

Centralized Access Management and Monitoring as a Service in Cloud Environments-A Critical Study

Ajay Prasad¹ & Prasun Chakrabarty²

¹ Sharda University, Greater Noida, India

² Sir Padampat Singhania University, Udaipur, India

Correspondence: Ajay Prasad, Department of IT, Sharda University, Greater Noida, India. E-mail: ajayprasadv@gmail.com; Prasun Chakrabarty, Sir Padampat Singhania University, Udaipur, India. E-mail: prasun.chakrabarti@spsu.ac.in

Received: July 9, 2012 Accepted: April 20, 2013 Online Published: April 26, 2013

doi:10.5539/cis.v6n2p126

URL: <http://dx.doi.org/10.5539/cis.v6n2p126>

Abstract

The aspect of virtualization and large scale distribution has brought forward the cloud computing phenomenon. Despite its popularity, most of the enterprises are still circumspect in getting into clouds completely. The major part of this circumspection owes to the factors of identity and access management, monitoring, auditing and reporting. The traditional access management will not suffice in the cloud context naturally. Also, every enterprise needs to monitor its employees as well as usage of services which will also assist in auditing. It will be better to have centralized monitoring clubbed with a centralized access management at the enterprise which coordinates with access management and monitoring as a service at the provider.

Keywords: cloud computing, security, centralized access management, monitoring, monitoring as a service

1. Introduction

1.1 About the Cloud Subject

Cloud with its name gives vague or rather confusing idea about its structure and form. But, as defined in Wiki, (2012a) "Cloud Computing is the delivery of computing as a service rather than a product where by shared resources, software and information are provided to computers and other devices as a metered service over a network (typically internet)". Practically, the services of cloud are provided through large data centers proprietarily maintained by organizations which are termed as cloud service providers. The cloud services are categorized in IaaS, PaaS and SaaS. Cyber Infrastructure (Mladen, 2008), thus is a vital part and that leads to the metered (Wiki, 2012a) services wherein the end users are required to pay for the services according to the usage. Evolving from a very primitive batch processing system to a highly distributed cloud computing is exciting and overwhelmingly lucrative in terms of cost efficiency. Cloud computing has attracted lots of attention these days which makes it even more necessary to assess it on the basis of issues and challenges pertaining to its usability, effectiveness and handling of user centric aspects and concerns.

In fact, the Cloud subjects the computing world into a vast arena of research because of its newness and vagueness. Identifying issues into a cloud is quite a task, taking into account the fact that the services are highly distributed and still organizations as end users are looking at it with suspicion and have not accepted it fully so that it can be assessed to satisfaction. Figure 1 also shows various users of cloud ranging from service authors to service users. The concerns falling in each user categories/purview are quite different and are unclear in many respects. But, as we know virtualization is the main aspect of cloud and hence the service users using SaaS as well as developers using PaaS will be the most concerned lot and does require satisfactory and viable answers/solutions to their concerns from the providers.

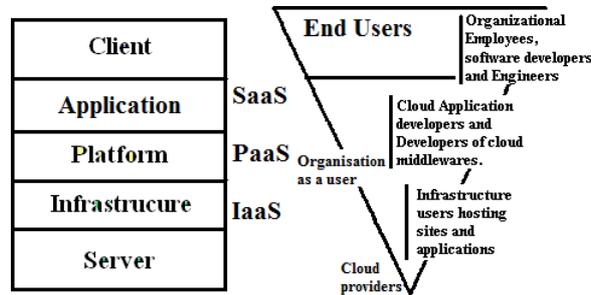


Figure 1. Cloud computing layers and users hierarchy

1.2 Scope of the Paper

As will be discussed in the forth coming sections, access management, monitoring and auditing are aspects which are concerning the users a lot. Moreover, if we view a user as an organization and not as an individual, then, too many perceptions and scopes open up with the access management. It is always a matter of great concern for an enterprise to keep vigilance on its employees to ensure proper usage of resources as well as to avoid malpractices which can affect the organizational working. We are hereby presenting a survey whereby aspects of security are discussed and further converging towards access management. Subsequently, the paper will focus towards the aspect of monitoring and will emphasize the need for centralized access management with centralized feature of monitoring. The paper mainly intends to draw attention towards monitoring in access management in clouds and propose a term 'Monitoring as a Service (MaaS)' into cloud computing. The final part of this paper is introducing an overview model for MaaS and analytical as well as survey methodology for assessing it.

2. Security in Clouds and IAM

2.1 Security Aspects in Cloud Computing

Microsoft provides a trustworthy Cloud (Microsoft Global Foundation services, 2009) by focusing on security and operational threats to businesses, set of security controls that mitigate risks and compliance framework. Microsoft has a dedicated OSSC (Microsoft Global Foundation services, 2009) team within Global Foundation Services to take care of security solutions for its online services. Many other Cloud Computing providers as listed in (Michael, 2012) like Amazon, Google, IBM, Citrix, VMware etc have been working to ensure security concerns in different ways. Microsoft (Microsoft Global Foundation services, 2009) views security to be handled in contexts of physical security, network security, data security, identity and access management, application security, host security auditing and reporting. These purviews can be mapped on to cloud user hierarchy mentioned in Mladen (2008) as shown in Figure 2.

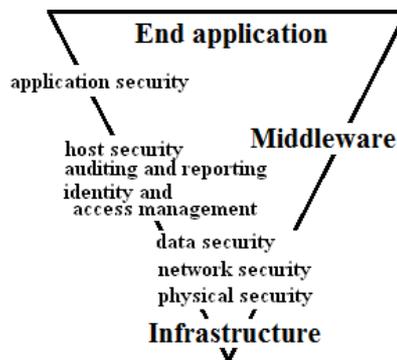


Figure 2. Security purview in clouds

2.2 Access Management and Monitoring

Access management, monitoring and auditing are highlighted as major points of concern and issues by most of the latest researchers (Ali Khajeh-Hosseini, Ian, & Ilango, 2010; Jay & Mark, 2008; Wiki, 2012b; Grobauer, Walloschek, & Stocker, 2011) in cloud security. Infact Ali Khajeh Hosseini and colleagues (Ali Khajeh-Hosseini, Ian, & Ilango, 2010) went further to mention that controlling and managing organizational employees as end

users will also be a issue worth discussing. Mostly the aspects of identity and access management and auditing and reporting require a base of physical, network and data security. Ensuring a trustworthy solution in base areas will automatically help in solving some of the problems in the upper areas (see Figure 3). However, R Chow et al. (Chow, Golle, Jakobsson, Shi, Staddon, Masuoka, & Molina, 2009) claims that the traditional access frameworks are unable to address multiple cloud resources and they don't naturally extend to clouds Most of the cloud solutions do have incorporated technologies pertaining the base areas (Yu, Wang, Ren, Lou, 2010; Sushil, Harrick, Sartaj, Mahadeo, & Bundit, 2010).

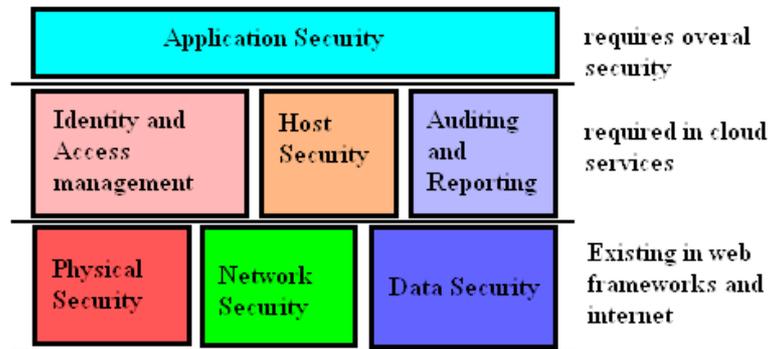


Figure 3. Security levels in cloud computing

However, it is the upper areas where most of compliance issues (concern C4 (Ali Khajeh-Hosseini et al., 2010)), data segregation, privileged user access, availability, recovery, investigative support and viability (Shubhashis, 2011) are encountered and needs to be addressed. Although the base areas of security are mostly handled and tested since the emergence of web services and distributed computing (Wiki, 2012b), the upper areas are the ones which are still trivially handled. Grobauer et al. (2011) the core cloud computing technologies revolve around web applications and services, virtualization IaaS offerings and cryptography. Sengupta et al. (2011) have very rightly addressed the security issues of cloud in form of concerns and implications. The C3 as put by Sengupta et al. is mostly pointing fingers to the authentication and authorization as talked about in (Microsoft Global Foundation services, 2009). The C4 falls under host security auditing and reporting as in (Microsoft Global Foundation services, 2009; Wang, 2010) and compliance issues as in (Jay et al., 2008). Access management needs to be addressed and at this point all the proposed access mechanisms in clouds are based on simple and sometimes singular aspect. Our observation is that, it is highly necessary that frameworks must be built around these core technologies so as to address systemic issues of access management in cloud environments.

2.3 Current Work in Access Management

At present the access management in clouds is mostly provided vividly and as a feature rather than a service by the clouds. Mostly present cloud providers make use of RBAC model complemented with underlying data centric policies, MAC/SLA model or a straight forward Access Control List (ACL) model. Yu et al. (2010) proposed a model which provides policy based access on the basis of data attributes by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. However, Proxy re-encryption is an overhead at the client computers. Mutual protection for cloud computing (MPCC) (Aiiad & William, 2010) follows a concept of reverse access control from user's to the providers unlike current Mandatory Access Control (MAC), Role Based Access Control (RBAC), and Discretionary Access Control (DAC) etc which is a bright approach though it needs to be assessed in terms of performance, viability and conformance. Ulrich Lang et al. (2010) suggests a model driven authorization system (openPMF), they also discuss the need and viability of security and conformance as a service in cloud architectures. A multi tenancy authorization system (Calero et al., 2010) authorization model works on the hierarchical RBAC, path based object hierarchies and federation.

With all the above models, a more centralized, automated and secure access management is the objective. But, most of the times access management issues are handled sparsely. That is, in most of the cases, all the issues are not taken care of. Identifying these issues and bringing all of them in one solution model is required. A systematic approach of listing the features and then modeling for the solution will be required. Henceforth, we are trying to identify the required features in access management over cloud environments.

3. Desired Features in Access Management

3.1 Need for Monitoring as a Service in Clouds

Cloud Security Alliance (CSA) in a document (Guidance for Identity & Access Management V2.1, 2010) emphasizes the need of centralized scheme for mapping corporate roles/policy to that of providers'. In this context still a centralized approach (of corporate policies and their mapping into provider's policies and deciding the access to the end users of the corporate) and dynamic as well as customizable policy mappings for cloud environments is still to be standardized and work needs to be done in this respect.

Shucheng et al. (2010) points towards the computation overheads on the data owner for key distribution and data management limiting the scalability with desirable fine grained and customized access policies.

Ulrich Lang (2010) stressed the fact that in identity and access management, authorization management must be atleast equally agile as cloud and the authorization system should be automated, manageable, fine grained and contextual. It also stressed the importance and scarcity of model driven security policy automation and reporting.

Jay Hieser et al. (2008) (Privileged user access) also suggests issues of organization while migrating on clouds has to be assessed as to how much control an organization would be having over its employees using cloud infrastructures. Also CSA (Guidance for Identity & Access Management V2.1, 2010) points out the need for logging control and access activities. Hence, proper authorization mechanism can also render proper auditing assistance to the providers as well as the user organizations. Our observation is that the aspect of putting monitoring in the context of authorization will help in auditing in many ways. Having monitoring and auditing support in the authorization and access framework can in many ways be conducive as well as viable for both service users as well as providers. Spring J. (2011) gives a broader perspective about monitoring in cloud while pondering through the cloud layers framed by CSA. Spring J stressed that long term monitoring can help extensive forensics as well as manageability. Middleware is the place where most of the role based access and monitoring is done and Spring J. also stressed the fact by mentioning it as most natural place to monitor as it mediates between application and OS. Our observation in this regard is that having a secure, long term and suitable monitoring is necessary and best fit with the IAM models. Also it is understood that users can ask for monitored or non monitored IAM as a service. Monitoring in access will also add to the trust value (Manuel, Thamarai, & Barr, 2009) between the user and the provider.

3.2 Desired Features along with Monitoring

Based on the above study, broadly, we can at this point state major requirements (features) that should be in a cloud access management:

1. Centralized roles/policy based;
2. Fine grained policies;
3. Automated;
4. Manageable;
5. Centralized Monitoring;
6. Multi-tenant;
7. Highly scalable;
8. Optimized in terms of performance;
9. Lesser computational overheads on the client side;
10. Increase in trust.

The aspect of centralized, fine grained and automated access mechanism is must for a large organization. The centralized access management will help in manageability and scalability. The automated digital signature process using X.509 PKI will ensure confidentiality. Also, a dynamic fine grained policy framework will help the organization to maintain customized policies that can be coordinated with the provider Access management services. Centralized access with monitoring as a service will help bring check in a great deal looking at the sudden burst (Andrew, n.d.) of internet and private lines (Figure 4) utilization in large corporate. Basically the Monitoring as a Service should have following properties in order to be efficient:

1. Substantial repositories
2. Long term Monitoring
3. Verifiable monitoring
4. Consistent time stamping

Repositories has to be maintained to keep records for long durations as well as the repositories has to maintained at both sides (users and providers). Consistent and appropriate time stamping has to be provided so that the digital signatures can be formulated keeping the time stamps in the plain text logs. The system must provide mechanisms and functions to verify logs so that it can't be manipulated by either side.

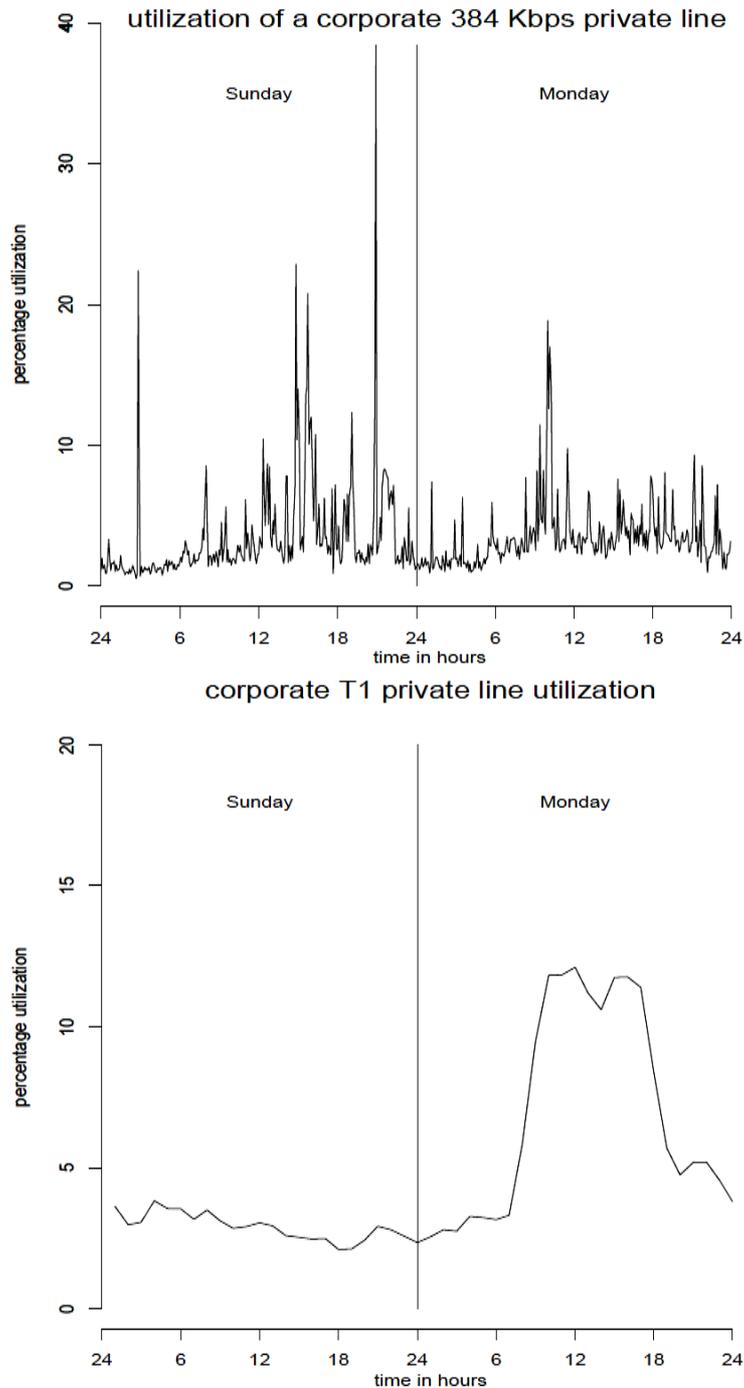


Figure 4. Sudden burst of network utilization in large organizations (courtesy: AT&T Labs – Research (Andrew, n.d.))

The logs and reports maintained at service providers, host systems and user systems are mostly short term and carry very little trust with them. Viewing this it becomes very important that a centralized repository is maintained in the purview of centralized monitoring which maintains the logs for substantially long term.

4. Overview Model of Access Management with Monitoring as a Service

4.1 Introducing the Model

Access management with monitoring can be implemented as a middleware at both user site as well as cloud site. A proper digitally signed procedure or dialogues can be formulated in order to verify a particular monitored report or logs. This would also bring a good amount of trust among the cloud users and providers. As shown in Figure 5 the monitoring is an independent module which processes the access requests to and fro from the end user to the middle-ware for authentication and authorization. The middleware will be responsible for the base activities like key exchanges, storing digital certificates, mapping roles and policies.

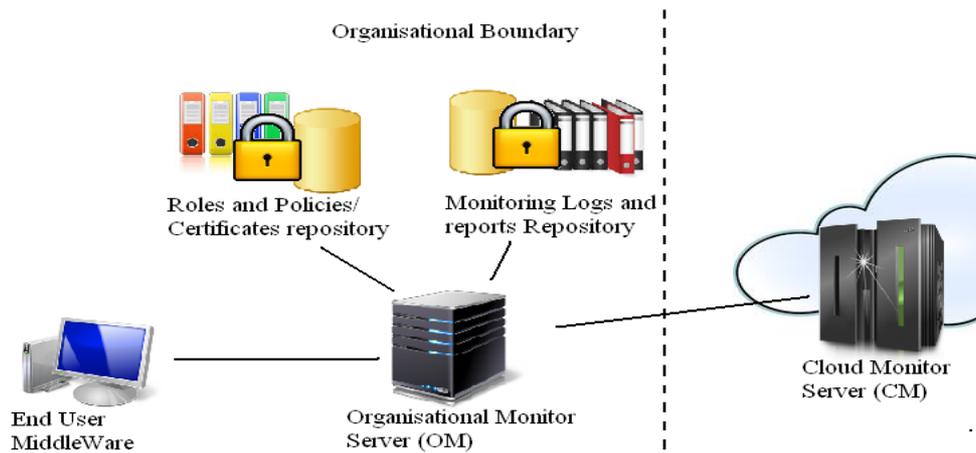


Figure 5 (a). Centralized monitor within organization

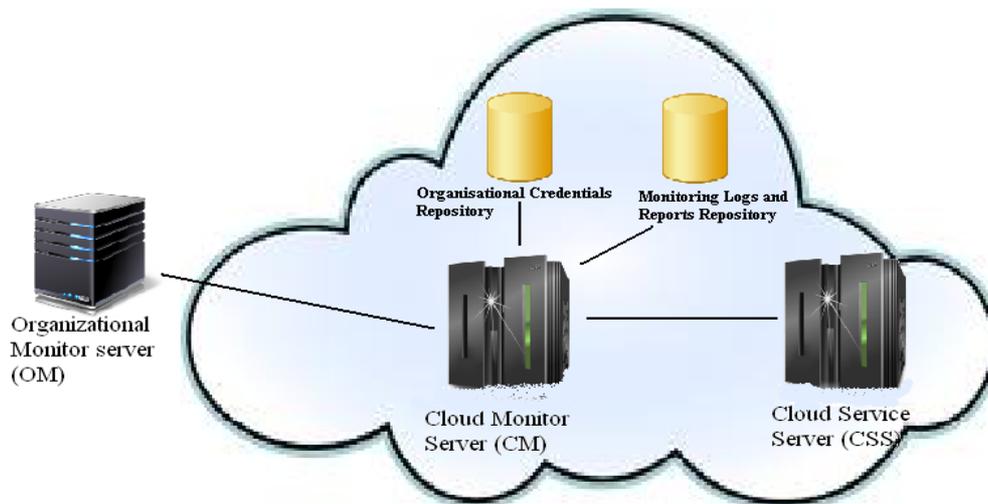


Figure 5 (b). Monitoring as a service by cloud providers

The monitor will be responsible to maintain roles and policies repository along with monitoring reports and logs. The monitor will forward only those requests further to access management which qualify the monitoring rules which can be set by the organization from time to time. The monitor will be like an access authentication gateway to the organizational users of cloud services. The monitor will be directly connected to the cloud for making a centralized authentication for every user. The middleware at every user node will be responsible to authenticate and authorize only after forwarded by the monitors. In the Figure 5 the middleware will be located at every user node. But, for every access the centralized roles and policies and use logs maintained at the monitor server will be effective. The access management middleware will come into play only after approval from the monitor. The providers of cloud services will also provide Access management and Monitoring as a service which will coordinate and communicate with the organizational monitoring server with specifically designed protocols. The

overall maintenance and logs will be made at both sides in order to verify digitally signed logs to avoid unauthorized manipulations in the logs.

Primarily, as shown in Figure 5 there would be five players in the centralized model.

1. End User (EU).
2. Middle Ware (MW).
3. Organizational Monitor (OM).
4. Cloud Monitor (CM).
5. Cloud Service Server (CSS).

The access parameters in the whole dialogues between the players will be:

1. User ID (UID).
2. Organization Ticket (OT).
3. Monitor Ticket (MT).
4. Use Ticket (UT).
5. Service ID (SID).
6. Log Volume (LV).
7. Start Time (ST).
8. End Time (ET).

Briefly, the user will sign in using UID and Service ID (SID), the middleware will forward it to the organizational monitor (OM) server which will verify the ID with the repositories and logs. The OM will then dispatch it along with the organization ticket (OT) to the cloud monitor server (CM) for use ticket (UT). The CM will verify the credentials and issue a use ticket (UT) along with log volume (LV where the logs are to be saved) by forwarding it to the cloud service server (CSS). The UT will be returned to the user MW through the OM and then the use of service will happen by the user. Upon closure the recording into the same log volume will take place in coordination with the OM and CM. The detailed model and analysis will be presented in the forth coming publications.

4.2 Assessing the IAM Model

Gregg et al. (2012) has formulated a set of questions which the users/organizations should ask the service provider before deciding upon a service provider and moreover before migrating onto clouds. These questions and, analyzing the feasibility of incorporating few of these in an automated access management can be done for making a better framework of access management in cloud. Manuel et al. (2009) suggests a framework for evaluating the trust worthiness of the grid/cloud resources considering the security levels, user's feedback values and performance criteria. The framework as suggested by Mannuel et al. (2009) can be used to testify any proposed model in lines of cloud access management and trust. As mention by Shucheng et al. (2010) the computation overheads pertaining to IAM must be minimized, thus, it is necessary to analyze every incorporated access management in clouds on the basis of performance also. Not much is available though to simulate cloud environments, but using cloudsim (Calheiros, Ranjan, Beloglazov, De Rose, & Buyya, 2011) can be handy as it provides help to simulate middleware by means of tools to model network behavior, federation of clouds, dynamic entity creation and dynamic workloads. Thus, performance of any proposed IAM model can be simulated using cloudsim so that its overall effect on QoS as well as cost can be studied and justified. However, other mathematical models can also be used to verify the simulations (Calheiros et al., 2011) and results.

5. Conclusion

Cloud computing is hot in terms of current day scenario in distributed computing. As suggested in many literatures the aspect of access management is of prime concern in cloud computing. Also, monitoring long term activities with appropriate verifiability is also primary and is unaddressed as a centralized implementation so far. The centralized Access Management must be fine grained automated and manageable as well as optimized in terms of performance. The monitoring in centralized form must have repositories with verifiability of long term logs with consistent time stamps at both sides. A model is introduced which mainly identifies major role players and overview dialogs among the role players. The centralized monitoring is appropriate only if it is supported by a MaaS by the service provider. Extra cost and performance issues will have to be analyzed and studied and the final optimized model has to be formulated in the subsequent papers.

References

- Aiiad, A., & William, C. (2010). Mutual Protection in a Cloud Computing Environment. *12th IEEE International Conference on High Performance Computing and Communications*.
- Ali Khajeh-Hosseini, Ian, S., & Ilango, S. (2010). *Research Challenges for Enterprise Cloud Computing*. Unpublished manuscript.
- Andrew, O. (n.d.). The low utilization and high cost of data networks. *AT & TLabs-Research*. Retrieved from <http://www.dtc.umn.edu/~odlyzko/doc/high.network.cost>
- Calero, J. M. A., Edwards, N., Kirschnick, J., Wilcock, L., & Wray, M. (2010). Toward a Multi-Tenancy Authorization System for Cloud Services. *Security & Privacy, IEEE*, 8(6), 48-55. <http://dx.doi.org/10.1109/MSP.2010.194>
- Calheiros, R. N., Ranjan, R., Beloglazov, A., De Rose, C. A. F., & Buyya, R. (2011). CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. *Software: Practice and Experience*, 41, 23-50. <http://dx.doi.org/10.1002/spe.995>
- Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009). Controlling data in the cloud: outsourcing computation without outsourcing control. *Proceedings of the 2009 ACM Workshop on Cloud Computing Security (CCSW 2009); 2009 November 13; Chicago, IL*. NY: ACM. pp. 85-90.
- Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding Cloud Computing Vulnerabilities. *Security & Privacy, IEEE*, 9(2), 50-57. <http://dx.doi.org/10.1109/MSP.2010.115>
- Guidance for Identity & Access Management V2.1. (2010). Retrieved from <http://www.cloudsecurityalliance.org/guidance/csaguide-dom12.pdf>
- Jay, H., & Mark, N. (2008). *Assessing the Security Risks of Cloud Computing*.
- Manuel, P. D., Thamarai, S. S., & Barr, M. I. A. E. (2009). Trust management system for grid and cloud resources. *Advanced Computing, 2009. ICAC 2009. First International Conference on, 13-15 Dec. 2*. pp. 176-181.
- Michael, G. (2012). *10 Security Concerns for Cloud Computing*. Retrieved January 2012, from <http://www.globalknowledge.ae/knowledge%20centre/white%20papers/virtualisation%20white%20papers/10%20security%20concerns%20for%20cloud.aspx>
- Microsoft Global Foundation services. (2009). *Securing Microsoft Cloud Infrastructure*. Retrieved May 2009, from <https://cloudsecurityalliance.org/securing-the-MS-Cloud.pdf>
- Mladen, A. V. (2008). Cloud Computing – Issues, Research and Implementations. *Journal of Computing and Information Technology*, 16(4), 235-246.
- Shubhashis, S., Vikrant, K., & Vibhu, S. S. (2011). Cloud Computing Security - Trends and Research Directions. *IEEE World Congress on Services*.
- Spring, J. (2011). Monitoring Cloud Computing by Layer, Part 1-Part 2. *Security & Privacy, IEEE*, 9(2), 66-68. <http://dx.doi.org/10.1109/MSP.2011.33>
- Sushil, K. P., Harrick, M. V., Sartaj, S., Mahadeo, P. J., & Bundit, T. (2010). Towards Analyzing Data Security Risks in Cloud Computing Environments. *Proc. Int'l Conf. Information Systems, Technology, and Management (ICISTM)*, Springer-Verlag, pp. 255-265.
- Ulrich, L. (2010). OpenPMF SCaaS: Authorization as a Service for Cloud & SOA Applications. In *Cloud Computing, Second International Conference, CloudCom 2010, November 30 - December 3, 2010, Indianapolis, Indiana, USA, Proceedings*. pp. 634-643, IEEE.
- Wang, C., Ren, K., Lou, W., & Li, J. (2010). Toward publicly auditable secure cloud data storage services. *Network, IEEE*, 24(4), 19-24. <http://dx.doi.org/10.1109/MNET.2010.5510914>
- Wiki. (2012a). *Cloud computing*. Retrieved January 2012, from http://en.wikipedia.org/wiki/Cloud_computing
- Wiki. (2012b). *Distributed Computing*. Retrieved January 2012, from http://en.wikipedia.org/wiki/Distributed_computing
- Yu, S., Wang, C., Ren, K., & Lou, W. (2010). Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing. *Proc. 29th IEEE Int'l Conf. Computer Comm.*, IEEE Press. pp. 534-542.