ISSN 2321-2926

Cloud Computing Architecture: A Framework

N. Santosh Ranganath

Assistant Professor, Dept. of Commerce and Management Studies, Dr.B.R.Ambedkar University, Srikakulam, Andhra Pradesh, India

Abstract: *Cloud computing has become an important platform for companies to build their infrastructures upon. If companies are thinking to take advantage of cloud based systems, they will have to seriously reassess their current security strategies as well as the cloud-specific aspects to be a successful solution provider. The focus of this study, based on existing literature, is to define a methodology for cloud providers that will protect users' data, information which is of high importance.*

On-demand provisioning of scalable and reliable compute services, along with a cost model that charges consumers based on actual service usage, has been an objective in distributed computing research and industry for a while. Cloud Computing promises to deliver on this objective: building on compute and storage virtualization technologies, consumers are able to rent infrastructure "in the Cloud" as needed, deploy applications and store data, and access them via Web protocols on a pay-per-use basis.

In addition to the technological challenges of Cloud Computing there is a need for an appropriate, competitive pricing model for infrastructure as a service. The acceptance of Cloud Computing depends on the ability to implement a model for value co-creation. In this paper, we discuss the need for valuation of Cloud Computing, identify key components, and structure these components in a framework. The framework assists decision makers in estimating Cloud Computing costs and to compare these costs to conventional IT solutions.

INTRODUCTION

Cloud computing is Internet based development and use of computer technology, whereby dynamically scalable virtualised resources are provided "services over the internet. Users need not have knowledge of, expertise in, or control over the technology infrastructure that supports them. The concept incorporates software as a service (SaaS), Web 2.0 and other recent, well-known technology trends, in which the common theme is reliance on the Internet for satisfying the computing needs of the users. An often-quoted example is Google Apps, which provides common business applications online that are accessed from a web browser, while the software and data are stored on Google servers. The cloud is a metaphor for the Internet, based on how it is depicted in computer network diagrams, and is an abstraction for the complex infrastructure it conceals.

Cloud is a term used to describe both a platform and type of application. A cloud Computing platform dynamically provisions, configures, reconfigures, and deprovisions servers as needed. Servers in the cloud can be physical machines or virtual machines. Advanced clouds typically include other computing resources such as storage area networks (SANs), network equipment, firewall and other security devices.

Cloud computing also describes applications that are extended to be accessible through the Internet. These cloud applications use large data centers and powerful servers that host Web applications and Web services. Anyone with a suitable Internet

ISSN 2321-2926

connection and a standard browser can access a cloud application.

A cloud is a pool of virtualized computer resources. A cloud can: Host a variety of different workloads, including batch-style back-end jobs and interactive, user-facing applications. Allow workloads to be deployed and scaled-out quickly through the rapid provisioning of virtual machines or physical machines, that allow Support redundant, self-recovering, highly scalable programming models that allow workloads to recover from many unavoidable hardware/software failures. Monitor resource use in real time to enable rebalancing of allocations when needed.

Cloud computing environments support grid computing by quickly providing physical and virtual servers on which the grid applications can run. Cloud computing should not be confused with grid computing. Grid computing involves dividing a large task into many smaller tasks that run in parallel on separate servers. Grids require many computers, typically in the thousands, and commonly use servers, desktops, and laptops. Clouds also support nongrid environments, such as a three-tier Web architecture running standard or Web 2.0 applications. A cloud is more than a collection of computer resources because a cloud provides a mechanism to manage those resources. Management includes provisioning, change requests, reimaging, workload rebalancing, deprovisioning, and monitoring.

Varieties of Cloud Computing

Cloud Computing is classified under various heads. On the basis of the type of usage or the location, it is classified under following heads:

1. Public Cloud - When a cloud is available to the general public on a pay-per-use basis, that cloud is called a ‘Public Cloud’. The customer has no visibility over the location of the cloud computing infrastructure. It is based on the standard cloud computing model. Examples of public cloud are Amazon EC2, Windows Azure service platform, IBM’s Blue cloud.

2. Private Cloud - The internal datacenters of business organizations which are not made available to the general public are termed as private cloud. As the name suggests, the private cloud is dedicated to the customer itself. These are more secured as compared to public clouds. It uses the technology of virtualization. A private cloud is hosted on the company’s own servers. Example of private cloud technology is Eucalyptus and VMware.

3. Hybrid Cloud - A combination of private and public cloud is called a hybrid cloud. Companies use their own infrastructure for normal usage and hire the cloud at events of heavy network traffic or high data load.

4. Community Cloud - In community cloud computing the cloud is shared between organizations of the same community or group. For example, government agencies of the same city can share the same cloud meant for the city however, agencies of other cities work on different cloud.

Cloud computing offers a wide range of applications and services to its users. Cloud services are offered on demand to the users on pay per use basis. The services offered ranges from processing and application integration and storage to communication services. The next classification of cloud computing is based on the type of service offered. These services can also be observed as different layers of cloud computing.

ISSN 2321-2926

1. Infrastructure as a Service (IaaS) - This is the primary and the bottom most layer of the cloud stack. This layer includes servers, networks and hardware appliance delivered as either infrastructure web services (for ex. AWS) or 'cloud centers' (for ex. Go Grid). The cloud provides an infrastructure including platforms (virtual), networks etc, on which applications can be placed. The consumers of IaaS could be system developers, system administrators, IT managers who deal in creating, installing, managing and monitoring IT infrastructure operations.

2. Platform as a Service (PaaS) - This being the second layer of the stack provides clouds platforms. At this layer, the cloud facilitates hardware resources, typically virtual machines which can be loaded with users' OS and software. This environment contains development language or framework like Java, .Net, Python, Ruby on Rails, etc. For example Google App Engine supports the Python framework, Microsoft Azure runs on .Net framework. PaaS consumers can use the tools and execution resources provided by cloud providers for developing, testing, deploying and managing applications serviced in a cloud environment.

3. Software as a Service (SaaS) - This is the top most layer of cloud stack. It refers to services that directly used by end users. At this layer, cloud provides software applications. You don't need to buy any software to use; instead of you can just use this from the SaaS provider's server through your browser. And you have to pay for the software as you make use of. The software applications are deployed as hosted services which the users can access via a network connecting SaaS providers and consumers.

CLOUD COMPUTING FRAMEWORK

Let us now take a glimpse as to what all comprises the cloud computing environment. The cloud computing environment is managed by five major performers or actors namely

- Cloud consumer; consumers (consumers, organizations) at the front end.
- Cloud provider; cloud service providers.
- Cloud auditor; party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementation.
- Cloud broker; party that negotiates relationships between cloud consumers and providers.
- Cloud carrier; intermediary for the transport of services between consumers and providers.

Acting and co-coordinating with each other these perform work in a three-layered framework as shown in the picture below:

The topmost layer is the service layer where the consumers consumes all the services being offered to them; SaaS, PaaS, IaaS. The middle layer is the resource abstraction and control layer. With this layer the consumers are provided with system elements to manage access to physical computing resources through software abstraction. The commonly used technology at this layer is the virtual machine technology. The lowest layer in the cloud computing framework is the physical resource layer which contains all the physical computing resources such as computers (CPU and memory), networks (routers, firewalls, switches, network links and interfaces), storage components like hard disk, power, etc.

Applications

Cloud computing can perform all operations possible on a normal computer of supplemented with the right middleware at the right time. This makes it a judicious technology with myriad applications.

- Unlimited access of data and applications from any part of the world.

- A cloud computing system reduces your cost of hardware. You can enjoy the access to fastest speed and processing without actually purchasing this hardware on your own. Moreover, no issues with the limited memory on your hard drive or flash drive. The cloud computing system manages it all.

- Cloud computing systems provide the organization to access the computer applications. The company needs to pay a metered fee to a cloud computing company instead of purchasing set of software licenses for each employee.

- Data back-up on the cloud

- Google's new chrome OS has used the concept of cloud computing, wherein users will be able to store their data online which can further be accessed and recovered from anywhere in the world from their cloud. It is integrated with applications like Google Docs, Google Calendar, Google Weather, Google Calculator, etc.

- Microsoft also headed the league with the launch of Windows Azure in 2009; an Operating System solely designed to allow developers to provide users with "Cloud Computing Technology" and products to use, on the fly.

- icloud is a cloud storage and cloud computing service introduced by Apple Inc. on June 6, 2011. It allows users to store data such as music files, videos etc on remote clouds (remote servers) which can later be downloaded into multiple Apple devices like iphones, ipads, iphones, and computers running Mac OS or Microsoft Windows.

CLOUD COMPUTING ARCHITECTURE

The majority of cloud computing infrastructure as of 2009 consists of reliable services delivered through data centers and built on servers with different levels of virtualization technologies. The services are accessible anywhere in the world, with The Cloud appearing as a single point of access for all the computing needs of consumers. Commercial offerings need to meet the quality of service requirements of customers and typically offer service level agreements, Open standards and open source software are also critical to the growth of cloud computing.

Tivoli Provisioning Manager automates imaging, deployment, installation, and configuration of the Microsoft Windows and Linux operating systems, along with the installation / configuration of any software stack that the user requests. Tivoli Provisioning Manager uses Websphere Application Server to communicate the provisioning status and availability of resources in the data center, to schedule the provisioning and deprovisioning of resources, and to reserve resources for future use. As a result of the provisioning, virtual machines are created using the XEN hypervisor or physical machines are created using Network Installation Manager, Remote Deployment Manager, or Cluster Systems Manager, depending upon the operating system and platform. IBM Tivoli Monitoring Server monitors the health (CPU, disk, and memory) of the servers provisioned by Tivoli Provisioning Manager.

DB2 is the database server that Tivoli Provisioning Manager uses to store the resource data. IBM Tivoli Monitoring agents that are installed on the virtual and physical machines communicate with the Tivoli Monitoring server to get the health of the virtual machines and provide the same to the user. The cloud computing platform has two user interfaces to provision servers. One interface is feature rich -- fully loaded with the WebSphere suite of products – and relatively more involved from a process perspective. For more information on this interface, One interface provides basic screens for making provisioning requests. All requests are handled by Web2.0 components deployed on the WebSphere Application Server.

CLOUD APPLICATION SERVICES

What's the difference between an application service and an infrastructure service? To answer this question, think first about the obvious distinction between applications and infrastructure: Applications are designed to be used by people, while infrastructure is designed to be used by applications. It's also fair to say that infrastructure usually provides a general, relatively low-level service, while applications provide more specific, higher-level services. An infrastructure service solves a broad problem faced by many different kinds of applications, while an application service solves a more targeted problem. And just as it's possible to identify different kinds of infrastructure services, it's also possible to distinguish different categories of application services, as this section illustrates.

a) SaaS Application Services

Users in most enterprises today rely on both purchased and home-grown applications. As these applications expose their services to remote software, they become part of the on-premises platform. Similarly, SaaS applications today frequently expose services that can be accessed by on-premises applications or by other cloud applications. Salesforce.com's CRM application, for example, makes available a variety of services that can be used to integrate its functions with on-premises applications. As organizations begin to create their own SaaS applications running on a cloud foundation, those applications will also expose services. Just as packaged and custom on-premises applications today are part of the on-premises platform, the services exposed by packaged and custom SaaS applications are becoming part of the cloud platform.

b) Search

Services exposed by SaaS applications are useful, but they're not the whole story. Other kinds of cloud application services are also important. Think, for example, of search engines such as Google and Live Search. Along with their obvious value to people, why can't they also offer cloud application services? The answer, of course, is that they can. Microsoft's Live Search, for example, exposes services that allow on-premises and cloud applications to submit searches and get results back. Suppose a company that provided a database of legal information wanted to let customers search both its own data and the Web in a single request. They could accomplish this by creating an on-premises application that both searched their proprietary data and, via the Live Search application service, the entire Web. It's fair to say that not many applications are likely to need this kind of service, but that's one reason why it's most accurate to think of search as an application service rather than an infrastructure service.

c) Mapping

Many Web applications today display maps. Hotel Web sites plot their locations, retailers provide store locators, and more. The people who create these applications probably don't have the time, interest, or budget to create their own mapping database. Yet enough applications need this function to justify creating a cloud application service that provides it. This is exactly what's done by mapping services such as Google Maps and Microsoft's Virtual Earth. Both provide cloud-based services that application developers can use to embed maps in Web pages and more. And as with search, these mapping services are adjuncts to existing Web sites that target users directly, i.e., they're cloud application services.

d) Other Application Services

Many other application services are available today. In fact, almost any Web site can expose its functionality as a cloud service for developers to use. Photo-sharing sites such as Google's Picasa and Microsoft's Windows Live Photo Gallery do this, for example, as do online contacts applications such as Google Contacts and Microsoft's Windows Live Contacts. One big motivation for exposing services is to make it easier to create mash-ups that exploit the functions of diverse Web applications. Vendors sometimes group cloud application services together under a common umbrella.

The services for accessing information in Google Contacts, Picasa, and more are all part of the Google Data APIs, for instance. Similarly, Microsoft groups several of its services together under the Live Platform brand, including Live Search, Virtual Earth, Windows Live Contacts, Windows Live ID, an Alerts service, a specialized storage service called Application-Based Storage, and several more. The line between cloud infrastructure services and cloud application services can sometimes be fuzzy.

General cloud storage services such as S3 and SSDS are clearly infrastructure, for example, as are cloud identity services. A mapping service such as Google Earth is just as clearly application-centric—only certain kinds of apps need it—as is a service like Live Search. But an Alerts service might be considered infrastructure, since it's more generally useful, and Windows Live ID is definitely infrastructure, even though Microsoft views both services as part of its Live Platform. Cloud platforms are a relatively new area, and so it shouldn't be surprising that defining a firm taxonomy is challenging. However you choose to view them, it's clear that cloud application services have an important role to play. Knowing what's available in the cloud should be a core competency today for everyone who designs and builds software.

LITERATURE REVIEW

"Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing (2009)" describes that "Cloud Computing has been envisioned as the next generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. This unique paradigm brings about many new security challenges, which have not been well understood. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. We first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for seamless integration of these two salient features in our protocol design.

"Data Management in the Cloud: Limitations and Opportunities, March 2009" is focused to discuss the limitations and opportunities of deploying data management issues on these emerging cloud computing platforms. We speculate that large scale data analysis tasks, decision support systems, and application specifically data marts are more likely to take advantage of cloud computing platforms than operational, transactional database systems (at least initially). We present a list of features that a DBMS designed for large scale data analysis tasks running on an Amazon-style offering should contain. We then discuss some currently available open source and commercial database options that can be used to perform such analysis tasks, and conclude that none of these options, as presently architected, match the requisite features. We thus express the need for a new DBMS, designed specifically for cloud computing environments.

"Security Guidance for Critical Areas of Focus in Cloud Computing, April 2009", is intended to provide security practitioners with a comprehensive roadmap for being proactive in developing positive and secure relationships with cloud providers. Much of this guidance is also quite relevant to the cloud provider to improve the quality and security of their service offerings. As with any initial venture, there will certainly be guidance that we could improve upon. We will quite likely modify the number of domains and change the focus of some areas of concern.

"Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control (2009)", "characterizes the problems and their impact on adoption. In addition, and equally importantly, we describe how the combination of existing research thrusts has the potential to alleviate many of the concerns impeding adoption. In particular, we argue that with continued research advances in trusted computing and computation-supporting encryption, life in the cloud can be advantageous from a business intelligence standpoint over the isolated alternative that is more common today.

"Crypto NET: Software Protection and Secure Execution Environment (2010)", describes protection of software modules which is based on strong encryption techniques, for example public key encryption and digital signature. These protected software modules are encapsulated in our designed XML file which describes a general syntax of protected software modules. In addition, our designed system also securely distributes software modules to authorized user. Secure software distribution system is based on well established standards and protocols like FIPS-196 based extended strong authentication protocol and SAML based authorization security policies. We also designed secure execution environment which is capable to execute signed and encrypted software modules, supports standard security services and network security protocols. These are: transparent handling of certificates, use of FIPS-201 compliant smart cards, single-sign-on protocol, strong authentication protocol, and secure asynchronous sessions".

"Security Issues for cloud computing (2010)" discusses security issues for cloud computing and present a layered framework for secure clouds and then focus on two of the layers, i.e., the storage layer and the data layer. In particular, the authors discuss a scheme for secure third party publications of documents in a cloud. Next, the paper will converse secure federated query processing with map Reduce and Hadoop, and discuss the use of secure co-processors for cloud computing. Finally, the authors discuss XACML implementation for Hadoop and discuss their beliefs that building trusted applications from untrusted components will be a major aspect of secure cloud computing.

"Deployment Models: Towards Eliminating Security Concerns from Cloud Computing (2010)" claims that Cloud computing has become a popular choice as an alternative to investing new IT systems. When making decisions on adopting cloud computing related solutions, security has always been a major concern. This article summarizes security concerns in cloud computing and proposes five service deployment models to ease these concerns. The proposed models provide different security related features to address different requirements and scenarios and can serve as reference models for deployment.

"A survey on security issues in service delivery models of cloud computing (2010)", discusses that the architecture of cloud poses such a threat to the security of the existing technologies when deployed in a cloud environment. Cloud service users need to be vigilant in understanding the risks of data breaches in this new environment. In this paper, a survey of the different security risks that pose a threat to the cloud is presented. This paper is a survey more specifically to the different security issues that has emanated due to the nature of the service delivery models of a cloud computing system.

"Addressing cloud computing security issues (2010)", aims at twofold; firstly to evaluate cloud security by identifying unique security requirements and secondly to attempt to present a viable solution that eliminates these potential threats. This paper proposes introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. The proposed solution calls upon cryptography, specifically Public Key Infrastructure operating in concert with SSO and LDAP, to ensure the authentication, integrity and confidentiality of involved data and communications. The solution, presents a horizontal level of service, available to all implicated entities, that realizes a security mesh, within which essential trust is maintained.

"Information security and cloud computing (2011)" gives a description of cloud computing followed by a general description of information security issues and solutions, and a brief description of issues linking cloud computing with information security. Security solutions must make a trade-off between the amount of security and its performance cost and impact on the end-user experiences. This is accentuated in a cloud computing environment where users desiring different levels of security share the same resources. An essential issue for cloud computing is the perception of security, which is beyond the simple technical details of security solutions. This paper includes a list of a few key information security challenges that also present significant research opportunities. Solving these key problems will encourage the widespread adoption of cloud computing.

"Security issues in cloud computing (2011)" mentions that Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Cloud computing has become a variable platform for companies to build their infrastructures upon. If companies are to consider taking advantage of cloud based systems, they will be faced with the task of seriously reassessing their current security strategy, as well as the cloud-specific aspects that need to be assessed. We outline here what cloud computing is, the various cloud deployment models and the main security risks and issues that are currently present within the cloud computing industry.

Problem Discussion

Outsourcing IT capabilities are a crucial and inevitable step for enterprises that want to survive in the currently high competitive climate. Until now most of the researches, that has been done so far, only consider the XaaS model only from a traditional IT outsourcing point of view rather than in the cloud computing context. This research will now include the evaluation of cloud solutions giving companies another possibility to outsource their IT resources.

Purpose & Objectives

The principal aim of this dissertation is to investigate the primary strategic issues in adopting cloud computing in an organisation. Following on from this research a roadmap will be developed that can be used to guide organisations through the process of successfully adopting or migrating to cloud computing. The purpose is now to see how the evaluation of cloud computing possibilities as an outsourcing option actually differs to traditional IT outsourcing. One aspect that needs to be covered with this purpose, is whether it is possible to evaluate the source through a cloud computing solution with the same concepts and theories used to evaluate traditional IT outsourcing.

- Document use cases for Cloud Computing in research for data storage and computing

- Develop guidance on the governance, legal and economic issues around using cloud services for storage and computing in academic research

- Make recommendations to JISC on possible further work in the area for data storage and computing

- Help business and governments to reap the cost benefits of cloud computing.

- While maintaining service availability, data confidentiality and integrity, privacy, transparency, accountability and responsibility.

- Creating trust and trust worthiness through promoting best practice and assurance standards

- Improving transparency on security practices to allow informed decisions

Methodology

With help of the theoretical framework, interviews have been launched with three companies to see what their general opinion and knowledge is on the evaluation of cloud computing and its maturity. Questions have been asked openly so that answers could not be directed or manipulated by the authors of the research. Extensive secondary research will be conducted. Acknowledged texts, standards documents, industry periodicals and white papers, analysts' reports and conference journals will be referenced. A critical analysis of the secondary research is applied in the formulation of the roadmap and framework proposed.

The data for this research will be collected from statements about privacy policy, acceptable use policy, terms of use and service level agreements available from the websites of the cloud vendors. In case of any such information missing from the websites, similar information will be sought via internet research of whitepapers, press releases and news articles of cloud computing in different IT magazines.

CONCLUSION

A new kind of application platform doesn't come along very often. But when a successful platform innovation does appear, it has an enormous impact. Think of the way personal computers and servers shook up the world of mainframes and minicomputers, for example, or how the rise of platforms for Ntier applications changed the way people write software. While the old world doesn't go away, a new approach can quickly become the center of attention for new applications. Cloud platforms don't yet offer the full spectrum of an on-premises environment. For example, business intelligence as part of the platform isn't common, nor is support for business process management technologies such as full-featured workflow and rules engines. This is all but certain to change, however, as this technology wave continues to roll forward.

Cloud platforms aren't yet at the center of most people's attention. The odds are good, though, that this won't be true five years from now. The attractions of cloud-based computing, including scalability and lower costs, are very real. If you work in application development, whether for a software vendor or an end user, expect the cloud to play an increasing role in your future. The next generation of application platforms is here. After challenging the theoretical framework against the data collected, the traditional IT outsourcing theories appeared to be valid also for the evaluation of cloud computing solutions. Some important concepts are added to the evaluation of cloud computing solutions in consequence of particularities present in the model. The research aim was to develop a roadmap that will enable successful adoption of cloud computing by organisations. Research evaluation was presented and the results and recommendation of the evaluation discussed.

REFERENCES

ANDREI, T. (2009): Cloud Computing Challenges and Related Security Issues;

ARMBRUST, M., FOX, A., et al. (2009): Above the clouds: A berkeley view of cloud computing [Technical Report]; University of California, Berkeley;

ARTZ, D. & GIL, Y. (2007) A survey of trust in computer science and the Semantic Web. Journal of Web Semantics, 5, 58-71.

AUDUN, J., SANG, et al. (2007) A survey of trust and reputation systems for online service provision. Decis. Support Syst., 43, 618-644.

BUYYA, R., YEO, C. S., et al. (2009) Cloud computing and emerging IT platforms: Vision, Hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25, 599 - 616.

CHELLAPA, R. (1997) Intermediaries in Cloud-Computing: A new Computing Paradigm. Cluster: Electronic Commerce.

CHOW, R., GOLLE, P., et al. (2009) Cloud Computing: Outsourcing Computation Without Outsourcing Control. 1st ACM Cloud Computing Security Workshop. ACM

CLOUDCOMPUTING (2010) Cloud Application Migration; cloudcomputing.sys-con.com, http://www.cloudcomputing.sys-con.com/node/1458739, 30/07/2010.

FARBER, D. (2008) Oracle's Ellison nails cloud computing; cnet news, http://news.cnet.com/8301-13953_10052188-80.html, 5/06/2010.

FELLOWS, W. (2008) Partly Cloudy, Blue-Sky THinking About Cloud Computing. Whitepaper. 451 Group

GAMBETTA, D. (2000) Can we trust. Trust: Making and Breaking Cooperative Relations, electronic edition, Department of Sociology, University of Oxford, 213-237.

GEELAN, J. (2009) Twenty-One Experts Define Cloud Computing. Cloud Computing Journal. Cloudcomputing.sys-con.com,12/4/2010 12/4/2010

HOGBEN, G. & CATTEDDU, D. (2009) Interoperability and Protection: Cloud Computing Benefits, Risks and Recommendations for Information Security. ENISA Quarterly Review.

HUSTINX, P. (2010) Data Protection and Cloud Computing under EU law; Panel IV: Privacy and Cloud Computing: in. Third European Cyber Security Awareness Day. BSA, European Parliament, European Parliament

IBM (2001): Autonomic Computing: IBM's Perspective on the State of Information Technology; IBM; 22

JEFFREY, K. & NEIDECKER-LUTZ, B. (2009): The future of Cloud Computing: opportunities for European Cloud Computing beyond 2010; 66

JENSEN, M. & SCHWENK, J. (2009) On Technical Security Issues in Cloud Computing. 2009 IEEE Conference on Cloud Computing. IEEE Computer Society

KRUKOW, K., NIELSEN, M., et al. (2008) Trust models in ubiquitous computing. Philosophical Transactions of the Royal Society A, 366, 3781-3793.

KRAUTHEIM, F. J. (2009) Private Virtual Infrastructure for Cloud Computing.

LUIS, M. V., LUIS, R.-M., et al. (2008) A break in the clouds: towards a cloud definition. SIGCOMM Comput. Commun. Rev., 39, 50-55.

MELL, P. & GRANCE, T. (2009a) The NIST Definition of Cloud Computing Version 15. National Institute of Standards and Technology

MELL, P. & GRANCE, T. (2009b) Perspective on Cloud Computing Standards. USA, NIST

MILLER, M. (2008) CLOUD COMPUTING: Web-Based Applications That Change the way You Work and Collaborate, Que Publishers.

REMPEL, J. K., HOLMES, J. G., et al. (1985) Trust in close relationships. Journal of Personality and Social Psychology, 49, 95-112.

SANTOS, N., GUMMADI, K. P., et al. (2009) Towards Trusted Cloud Computing. Max Planc Institute for Software Systems

VOONA, S. & VENKANTARATNA, R. (2009): Cloud Computing for Banks; Infosys Technologies Ltd;

VOUK, M. (2008) Cloud Computing - Issues, Research and Implementations. Journal of Computing and Information Technology.