# A Survey of Trust Management Models for Cloud Computing

**Conference Paper** · May 2015

CITATIONS
5

READS
1,354

**4 authors**, including:

Flavio Corradini
University of Camerino
**255** PUBLICATIONS **1,542** CITATIONS
SEE PROFILE

Fabrizio Ippoliti
University of Camerino
**6** PUBLICATIONS **12** CITATIONS
SEE PROFILE

Fausto Marcantoni
University of Camerino
**15** PUBLICATIONS **32** CITATIONS
SEE PROFILE

# A Survey of Trust Management Models for Cloud Computing

Flavio Corradini, Francesco De Angelis, Fabrizio Ippoliti and Fausto Marcantoni
*Computer Science Division, University of Camerino, Via del Bastione 1, 62032, Camerino, Italy*
{*flavio.corradini, francesco.deangelis, fabrizio.ippoliti, fausto.marcantoni*}*@unicam.it*

Keywords: Cloud Computing, Privacy, Security, Trust Relationship, Trust Model, Trust Management.

Abstract: Over the past few years, cloud computing has been widely adopted as a paradigm for large-scale infrastructures. In such a scenario, new security risks arise when different entities or domains share the same group of resources. Involved organizations need to establish some kind of trust relationships, able to define appropriate rules that can control which and how resources and services are going to be shared. The management of trust relationships represents a key challenge in order to meet high security requirements in cloud computing environments. This allows also to boost consumers confidence in cloud services, promoting its adoption. Establishing trust with cloud service providers supports to have confidence, control, reliability, and to avoid commercial issues like lock in. This paper proposes a survey of existing trust management models addressing collaboration agreements in cloud computing scenarios. Main limitations of current approaches are outlined and possible improvements are traced, as well as a future research path.

## 1 INTRODUCTION

Over the past few years, cloud computing has been widely adopted in almost every kind of organizations, for providing flexible and on-demand infrastructures, platforms and software as a service. Customers benefit from cloud services in their daily life, sometimes without even being aware that they are using services developed on a cloud computing infrastructure. In addition to the well-known benefits resulting from cloud computing adoption, several issues have emerged during its evolution: most of them relate to security, privacy and trust management. In particular, its proliferation has placed even more attention to trust management, representing one of the key challenges in the adoption of cloud computing technologies.

The speed and flexibility of adjustment to vendor offerings have motivated correct understanding of cloud computing paradigm, but, at the same time, this fact has introduced a higher risk to data privacy and security (Pearson and Benameur, 2010). From the cloud customer point of view, who may be either citizens, businesses or organizations, this represents a crucial concern, especially when entrusting cloud service providers (CSPs) for private or sensitive information, like financial or health data or business-confidential information. The resulting lack of trust is a key inhibitor to cloud adoption in domains where confidential or sensitive information is involved.

Indeed, according to a study presented by researchers at UC Berkeley (Armbrust et al., 2010), trust management and security aspects are ranked among the top 10 obstacles for adopting cloud computing. A more recent survey conducted by KPMG (KPMG International, 2013) affirms that major concerns affecting cloud adoption are about control and data security. In particular, CSPs report that customers main concern over switching to cloud is losing control, an issue voiced by almost half of all respondents. A even more recent white paper by Cloud Industry Forum addressing the UK scenario (Cloud Industry Forum, 2014), confirms that among most significant concerns about cloud adoption there are: data security (61%); data privacy (54%); fear of loss of control/manageability (24%); respectively as first, second and fourth reasons.

Lack of consumer trust is confirmed too from a study about attitudes on data protection and electronic identity in the European Union (European Commission, 2011), where less than one-third of European citizens surveyed trust phone companies, mobile phone companies and Internet service providers. Besides, 70% of them are concerned about their personal data held by companies being used for different aims than the agreed ones.

Main contribution of this work is to present a survey of most relevant approaches of trust models for cloud computing, categorized in different classes. Af-

ter this exhaustive comparison, major limitations of existing models are outlined and possible improvements are traced, as well as a future research path.

The remainder of this paper is organized as follows: the concepts of trust and reputation, starting from their origin to the the definition in computer science are described in section 2. Section 3 provides a classification of trust management models and for each group a detailed description of most relevant works in literature. Section 4 presents main limitations of current trust models and possible improvements. Finally, section 5 traces some conclusions and future work to be realized.

# 2 BACKGROUND

Trust and reputation concepts have their origin in the social sciences that study the nature and behavior of human societies (Gambetta, 1988), basically representing an act of faith. Trust management was originally developed by (Blaze et al., 1996), addressing important issues in network services security: centralized control of trust relationships, inflexibility to support complex trust relationships in large scale networks, and the heterogeneity of policy languages. Moreover, a widely accepted definition of trust, coming from cross-disciplinary set of academic literature, states as follows (Rousseau et al., 1998): "Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another". What arises from these general definitions is that trust is basically an attitude, a form of confidence in another, a belief that the other, despite a capacity to harm, will do the right thing in relation to the trustor (Nissenbaum, 1999). So, dealing with trust presupposes the acceptance of some kind of risk, even if its nature may be unclear or ambiguous. Moreover, trust cannot be just a common value that can be identified by a user and valid for every aspects of cloud services.

Furthermore, trust relates not only to technological aspects, but also social factors like reputation. Reputation is maybe a company's most valuable asset (Nissenbaum, 1999).

## 2.1 Defining Trust in Computer Science

Trust represents an essential aspect of every system where different entities have to collaborate. For such a complex concept, there is no universally accepted scholarly definition. However, trust relies to the competence of an entity to act dependably, securely and reliably within a specified context, as discussed in (Grandison and Sloman, 2000). Usually, trust lifecycle composes of three activities, that are: trust establishment, trust update and trust revocation. Moreover, trust is often divided into two classes: direct trust and recommended trust (Zhu et al., 2003). Direct trust represents the trust based on own experience with the other entity. Instead, when two entities have no direct interactions, then trust relationship can be established by another entity's recommendation, called recommended trust.

Another fundamental aspect of trust is the subjectivity, making even more complex its assessment. The term subjective relates to the perception of a subject toward an object. The properties and qualities assigned to an object depend on the subjects perception: for this reason, it may differ from one individual subject to the other (Solhaug and Stølen, 2012).

For these reasons, the notion of trust implies the modeling of trust management systems. A trust management system is a specific technique, normally used in distributed scenarios, able to manage and validate trust relationships agreed between different entities. A trust relationship is a particular kind of relation that defines privileges and restrictions. In this way, a trustor relies upon a trustee according to its ability to perform a specific action or provide a specific service, within a particular context (Grandison and Sloman, 2000). In case the reader is interested, in (Perez et al., 2014) a work providing a taxonomy of trust relationships in authorization domains for cloud computing can be found.

## 2.2 Trust in Cloud Deployment Models

Cloud services can be deployed in different ways, depending on the organizational structure and the provisioning location. Four deployment models are loosely distinguished, namely public, private, community, and hybrid cloud (Mell and Grance, 2011). The questions related to trust differ across various deployment models (Kumar et al., 2013).

Trust management in a *private* cloud does not represent a main concern if the organization does not rely on third-party CSPs. *Public* cloud model is the most common, but it introduced many risks about security and loss of control over data. *Community* cloud can be owned and managed by the same organizations in the community, a third party, or some combination of them. If there is a third party involved, the problem will occur as well as the corresponding case of the private model. Otherwise the problem is limited to trust relationships discussed and agreed between community subjects. In *hybrid* cloud, a private cloud is involved in the deployment model, besides a public

one. For this reason, trust management issues related to the public model shift to the hybrid one as well. This happens when the private cloud involved needs to scale out relying to the public model: issues about security and privacy become part of the scenario.

### 2.3 Cloud Transparency Initiatives

CSA (Cloud Security Alliance, 2014c), an international nonprofit organization, provides an important contribution: it aims to promote diffusion and use of best practices for providing security assurance within cloud computing. Among its initiatives, there is one gaining particular attention: "Security, Trust & Assurance Registry" (STAR) (Cloud Security Alliance, 2011). STAR program is a comprehensive set of contribution for cloud provider trust and assurance. It is based upon two components: the "Cloud Controls Matrix" (CCM) (Cloud Security Alliance, 2014a) and the "Consensus Assessments Initiative Questionnaire" (CAIQ) (Cloud Security Alliance, 2014b). CCM is a meta-framework of cloud-specific security controls, referred to leading standards, best practices and regulations. While CAIQ is a set of questions a cloud consumer and cloud auditor may wish to ask of a CSP. It provides a series of "yes or no" control assertion questions which can then be customized to suit each unique customer's demands.

However, despite these efforts, the overall situation shows indecision about if some kind of formal accreditation from a trusted independent organization would be advantageous for the cloud market.

## 3 TRUST MODELS

Trust modeling is the evaluation process of a system trust, as described in subsection 2.1. This modeling recognizes issues affecting trust of a system and helps in identifying areas where low levels of trust may discredit the system usability (Sanchika Gupta and Abraham, 2013). There exist several classification approaches of trust models for cloud computing present in literature (Firdhous et al., 2012b), (Huang and Nicol, 2013), (Kanwal et al., 2013). (Firdhous et al., 2012b) focuses the categorization according to a specific set of cloud computing parameters the authors have selected. For each trust model analysed in the paper, they analyse some features such as: if an identity management and/or authentication system is involved, which cloud deployment layers are involved or if a Service Level Agreements (SLAs) takes part in the model. (Huang and Nicol, 2013) discusses existing trust mechanisms for cloud, identifying the following categories: reputation based, SLA verification based, cloud transparency, trust as a service, and finally further analysis about formal accreditation, audit, and standards. Furthermore, (Kanwal et al., 2013) proposes a five classes sorting of trust models: Agreement based, Certificate/Secret keys-based, Feedback based, Domain based, and Subjective trust.

Our approach presents a different, simplified classification aiming to reduce the topic complexity, in order to provide a high-level analysis. Following in this section, trust models are categorized, described and briefly analysed upon the following groups:

- Policy Based;
- Recommendation Based;
- Reputation and Feedback Based.

We decided to simplify the classification, avoiding complexity and ambiguity while categorizing specific trust models that might belong to different groups, as it usually happens with some hybrid models. A small overview is also reserved to biological techniques for defining trust models, since they are gaining some attention in the literature.

However, due to limitations of space, we are unable to present all the existing body of literature. For this reason, priority has been assigned to last years' efforts, while less recent papers are in some case cited.

### 3.1 Policy Based

Trust management models in this group are based on contracts and agreements signed by CSPs for the delivery of their services to customers. The most common agreements are SLA and service policy statements (SPS), providing the basis for trust establishment. In particular, SLA play an important role to make the service trustworthy: it is a negotiation involving from one side CSPs and, from the other one, cloud customers. Various security concerns and quality of service attributes are included in contracts and agreements to establish trust on CSP. A relevant issue of this category is represented by the fact that SLA focuses just on the "visible" elements of cloud service performance (Huang and Nicol, 2013).

**(Alhamad et al., 2010)**. This paper describes the requirements and benefits of using information contained in SLAs, to manage trust in cloud environment, providing a high level architecture capturing major features required, as well as a protocol for the trust model. Aim of the proposed solution is to define reliable criteria for the selection process of CSPs. In other words, its goal is to recommend the "most related and trusted resources" among several CSPs,

meaning that analysed services match all the identified functional requirements. With the term of functional requirements, the authors refer to the detection of the average of several specific dataset or other kinds of data statistical analysis. Whereas, examples of non-functional requirements are represented by the level of privacy to ensure secure data storage or the time used to perform assessment tasks.

**(Sato et al., 2010)**. In the work, the authors introduce the notion of *contracted trust* that check CSPs services, according to contracts and related documents, such as SPS. The fundamental idea is to provide a two levels hierarchy for trust, namely internal trust and contracted trust. The first one is established directly on the cloud platform, if every basic operations are in full control of the customers. Internal trust is achieved via Trusted Platform Module (TPM) that assesses and validates the virtual machine configurations, keeping track of every processes running on cloud platform that assures the process execution control on cloud. On the other hand, the contracted trust is based on SPS, meaning that CSP are involved in this trust layer by negotiating the desired security and QoS requirements of customers.

**(Chakraborty and Roy, 2012)**. The authors show a framework that evaluates trustworthiness of a CSP service using a quantitative trust model. They identified and formalized two classes of parameters, namely *pre-SLA parameters* and *post-SLA parameters*. The first case is the simple one, that is when an initial set of relevant parameters can be obtained directly from SLA statements or other description about the service, available from the CSP. Instead, the second group can be extracted from the session histories or logs. A customer needs to obtain at least one pre-SLA parameter to estimate initial trust value of a CSP. However, measuring trustworthiness based on that is biased toward the single parameter and is not an advantageous solution. For this reason, a user should try to obtain and evaluate as many parameters as possible to obtain a complete trust value about a CSP. In addition, a third party auditor may also be involved in this assessment.

**(Marudhadevi et al., 2014)**. The work presents a *trust mining model* (TMM) to identify trusted cloud services while negotiating an SLA. The challenge for the user is to monitor the services provided from the CSP and check if they meet the conditions mentioned in the agreement. To perform this, the user needs further information such as prior data or knowledge about what is happening on the CSP side, which can help him to better realize the effective QoS. The trust model evaluates the trust degree on the prior data obtained about the service at the time of the SLA. Then, this information is divided into multiple common attributes like the number of service denials, average response time, task success ratio and number of complaints registered by the users. Usually, attributes used to formulate any trust model can be either objective or subjective, while this work uses both types of values. In this way, advantages introduced with this approach are both for CSPs and end users. From one side, the CSP can monitor the performance and improve its services to establish better trust relations with the users. And from the other side, the customer can perceive as secure working with the CSP.

## 3.2 Recommendation Based

Recommended trust occurs when two entities, the trustor and the trustee have no previous interaction background with each other. In such a scenario, when there is no information that the end user can relate on, the trust relationship can be established by another entity's recommendation, usually a third-party auditor. In this way, end users can have a baseline to evaluate services or providers.

**(Kong and Zhai, 2012)**. The work proposes a particular mechanism, called *Trust-based Recommendation System in service-oriented Cloud computing* (TRSC), which evaluates CSP services based on the trust of them. In TRSC, the resulting trust value is obtained combining direct trust and recommendation trust. Direct trust of an user on a cloud service is computed as usual, that is according on the direct interaction. While the recommended trust is evaluated taking into account opinions coming from users, or other authority of the field, who are trusted by the user, considering that this kind of trust is more reliable.

**(Noor et al., 2013)**. The authors developed a platform for a credibility-based trust management of cloud services, called *Cloud Armor*. The key features of the presented platform are: i) usage of a web crawling approach to automatically discover cloud services; ii) an adaptive and robust credibility model to evaluate credibility of feedbacks; and iii) a trust-based recommender to recommend trustworthy cloud services that suit the users needs. Cloud Armor provides an environment where customers can give feedbacks and request trust assessment for a particular cloud service.

**(Rizvi et al., 2014)**. Aim of the authors is to propose objective trust model, since it involves third-party auditors to develop unbiased trust between CSP and users. In this way, customers have a baseline to assess services and CSPs. In this case, third-party auditor assigns score for each CSP, basing on predetermined criteria significant to trust. More precisely, when a CSP is willing to enter the cloud market, it ap-

plies to be scored by the third-party auditor. The evaluation can be done using different set of criteria, such as those proposed by CSA (Cloud Security Alliance, 2013). However, when scoring a CSP, the customer feedback is taken into account too. For each criteria identified and evaluated by the third-party auditor, the obtained score will be integrated with feedback coming from end users. Like other recommendation-based systems, the approach used in this case is similar to ones adopted by the e-commerce trust models.

**(Singh and Chand, 2014)**. This work proposes a trust evaluation framework able to determine final trust of CSP. The mechanism takes into account, in addition to the user's past experiences, also friends and third party's recommendations. The proposed solution has been simulated through a typical cloud computing scenario.

Similar recommendation based models can be found in (Han et al., 2009) and (Li and Ping, 2009).

## 3.3 Reputation and Feedback Based

Even if some work in literature discusses about this two groups in a separate way, we prefer to refer to them as a whole class. Because of their similarity, in this way the aim is avoiding ambiguity. The reputation of an entity is the aggregated opinion of a community towards that entity (Huang and Nicol, 2013). Thus, an entity with high reputation is the one trusted by various entities in the community. In this way, an entity that needs to retrieve trust opinion on a trustee, may use the reputation to evaluate the trust level of that subject. The reputation of a CSP helps end users (especially individual users) in choosing a cloud service from many options without particular requirements. A similar approach is defined as "social trust". As already said, this group includes trust models that collect feedback and opinions from other users, evaluating the trust on services and providers. Trust model collects and manages the feedback regarding different QoS and security parameters offered by CSPs. Based on this information, users will prefer the CSP that guarantees all the necessary QoS and security attributes for its customers.

**(Krautheim et al., 2010)**. In this work, a trust model called *Trusted Virtual Environment Module* (TVEM) is presented as a software appliance. For cloud environments already provided with Trusted Platform Module (TPM) virtualization techniques, TVEM introduces better features like improved application program interface (API), cryptographic algorithm flexibility, and a configurable modular architecture. Also a unique Trusted Environment Key is introduced, combining trust from the information owner, and the CSP to create a dual root of trust for the TVEM that is distinct for every virtual environment and separate from the platforms trust. The TVEM software is protected by hardware enforced memory and process isolation via Intels Virtualization Technology for Directed I/O (VT-d) (Abramson, 2006) and Trusted eXecution Technology (TXT) (Intel Corporation, 2010).

**(Habib et al., 2011)**. This paper describes a trust model based on prepositional logic terms (PLT), called multi-faceted trust management system, to help the cloud service customers to assess trustworthy CSPs. Aim of the proposed solution is to model ambiguity of trust information collected from various sources using a specific set of QoS properties like security, latency, availability, and customer support. The trust model becomes able to integrate two different trust management techniques including reputation and recommendation where logic operators are used.

**(Noor and Sheng, 2011)**. This approach overviews the design and implementation of a Trust as a Service framework. The proposed system is based on a credibility model, responsible for distinguishing between the believable and the malicious trust feedbacks, taking into account the majority consensus of feedbacks too. In addition to the credibility model, the other salient feature of the discussed framework is that it allows trust feedback assessment and storage to be managed distributively, avoiding common drawbacks of centralized architectures.

**(Pawar et al., 2012)**. The authors propose an uncertainty model, which calculates trust values based on different parameters, namely (i) SLA monitoring compliance, (ii) service provider ratings, and (iii) service provider behavior. More in detail, the SLA monitoring defines the opinion about a CSP from the established SLAs about its services. Each of them are provided with a single SLA that includes several common indicators, such as CPU, memory, disk space usage, number of virtual machines. For each indicator of an SLA, a monitor evaluating the compliance/non-compliance of the indicator is provided. Then, CSP ratings are determined with the computation of all ratings, based on consensus and conjunction ratings. To calculate trust values, the model take into account features like belief, disbelief, uncertainty, and base rate.

Similar approaches can be found in (Firdhous et al., 2011a), (Firdhous et al., 2011b), and (Wang et al., 2014). Before the rise of cloud computing, other reputation-based techniques have been developed in the following trust models: *Peertrust* (Xiong and Liu, 2004), *Trummar* (Derbas et al., 2004), *Patrol-F* (Tajeddine et al., 2006), *Patrol* (Tajeddine et al., 2007), and *CuboidTrust* (Chen et al., 2007).

### 3.4 Biological Techniques

Approaches coming from biological sciences have been recently introduced to improve the definition of trust models for cloud computing. Since this activity is a complex task, the application of this kind of algorithms and techniques that have already been used in fields different from the biological one.

**(Wang et al., 2010a)**, **(Wang et al., 2010b)**. The proposed model discussed in these works is inspired by the biologic gene technique. The discussed solution, called *Cloud Trust model based on Family Gene* (CTFG), is composed of three steps: initialization, identification, and the assignment of the family gene system in the cloud. The work proposes also a formal definition of a model and correlation conception of family gene, cloud family, trust relation, gene identification, and gene assignment.

**(Firdhous et al., 2012a)**. The authors propose that the Bees Algorithm that was used to solve issues in diverse fields could be successfully adapted to address the trust issue in the cloud computing system. The Bees Algorithm is a population based search and optimization algorithm developed based on the food foraging behaviour of honey bees. The work is inspired by some comparative studies carried out on cloud computing and the bees environments.

Another work, referring to trust management in P2P networks, can be found in (Wang et al., 2006) where the authors describe a reputation based trust model inspired by swarm intelligence paradigm.

## 4 DISCUSSION

As previously discussed, the first step of cloud computing adoption is the end user choice: when a customer needs to decide if he can entrust a particular CSP or not. This becomes way more relevant when the decision involves confidential or sensitive data.

For what concerns policy based models, in particular those which rely on SLAs, a major concern can be identified since SLAs rarely focus on characteristics such as security and privacy, concentrating on elements easier to assess and to monitor too. These last features include the set of service performances such as network bandwidth, services uptime, usage condition of virtual machine, and so forth. Moreover, there is a lack of tools for end users to effectively verify SLA conditions observance. Action that, in many cases, may be performed by a third-party auditor.

About the recommendation based models, some constraints emerge because of the lack of a standardization process: from one side the selection of which criteria about services provided by a CSP are suitable to be evaluated and then be recommended is tricky; and from the other side, how and by whom a third-party auditor could be professionally certified is not always clear.

For reputation based models, the main limitation is usually the improbable chance to retrieve a huge number of customers to evaluate the CSP, giving a specific rate, for a wide set of complex and detailed criteria. So, in this case, more efforts need to be focused on criteria definition. Moreover, cloud customers do not get any kind of reward for giving their feedback, which is another important challenge for reputation based approaches.

What arises from the presented scenario is that management, mitigation and solving of presented limitations, through the definition of complex trust models, can actually represent the key enabler to boost cloud computing adoption, where constrained because of trust reasons. A correct and wise definition of trust models can surely help customers in the selection process of the CSP that is providing more trustworthy services.

## 5 CONCLUSIONS

After giving an exhaustive analysis of the origin of trust relationships management and its relevance in the cloud computing scenario, we presented major contributions to address the issue. Actually, cloud computing environment still presents trust issues as an ambiguous area, representing a barrier to cloud adoption for particular real cases. A higher trust can attract customers that currently are avoiding cloud solutions because they are afraid for their data and seeking a greater confidence level. The lack of a commonly reliable and efficient trust evaluation system is to consider a major issue. Several trust models have been proposed and discussed, but what is missing is an accepted criteria to evaluate the effectiveness of such models for a cloud computing scenario.

As future work, it could be of particular interest realize a systematic literature review on trust models, also considering accountability (Pearson, 2011; Jaatun et al., 2014): the work might settle an exhaustive analysis of the trust management scenario for cloud paradigm. Furthermore, another important issue to address is represented by the trust evaluation and definition of trust models for multi-cloud environments. In this case, the assessment of trustworthiness of multi-cloud service providers is more complex and may be achieved with different approaches compared to single-cloud scenario.

# REFERENCES


Abramson, D. (2006). Intel virtualization technology for directed i/o. *Intel technology journal*, 10(3):179–192.

Alhamad, M., Dillon, T., and Chang, E. (2010). Sla-based trust model for cloud computing. In *Network-Based Information Systems (NBiS), 2010 13th International Conference on*, pages 321–324. IEEE.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., et al. (2010). A view of cloud computing. *Communications of the ACM*, 53(4):50–58.

Blaze, M., Feigenbaum, J., and Lacy, J. (1996). Decentralized trust management. In *Proceedings., 1996 IEEE Symposium on Security and Privacy*, pages 164–173. IEEE.

Chakraborty, S. and Roy, K. (2012). An sla-based framework for estimating trustworthiness of a cloud. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, pages 937–942. IEEE.

Chen, R., Zhao, X., Tang, L., Hu, J., and Chen, Z. (2007). Cuboidtrust: a global reputation-based trust model in peer-to-peer networks. In *Autonomic and Trusted Computing*, pages 203–215. Springer.

Cloud Industry Forum (2014). Cloud uk: Uk cloud adoption snapshot & trends for 2015, the normalisation of cloud in a hybrid it market. http://cloudindustryforum.org/downloads/whitepapers/CIF_WP_14.pdf. Accessed: 2014-12-15.

Cloud Security Alliance (2011). Cloud security alliance - security, trust & assurance registry (star). https://cloudsecurityalliance.org/star/. Accessed: 2014-12-15.

Cloud Security Alliance (2013). The notorious nine cloud computing top threats in 2013. https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf. Accessed: 2014-12-15.

Cloud Security Alliance (2014a). Cloud security alliance - cloud controls matrix (ccm). https://cloudsecurityalliance.org/research/ccm/. Accessed: 2014-12-15.

Cloud Security Alliance (2014b). Cloud security alliance - consensus assessments initiative questionnaire (caiq). https://cloudsecurityalliance.org/research/cai/. Accessed: 2014-12-15.

Cloud Security Alliance (2014c). Cloud security alliance website. https://cloudsecurityalliance.org/. Accessed: 2014-12-15.

Derbas, G., Kayssi, A., Artail, H., and Chehab, A. (2004). Trummar - a trust model for mobile agent systems based on reputation. In *Pervasive Services, 2004. ICPS 2004. IEEE/ACS International Conference on*, pages 113–120. IEEE.

European Commission (2011). Attitudes on data protection and electronic identity in the european union. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf. Accessed: 2014-12-15.

Firdhous, M., Ghazali, O., and Hassan, S. (2011a). A trust computing mechanism for cloud computing. In *Kaleidoscope 2011: The Fully Networked Human?-Innovations for Future Networks and Services (K-2011), Proceedings of ITU*, pages 1–7. IEEE.

Firdhous, M., Ghazali, O., and Hassan, S. (2011b). A trust computing mechanism for cloud computing with multilevel thresholding. In *Industrial and Information Systems (ICIIS), 2011 6th IEEE International Conference on*, pages 457–461. IEEE.

Firdhous, M., Ghazali, O., and Hassan, S. (2012a). Applying bees algorithm for trust management in cloud computing. In *Bio-Inspired Models of Networks, Information, and Computing Systems*, pages 224–229. Springer.

Firdhous, M., Ghazali, O., and Hassan, S. (2012b). Trust management in cloud computing: A critical review. *arXiv preprint arXiv:1211.3979*.

Gambetta, D. (1988). Trust: Making and breaking cooperative relations.

Grandison, T. and Sloman, M. (2000). A survey of trust in internet applications. *Communications Surveys & Tutorials, IEEE*, 3(4):2–16.

Habib, S. M., Ries, S., and Muhlhauser, M. (2011). Towards a trust management system for cloud computing. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on*, pages 933–939. IEEE.

Han, S.-M., Hassan, M. M., Yoon, C.-W., and Huh, E.-N. (2009). Efficient service recommendation system for cloud computing market. In *Proceedings of the 2nd international conference on interaction sciences: information technology, culture and human*, pages 839–845. ACM.

Huang, J. and Nicol, D. M. (2013). Trust mechanisms for cloud computing. *Journal of Cloud Computing*, 2(1):1–14.

Intel Corporation (2010). Enhanced data protection with hardware-assisted security - intel trusted execution technology. http://www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution-technology/malware-reduction-general-technology.html. Accessed: 2014-12-15.

Jaatun, M. G., Pearson, S., Gittler, F., and Leenes, R. (2014). Towards strong accountability for cloud service providers. In *Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on*, pages 1001–1006. IEEE.

Kanwal, A., Masood, R., Ghazia, U. E., Shibli, M. A., and Abbasi, A. G. (2013). Assessment criteria for trust models in cloud computing. In *Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing*, pages 254–261. IEEE.

Kong, D. and Zhai, Y. (2012). Trust based recommendation system in service-oriented cloud computing. In *Proceedings of the 2012 International Conference on Cloud and Service Computing*, pages 176–179. IEEE Computer Society.

KPMG International (2013). Breaking through the cloud adoption barriers. http:// www.kpmg.com/ Global/en/IssuesAndInsights/ArticlesPublications/ cloud-service-providerssurvey/Documents/cloud-service-providerssurvey.pdf. Accessed: 2014-12-15.

Krautheim, F. J., Phatak, D. S., and Sherman, A. T. (2010). Introducing the trusted virtual environment module: a new mechanism for rooting trust in cloud computing. In *Trust and Trustworthy Computing*, pages 211–227. Springer.

Kumar, V., Chejerla, B., Madria, S., and Mohania, M. (2013). A survey of trust and trust management in cloud computing. *Managing Trust in Cyberspace*, page 41.

Li, W. and Ping, L. (2009). Trust model to enhance security and interoperability of cloud environment. In *Cloud Computing*, pages 69–79. Springer.

Marudhadevi, D., Dhatchayani, V. N., and Sriram, V. S. (2014). A trust evaluation model for cloud computing using service level agreement. *The Computer Journal*, page bxu129.

Mell, P. and Grance, T. (2011). The nist definition of cloud computing.

Nissenbaum, H. (1999). Can trust be secured online? a theoretical perspective.

Noor, T. H. and Sheng, Q. Z. (2011). Trust as a service: A framework for trust management in cloud environments. In *Web Information System Engineering–WISE 2011*, pages 314–321. Springer.

Noor, T. H., Sheng, Q. Z., Ngu, A. H., Alfazi, A., and Law, J. (2013). Cloud armor: a platform for credibility-based trust management of cloud services. In *Proceedings of the 22nd ACM international conference on Conference on information & knowledge management*, pages 2509–2512. ACM.

Pawar, P. S., Rajarajan, M., Nair, S. K., and Zisman, A. (2012). Trust model for optimized cloud services. In *Trust Management VI*, pages 97–112. Springer.

Pearson, S. (2011). Towards accountability in the cloud. *Proc. IEEE Internet Computing*, pages 64–69.

Pearson, S. and Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. In *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on*, pages 693–702. IEEE.

Perez, J. M. M., Bernabe, J. B., Calero, J. M. A., Clemente, F. J. G., Perez, G. M., and Skarmeta, A. F. G. (2014). Taxonomy of trust relationships in authorization domains for cloud computing. *The Journal of Supercomputing*, pages 1–25.

Rizvi, S., Ryoo, J., Liu, Y., Zazworsky, D., and Cappeta, A. (2014). A centralized trust model approach for cloud computing. In *Wireless and Optical Communication Conference (WOCC), 2014 23rd*, pages 1–6. IEEE.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., and Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of management review*, 23(3):393–404.

Sanchika Gupta, P. K. and Abraham, A. (2013). Cloud computing: Trust issues, challenges, and solutions. *Managing Trust in Cyberspace*, page 13.

Sato, H., Kanai, A., and Tanimoto, S. (2010). A cloud trust model in a security aware cloud. In *Applications and the Internet (SAINT), 2010 10th IEEE/IPSJ International Symposium on*, pages 121–124. IEEE.

Singh, S. and Chand, D. (2014). Trust evaluation in cloud based on friends and third party's recommendations. In *Engineering and Computational Sciences (RAECS), 2014 Recent Advances in*, pages 1–6. IEEE.

Solhaug, B. and Stølen, K. (2012). Uncertainty, subjectivity, trust and risk: How it all fits together. In *Security and Trust Management*, pages 1–5. Springer.

Tajeddine, A., Kayssi, A., Chehab, A., and Artail, H. (2006). *PATROL-F - A comprehensive reputation-based trust model with fuzzy subsystems*. Springer.

Tajeddine, A., Kayssi, A., Chehab, A., and Artail, H. (2007). Patrol: A comprehensive reputation-based trust model. *International Journal of Internet Technology and Secured Transactions*, 1(1):108–131.

Wang, T., Ye, B., Li, Y., and Yang, Y. (2010a). Family gene based cloud trust model. In *Educational and Network Technology (ICENT), 2010 International Conference on*, pages 540–544. IEEE.

Wang, T., Ye, B., Li, Y., and Zhu, L. (2010b). Study on enhancing performance of cloud trust model with family gene technology. In *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on*, volume 9, pages 122–126. IEEE.

Wang, W., Zeng, G., and Yuan, L. (2006). Ant-based reputation evidence distribution in p2p networks. In *Grid and Cooperative Computing, 2006. GCC 2006. Fifth International Conference*, pages 129–132. IEEE.

Wang, X., Su, J., Hu, X., Wu, C., and Zhou, H. (2014). Trust model for cloud systems with self variance evaluation. In *Security, Privacy and Trust in Cloud Systems*, pages 283–309. Springer.

Xiong, L. and Liu, L. (2004). Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. *Knowledge and Data Engineering, IEEE Transactions on*, 16(7):843–857.

Zhu, H., Bao, F., and Deng, R. H. (2003). Computing of trust in distributed networks. *IACR Cryptology ePrint Archive*, 2003:56.