Universität Darmstadt, 2009.

[22] A. S. et al., "Reputation and trust-based systems for ad hoc and sensor networks," in *Algorithms and Protocols for Wireless Ad Hoc and Sensor Networks*. Wiley and Sons, 2008.

[23] J. Abawajy, "Determining service trustworthiness in intercloud computing environments," *Int. Symposium on Parallel Architectures, Algorithms, and Networks*, vol. 0, pp. 784–788, 2009.

[24] SearchCIO, "What to look for in a cloud computing SLA," June 16 2009.

[25] G. Akerlof, "A market for lemons," *The Quarterly Journal of Economics*, vol. 84, no. 3, pp. 488–500, August 1970.

[26] R. Kerr and R. Cohen, "Smart cheaters do prosper: defeating trust and reputation systems," in *AAMAS '09: Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems*, 2009, pp. 993–1000.

[27] A. Jøsang and J. Golbeck, "Challenges for robust of trust and reputation systems," in *Proceedings of the 5th Int. Workshop on Security and Trust Management (STM 2009)*, 2009.