World of Computer Science and Information Technology (WCSIT)
ISSN: 2221-0741
Vol. 1, No. 6, 247-252, 2011

A Study on the Readiness of Cloud Computing for Captious Computations

[1]Prof:GhantaSrinivasaRao,
Dept. Of CSE,Tenali Engineering College,
Tenali,AP,INDIA
Srghanta71@gmail.com

[2]Dr.ShaikNazeer,
Dept.of CSE, Bapatla Engineering College,.
Bapatla , AP,INDIA
shk_nazir@yahoo.co.in

[3]U.UshaRani,
Dept. of CSE,Tenali Engineering College,
Tenali,AP,INDIA.
usha.srinu@rediffmail.com

[4]Gogineni Vijay Krishna,
Dept.ofCSE,Tenali Engineering College,
Tenali,AP,INDIA.
vijay_gogineni@yahoo.co.in

Abstract— The emergence cloud computing in the computing arena has had major effect in way we utilize computing resources. It is being heralded by many as the new computing paradigm, coming with disruptive technologies which are expected to foster all sorts of innovations. However, further investigations suggest that cloud computing it is nothing new, rather an evolution of different existing technologies creatively integrated together. Therefore, it has inherited strengths and weaknesses of existing technologies, but has lowered the entry bar to computing making it an interesting proposition. In this paper we propose a security wrapper, which affords enough protection to the classified data as it flows in the cloud. The wrapper offers security to data in motion and at rest, and incorporates adaptive SLA negotiation.

Keywords- Cloud Computing; Security Wrapper; Cloud Providers; Service Level Agreement.

I. INTRODUCTION

The cloud computing model is composed of five characteristics, which are on-demand self service, broad network access, resource pooling, rapid elasticity and measured services. It has three service models; software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). Cloud computing can be deployed as a private cloud, community cloud, public cloud or hybrid cloud.

There is no agreement on its definition this has lead to all sorts of definitions being proposed. For example, NIST defines cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [24]. The lack of clear definition is a source of confusion in the design and implementation of cloud computing solutions.

While currently the use of cloud computing for personal use is widespread. Most researchers and practitioners recommend caution before using it for critical applications. Specifically, users or organizations are required to inquire on the following issues from the cloud providers: privileged user access, regulatory compliance – external security audits and security certifications, data location, data segregation and use of data protection routines such as encryption, recovery, investigative support and long term viability (hosting, scalability, instant provision and cost saving). Answers from these issues will allow them to make an informed decision on whether to move their sensitive data or critical applications to the cloud.

In the next few years Cloud computing spending worldwide will continue to grow. For example IDC predicts IT cloud service spending to grow from about $6 billion in 2008 to about $42 billion by 2012 accounting for 25 percent annual IT expenditure growth [16]. This growth highlights the potential of cloud computing in the technological development and the realization of the industry of the new kid in the computing garena.

Cloud computing has the potential to set a stage for company innovation (through networking, remote access and collaboration) as more resources are devoted to developing solutions rather than the traditional chores of maintenance and upgrades.

The main advantages of cloud computing are cost saving, high availability, and easy scalability [17]. It frees the use the user from the hassle of having to install and maintain the software at the cost of the user security, privacy and loss of control of platforms, data and information. Cloud computing lowers the cost of application development and makes the process to be truly distributed and scalable. This enables startups companies to enter the process at the lowest cost. There are still a number of challenges which cloud computing must address for it to be a success. These include reliability, security, privacy, user loss of control of data and

information, the additional cost of the necessary bandwidth, and the dangers of vendor lock-in into specific cloud vendor. Is cloud computing a disruptive scientific innovation we have been waiting, which is going to shake the foundations of computing and provide a paradigm shift? The challenges it faces are many and formidable, the computing industry and the academic community have their work cut out. However, the potential for being successful are huge, therefore it is a matter of time before we know the verdict on the future of cloud computing.

In this paper we analyze and provide solutions to the specific security challenges which must be addressed in the cloud. We propose a security wrapper which follows data as it transits in the cloud. The wrapper incorporates security mechanisms and adaptive service level agreements negotiations.

The rest of the paper is organized as follows. In section two we give background and related information to cloud computing. The data ownership, processing, control, movement and trust issues are discussed in section three Section four looks at the security challenges, possible attacks and proposed solutions in the cloud computing. Summary and conclusions are discussed in section five.

II. BACKGROUND AND RELATED INFORMATION

Conceptually cloud computing is attractive, because it means less management, more scalability, possibly broader access (particularly for companies with multiple locations, teleworkers and flexible working). However, there is a perception among consumers that the company computing infrastructure remains more secure and highly accessible when everything is held internally. This viewpoint is likely to be challenged by the technological trends that suggest cloud computing is the only game in town.

It is evident that the Cloud computing has the potential to be a game changer in the computing landscape. Research shows that it has attracted vendors, consumers and even governments. Major vendors providing cloud computing are Amazon [3], Google [14], Sales force [25] and Microsoft [18]. Other players include AppNexus [4], Go Grid [13], Grid Layer [15], Mosso [19], and XCalibre Communications [7]. It will become the foundation for a greatly expanded IT industry by lowering cost and technical barriers to developers and users alike. A key will be whether it overcomes the challenges it currently faces.

The use of cloud computing will be enhanced and extended by other seemingly unrelated computing paradigms such as Autonomics computing which is an initiative started by IBM to provide computing systems with ability to manage itself in computing landscape which is complex. Autonomics computing can help in addressing the following systems behavior in cloud computing [5]:

• Management of unpredictable system behavior and unforeseen user behavior and abuse.
• Better management of quality of service, primarily to gain greater confidence from the user community, thereby adding value to existing deployment.
• Better management of energy consumption.
• More effective resource management to supports capability so that resources behave elastically at higher usage levels.

The role of the traditional Operating Systems (OS) is changing with the advent of new computing approaches such as virtualization, cloud computing and other application development frameworks (ADF) which enable the faster development of applications that work with multiple Oss making traditional OS less important (key players in the ADF market include Django, Ruby on Rails and Microsoft Silverlight) [11]. This change will spur a rush towards new innovations and competition in the quest for producing a dominating Operating System. The obvious victim of this rush is likely to be security and privacy in OS. The usual story then repeats that once the Operating System is insecure the applications running on top will be insecure as well.

Cloud computing have ignited the old war on Operating Systems domination. In the last few years a lot of cloud aware operating systems have been made available. For example, the private cloud –Eye OS [10] and their collaboration with IBM. Google Chrome OS is another cloud OS that is more internet aware than most [20]. Part of the security scheme for Chrome is that it's hard to make any unauthorized changes to the system. The root file system, which stores the core files needed to make software run, is stored in a read-only format. On top of that, every time the user boots the machine, Chrome OS verifies cryptographic signatures that ensure that the operating system software is properly updated, and matches the build Google has approved. There is a great deal of truth that cloud providers like Google can maintain the security of systems better than individual companies. This specifically involves server security and not data security. The reasons for this are that companies must trust Google, the privacy of their data cannot be guaranteed and Google is much bigger and attractive target for hackers [28]. When you use cloud computing services, you are limiting yourself to the amount of advanced security tools that you can put on the system. Tools such as data leak prevention (DLP), and misuse and abuse detection. Further, you cannot limit the access to only internal staff. There are many other cloud security tools that cannot be put in place in cloud environments, unless the cloud environment is specifically designed for them [9]. You have little control over how much audit information is collected. For example, you likely do not have access to failed log-in attempts, so you cannot proactively look for attack reconnaissance. Likewise, while you may maintain the ownership of your own data, you do not likely own all of the access log data. That potentially creates legal problems. For example, if someone does illicitly access your information, you might need to get a court order to see where they are coming from. If however you maintained your data internally, you would have instant access to all this information.

A. Cloud Computing Challenges

Cloud computing is still relatively new and has not yet been widely adopted. There are a lot of challenges to be addressed by the computing industry and researchers.

Most of the Cloud computing resources will be based outside of the organization. Therefore its designs and platforms are controlled by the provider. More worrying is that users cannot change the platform's technology when they want, while providers can do so when and how they see fit in most cases without the consent of the users.

Performance concerns may prevent some companies from using cloud computing for transaction oriented and other data intensive applications.

Security and privacy are the main concerns when companies think of using cloud computing. This is because their business information and critical IT resources are outside the company firewall. Users worry about the security and privacy of their information should there be a security break. They want to be sure that providers follow standard security practices, which requires disclosure and inspection. For example, users do not want to share the same virtual hardware and network resources with multiple customers. Another concern is that information can be anywhere in the world, making it subjected to national and international data storage laws related to privacy and record keeping. Various governments or regional bodies such as EU, have privacy regulations that prohibit the transmission of some types of personal data outside their jurisdiction. In the last decade there have been significant improvements in the design and rollout of large bandwidth. However, depending on the model of cloud computing usage, the bandwidth cost can turn out being very high. For example, if a company makes a multi terabyte database available via cloud computing the cost can be prohibitive. There are few open cloud computing standards for elements and processes such as APIs, the storage server images for disaster recovery, and data import and export. This is hampering adoption by limiting portability of data and applications between systems. Portability will become more important as more cloud providers emerge and the market become more competitive. It can be difficult for companies to move from one provider to another or to bring back data into their internal systems. Even when they bring back data the efforts involved in reformatting data and Applica ions is going to be expensive as the company may be required to acquire new skills from outside the company.

As a part of the service level agreement (SLA), Cloud providers must demonstrate that their systems will provide the necessary audit and protection of user's information. They must be able to show how they keep unauthorized personnel from accessing user's information. In some cases providers have allowed third parties to conduct security audit and document in order that it can be used by potential customers to show the due diligence paid by the provider in securing its systems. Experience shows that it is not easy for cloud providers to demonstrate all these aspects in order to instill trust on the part of users.

Users should be realistic in their view of loss of control by comparing their ability against that of the third party in terms of supporting high availability, continuity, disaster recovery, power consumption, and the on-going management of technical and physical infrastructure. Therefore, demonstrating cloud computing benefits is going to be a hard task, especially in the light of high user expectations. Cloud computing usage is going to be a business driver and hence any considerable loss of service will have negative repercussions on the business.

Internet access is crucial for cloud computing provision. There are a lot of places in the world where the internet availability is still a problem. This issue must be resolved by the governments in order to ensure that there is equity in the availability of the internet. Therefore, technological, sociological and political challenges must be overcome for this to be a reality. Otherwise we are going to have a cloud computing divide which will consignee these communities to the dark ages of computing. The number of cloud providers is still very small to provide enough competition in the market place that will offer better quality of service and increase choice to users.

It is also true that some computing problems may not for the time being, be solved in the cloud. Problems such as high-end databases are better hosted within a dedicated environment or applications that process sensitive information.

B. Emerging Cloud Computing Standards and legislations

Benjamin Tom have in his paper on standards and how dysfunctional they are makes an observation that, the standards process is littered with vendor self interest, infighting and politics to such an extent that the merits and the emerging standards are watered down [27].Five cloud computing standards are emerging to provide interoperability and prevent vendor lock-in. The first standard is the Open Cloud Manifesto [22], which is a set of principles defining cloud computing and steps for keeping cloud systems interoperable. The Open Virtualization Format is the specification [1], proposed by the Distributed Management Task Force, which aims to make virtualization simpler by having vendors agree to metadata formats for virtual machines is the second standard. The third standard is being proposed by the Organization for the Advancement of Structured Information Standards [21]. The group that developed XML is working on specification for cloud deployment, management and security. The Open Cloud Computing Interface, proposed by the Open Grid Forum [23] is the standard application programming interface for cloud infrastructure systems is the fourth standard. The fifth set of standards is the Trusted Cloud, which are security standards for cloud computing, including identity management, under development by the Cloud Security Alliance [2]. There are currently no security standards for cloud computing, until such standards have been developed, and used effectively to measure provider services and enforce accountability, any failures will fall on the customer's in house IT organization. In understanding of this reality, companies should be careful about putting mission-critical and core processes into a

public cloud, and private cloud architectures should be designed to minimize any security concerns while realizing the benefits of cloud optimization. Governments and standards bodies should provide a well-coordinated support in the form of necessary standards, guidance, policy decisions, and issue resolution to ensure agencies have the necessary tools to efficiently plan and carry out migrations to cloud environments.

All Cloud providers use APIs that have the structure of Web services standards such as SOAP. The major problem with these APIs is that they are still proprietary because they use the provider's own semantics within the standards structures. This is going to have a major impact on user's ability to move their data from one provider to the next to avail of better services or cost. The threat of vendor lock-in becomes really in this mode of operation. In the long run innovation is going to suffer and cloud computing as a paradigm may not achieve its full potential.

In cloud computing there are a lot of concerns regarding data security, privacy, and legal compliance. Worse, data stored online has less privacy protection both in practice and under the law. It is the responsibility of the company to develop controls that ensures that the vendor chosen will have the appropriate controls in place and are in compliance with laws such as the Sarbanes-Oxley act, the Gramm-Leach-Bliley act, various regional data privacy regulations such as EU Directive 95/46/EC - The Data Protection Directive, and in some cases country specific regulations limitations.

III. DATA PROCESSING IN THE CLOUD AND SERVICE LEVEL AGREEMENT

There are several criteria used to charge user's such as time spend on the cloud system, level of consumption of resources such as bandwidth, data transferred, or storage space used. These charging mechanisms will improve and very likely become affordable as the cloud matures. Other forms of charging will be possible, such as security and privacy levels afforded to the data and the level of control to data by using audit or forensics tools.

A. Data ownership, control and trust

The question of data ownership is becoming more difficult and confusing by the day. For example in US once you submit data online you cannot claim ownership of it. Furthermore, the data can be sold modified without your consent. Users of cloud computing are worried and likely so that they lose control of their data and information. Closer analysis shows that data is given much better protection when in the hands of cloud service providers. The regulatory compliance requires that there is transparency in data and information processing. However, for the cloud computing to be successful then credibility and trust of the provider will be critical. We trust different providers with our data, but some of the data processed in cloud computing is sensitive and hence the reluctance of users .The problem is further compounded because along the information value chain, everyone "owns" either the tangible or intangible value of data depending on their role within or across elements of the value chain. These roles can be data creators, data providers, data enriches, data buyers, data consumers, data sponsors, and data regulators. It is therefore reasonable to assume that an individual or a group takes on one or more roles at any given point in time.

B. Data movement

The cloud computing infrastructure consists of servers at one location or distributed across many sites connected to the internet and host applications and user's data and information. They also include virtualization, grid, management, database and other types of software; user interfaces, API; a communication infrastructure for connecting to users over the internet or a private network; and a usage monitoring and billing mechanism. Clients usually use browsers or dedicated software to access the cloud applications which they control via APIs. This setup is designed to support multiple tenants with high service levels anytime and anywhere [17].

Data centers which are being built all over the world by Amazon, Microsoft, Intel, and Google are the largest power consumers [12]. However, data centers provide high density server solutions, flexible computing, thin provisioning and virtualization. The use of virtualization as core technique in cloud computing; saves power, space and increased utilization giving cloud computing its green credentials. Although, it is important to realize that virtualization creates a new set of formidable security and privacy problems. Moving data to the cloud invites a number of real dangers, particularly if organizations fail to apply restrictions and controls on their data that gets moved. These concerns and risks are not new; organizations have experienced them in traditional storage outsourcing, off shoring, and other forms of remote data access. Moving data to the cloud create challenges concerning ownership of assets, potential loss of control of data location, and accountability for data recovery and discovery. Moreover, the flexibility of being able to move data within and between clouds presents major problems and the following questions have not been answered adequately:

i. Where is your data now running after several fail over and migration?

ii. Are the data protection laws to which your company is subjected being upheld?

iii. Is what you are doing with the data legal in the territory in which you find your data and applications running?

According to Vinton Cerf [6] most of the digital data generated and stored is in the form that cannot last long. He suggests that we solve the problems of long-term storage, retrieval, and interpretation of our digital data. Cloud computing may provide tools for digital data interpretation which are backward compatible. This means that it may be possible to host in the cloud applications which have been phased out, do not have license or the vendor who wrote the application has gone out of business. The following are important questions to consider when data moves in the cloud. Is it possible to provide more security to sensitive data when it is outside the company control? Which security mechanisms will provide this security bubble? Can auditing and forensics functions be carried out by the customer or third party on sensitive data when it is on the cloud? Can secure delete

be achieved in the cloud? What about secure data migration?

IV.POSSIBLE ATTACKS TO THE CLOUD COMPUTING

In order to provide seamless access to resources user's data and information is stored and processed in cloud provider's servers or data centers. As a result users have limited or no control of their data and information. The loss of control of data and information and the inability to be able to conduct security audit is one of the major concerns and stumbling block in the wide usage and adoption of cloud computing. Other concerns are security and privacy.

Some of the questions which must be asked when evaluating the cloud computing alternatives include: what do you feel about the possibly having your proprietary business information in the same cloud as your competitor? What happens if there is a system failure – is the data secure? How reliable is your cloud provider? For example, it has been demonstrated [26] that it is possible to map the internal cloud infrastructure, identify where a particular target VM is likely to reside, and then instantiate new VMs until one is placed co-resident with the target. This then enables the attacker to mount cross-VM side-channel attacks to extract information from a target VM on the same machine [26]. Cloud computing uses the Web as a means to access the infinite resources it aims to provide. Using the Web leaves the data and information being processed vulnerable to Web information disclosure. Currently, there is no efficient countermeasure to this problem [8].

V. PROPOSED SOLUTION

The use of encryption in most of the current ICT infrastructure is a largely solved problem. When encryption is used in the cloud, it turns out to be a very challenging problem .Two of the factors contributing to make this problem difficult are lack of control and key management. In this work we propose a security and privacy wrapper that will protect data as it moves beyond the organization boundaries.

The wrapper will consist of basic security and privacy mechanisms, mechanism for adaptive SLA negotiations. For the wrapper to work it must have a learning module for understanding, for example, the change in location as illustrated in figure 1.

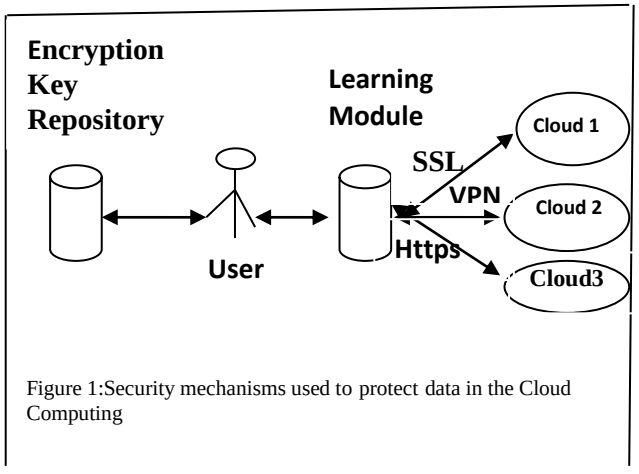

Figure 1:Security mechanisms used to protect data in the Cloud Computing

The proposed solution utilizes different types of security mechanisms in a multi-layered approach. The type of security mechanism used depends on the classification of data before it moves to the cloud. Specifically, the protocols used include Secure Socket Layer (SSL), HTTPS and VPN connections where available. The use of encryption in the cloud consumes more processor time, so it lowers the number of customers per resource and increases overall costs. This is because more computations are done on both sides of the transactions. That is why most cloud providers offer basic encryption on a few sensitive database fields, such as passwords and account numbers. There are usually options available from the cloud provider to encrypt the entire database, but this may dramatically increase cost to the point where cloud hosting is more expensive than internal hosting. The keys used for encryption in our solution are kept by customer. Since the keys are managed by the customer carrying out crypto-shredding is easy. Therefore, there is no need to trust the cloud provider. This approach works as long as the data is in motion or at rest. When data requires processing or searching our solution does not provide security. The current state-of-the art shows that it is possible to process and search encrypted data. Although it has been shown possible to process and search encrypted data, current techniques are very expensive in both computation and bandwidth, and show little signs of becoming practical soon. Hardware-based security initiatives such as the Trusted Platform Module and Intel's Trusted Execution Technology can be leveraged to give privacy guarantees in cloud computing. However, for all these proposed solutions significant research must be done before a usable solution is developed.

VI.SUMMARY

From the above discussion it is clear that, for the Cloud Computing to be successful there must be a paradigm shift in all key players. This will involve a completely new way of looking at data control, trust issues, privacy and standards and legislation. While as a world community we seem to have weathered storm of international laws, in the case of Cloud Computing the jury is still out The number of activities such as meetings (conferences, workshops, seminars), new start-up companies, new OS, protocols, hardware and involvement of public and private sector clearly demonstrate the potential of cloud computing. Interests come from all walks of life. A technological solution only seem unlikely to solve the security and privacy problems of cloud computing. It will require an unprecedented integration of the legal and procedural frameworks for computing transactions .Cloud computing will lead to a paradigm shift in computing, which will shake the foundation of computing. For example, we may expect to see cloud services being sold on the basis of the security and privacy they can provide. Metrics for enabling providers to convince users that their products are much better are being researched and developed and will soon be available. For cloud computing to be successful the issue of users control must be resolved technically, politically and socially .Users must be given

assurances that their data and information is well protected, its integrity is maintained and is available when required. The issue of protection of the intellectual properties and copyrighted materials is going to be very contentious. For example, a start-up company has an idea which is being tested on the cloud. A few months later the same or similar idea is patented by the cloud provider or another company which used the same cloud provider's resources. Whom does the start-up company sue for stealing their idea? In the future we expect more providers, richer services, established standards and best practices. Companies will develop private clouds behind their firewalls for use with employees, partners, and others. We will see more research efforts being directed to areas such as cloud security metrics, intelligent infrastructure, dynamic cloud services and scaling, and automatic and adaptive SLA. However, the SLAs being offered by cloud providers at the moment leave much to be desired. They are written by lawyers in language understood by lawyers. We have a long way to go before regulations will provide the necessary protection to consumers. What is being touted to be new in the cloud computing is that you abstract the computer from the physical resources. In other words, you no longer have specific machines in specific places dedicated to specific functions or applications. Rather, a piece of software runs across several machines, optimizing all available resources. Within the cloud issues of user access, authentication, encryption and location of storage exist and must be considered upfront. The urgency and importance of research and development in the cloud computing space and the need for more investment is clearly summarized by the following quote from 'Jonathan Livingston Seagull' by American writer Richard Bach. "A cloud does not know why it moves in just such a direction and at such a speed...It feels an impulsion...this is the place to go now. But the sky knows the reasons and the patterns behind all clouds, and you will know, too, when you lift yourself high enough to see beyond horizons."

VII CONCLUSION

Our conclusion is that cloud computing is not ready to run mission critical applications. There is need for a lot of research to address challenges in the areas of security and privacy, data protection, reliability and interoperability, standards and governance and compliance. Further, usage of cloud computing creates data centers that will attract hackers making them and consumers data difficult to protect. Lastly, it is becoming clear to researchers, practitioners, consumers and politicians that for cloud computing to be successful a team or partnership approach is necessary. The security wrapper proposed in this paper affords protection to the classified data as it flows in the cloud. The wrapper offers security to data in motion and at rest, and incorporates adaptive SLA negotiation. The wrapper is going to serve as the basis for the cloud computing framework.

REFERENCES

[1] Open Virtualization Format Specifications. 2009. p. 1-41.

[2] Alliance, C.S. Trusted Cloud. 2010 [cited 2010 December 18]; Available from: http://www.trusted-cloud.com/.

[3] Amazon. Amazon Elastic Compute Cloud (Amazon EC2). 2010 [cited 2010 December 18]; Available from:

http://aws.amazon.com/ec2/.

[4] Appnexus. AppNexus: Home. 2010 [cited 2010 December 18];Available from: http://www.appnexus.com/.

[5] Cécile Germain-Renaud and O.F. Rana, "The Convergence of Clouds, Grids, and Autonomics," IEEE Internet Computing, 2009. 13(6): p. 9.

[6] Cerf, V.G., "Future Imperfect," IEEE Internet Computing, 2010. January/February: p. 30-34.

[7] Communications, X. XCalibre Communications. 2010 [cited 2010 December 18]; Available from: http://xcalibre.co.uk/new-page.htm.

[8] Conti, G., Googling Security How much does Google know about you? 2009: Addison-Wesley.

[9] Erdogmus, H., "Cloud Computing: Does Nirvana Hide behind the Nebula?" IEEE Software, 2009. 26(2): p. 4-6.

[10] EyeOS. eyeOS - Web Desktop, Cloud Computing Operating System and Web Office. 2010 [cited 2010 December 18]; Available from:http://www.eyeos.org/.

[11] Geer, D., "The OS Faces a Brave New World," IEEE Computer, 2009. 42(10): p. 15-17.

[12] Gilder, G. The Information Factories. 2006 [cited 2010 December 18]; Available from:http://www.wired.com/wired/archive/14.10/cloudware.html.

[13] GoGrid. Cloud Hosting, Cloud Servers, Hybrid Hosting, Cloud Infrastructure from GoGrid. 2010 [cited 2010 December 18]; Available from: http://www.gogrid.com/.

[14] Google. Google Mail. 2010 [cited 2010 December 18]; Available from: mail.google.com/mail/.

[15] Gridlayer. Enterprise Hosting, Cloud Computing, Dedicated Hosting.2010 [cited 2010 December 18]; Available from: http://thegridlayer.com/.

[16] Leavitt, N., "Is Cloud Computing Really Ready for Prime Time?" IEEE Computer, 2009. 42(1): p. 15-20.

[18] Microsoft. Windows Azure Platform. 2010 [cited 2010 December 18];Available from: http://www.microsoft.com/windowsazure/.

[19] Mosso. MossoCrunchBase. 2010 [cited 2010 December 18]; Available from: http://www.crunchbase.com/company/mosso.

[20] Naone, E. Google Gives a First Look at the Chrome OS. TechnologyReview 2009 [cited 2010 December 18]; Available from:http://www.technologyreview.com/web/23987/.

[21] Oasis. Organization for the Advancement of Structured Information Standards. 2010 [cited 2010 December 2010]; Available from: http://www.oasis-open.org/who/.

[22] OpenCloudManifesto. Open Cloud Supporters. 2010 [cited 2010 December 2010]; Available from: http://www.opencloudmanifesto.org/supporters.htm.

[23] OpenGridForum. Open Cloud Computing Interface Working Group. 2010 [cited 2010 December 18]; Available from: http://www.ggf.org/gf/group_info/view.php?group=occi-wg.

[24] Peter Mell and T. Grance, "The NIST Defition of Cloud Computing," 2009, National Institute of Technology and Standards. p. 1-2. [25] Salesforce. CRM - salesforce.com Europe. 2010 [cited 2010

December 18]; Available from: www.salesforce.com.

[26] Thomas Ristenpart, et al. Hey, "You, Get Off of My Cloud! Exploring Information Leakage in Third-Party Compute Clouds," in ACM Conference on Computer and Communications Security (CCS). 2009:ACM.

[27] Tomhave, B., "Dysfunction Junction: Do Standards Function?," ISSA Journal, 2010. February: p. 12-16, 42.

[28] Winkler, I. The Real Problems With Cloud Computing. 2009 [cited 2010 December 18];Availablefrom:http://www.csoonline.com/article/500344/winkler-the-real-problemswith-cloud-computing.

[29] Fredrick Mtenzi, Kevin Street, Dublin 8, Dublin, IrelandIs Cloud Computing Ready for Critical Applications?