The Security in Private Cloud Computing

Abhinava Kumar Srivastava , Divya Kant Yadav,Sandeep Kumar Pandey
Institute of Technology and Management (CS),

Received: 15-01-2013, **Revised:** 21-03-2013, **Accepted:** 12-04-2013, **Published online:** 23-05-2013

Abstract— **Cloud computing security (sometimes referred to simply as "cloud security") is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Private Cloud computing has elevated IT to newer limits by offering the market environment data storage and capacity with flexible scalable computing processing power to match elastic demand and supply, whilst reducing capital expenditure.**

However the opportunity cost of the successful implementation of Cloud computing is to effectively manage the security in the cloud applications. Security consciousness and concerns arise as soon as one begins to run applications beyond the designated firewall and move closer towards the public domain. The purpose of the paper is to provide an overall security perspective of Cloud computing with the aim to highlight the security concerns that should be properly addressed and managed to realize the full potential of Cloud computing. Gartner's list on cloud security issues, as well the findings from the International Data Corporation enterprise panel survey based on cloud threats, will be discussed in this paper.

***Keywords*- Cloud computing, Security, Public cloud, Private cloud, Hybrid Cloud, policies, cloud transparency.**

I. INTRODUCTION

The success of modern day technologies highly depends on its effectiveness of the world's norms, its ease of use by end users and most importantly its degree of information security and control. Cloud computing is a new and emerging information technology that changes the way IT architectural solutions are put forward by means of moving towards the theme of virtualization of data storage, of local networks (infrastructure) as well as software [1-2].

In a survey undertaken by the International Data Corporation (IDC) group between 2008 and 2009, the majority of results point to employing Cloud computing as a low-cost viable option to users [3]. The results also show that Cloud computing is best suited for individuals who are seeking a quick solution for startups, such as developers or research projects and even e-commerce entrepreneurs. Using Cloud computing can help in keeping one's IT budget to a bare minimum. It is also ideally suited for development and testing scenarios. It is the easiest solution to test potential proof of concepts without investing too much capital. Cloud computing can deliver a vast array of IT capabilities in real time using many different types of resources such as hardware, software, virtual storage once logged onto a cloud.

Cloud computing can also be part of a broader business solution whereby prioritized applications utilise Cloud computing functionality whilst other critical applications maintain organisational resources as per normal. This allows for cost saving whilst maintaining a secure degree of control within an orgainsation. Cloud computing can be seen as a service-oriented architecture (SOA) exploring almost every computing component including, but not limited to distributed computing, grid computing, utility computing, on-demand, open source, Peer-to-Peer and Web 2.0 [2]. It is a natural next step from the grid model to a supply and demand utility model. In minimizing potential security trust issues as well as adhering to governance issues facing Cloud computing, a prerequisite control measure is to ensure that a concrete Cloud computing Service Level Agreement (SLA) is put in place and maintained when dealing with outsourced cloud service providers and specialised cloud vendors.

Currently Cloud computing clients have to trust 3rd party cloud providers on many fronts, especially on the availability of cloud service as well as data security. Therefore the SLA forms an integral part of a client's first line of defense. The SLA thus becomes the solitary legal agreement between the service provider and client. The SLA together with other key Cloud considerations will be unpacked further on in this paper. The remainder of this paper is structured as follows: Section II introduces the different types of Cloud models also known as deployment models together with its security implications, Section III explains Cloud computing architectural delivery models with a security insight, followed by Section IV that discusses Cloud computing concerns, particularly focusing on Gartner's list on cloud security issues. Section V pertains to the information security requirements that are applied to Cloud computing. Section VI unpacks the findings from the IDC enterprise panel survey based on cloud shortfalls and finally Section VII highlights how Cloud computing security can be managed.

II. TYPES OF CLOUDS

In providing a secure Cloud computing solution, a major decision is to decide on the type of cloud to be implemented. Currently there are three types of cloud deployment models offered, namely, a public, private and hybrid cloud. These, together with their security implications will be discussed below. Within this paper vendors are referred to as cloud providers, or companies specialising in providing a tailor made cloud solution. These entities have established cloud infrastructure including virtual servers for storage matching required processing power. Organisations are entities, including business managers, executives and end-users, entering into an agreement with cloud vendors to utilise their cloud capabilities for personal or private use.

A. Public Cloud

A public cloud is a model which allows users' access to the cloud via interfaces using mainstream web browsers. It's typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimisation. This helps cloud clients to better match their IT expenditure at an operational level by decreasing its capital expenditure on IT infrastructure [4]. Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.

Therefore trust and privacy concerns are rife when dealing with Public clouds with the Cloud SLA at its core. A key management consideration, which needs to be answered within the SLA deals with ensuring that ample security controls are put in place. One option is for both the cloud vendor and client mutually agree in sharing joint responsibility in enforcing cloud checks and validation are performed across their own systems. The alternative option will be for each party to set out individual roles and responsibilities in dealing with cloud computing security within their utilization boundaries.

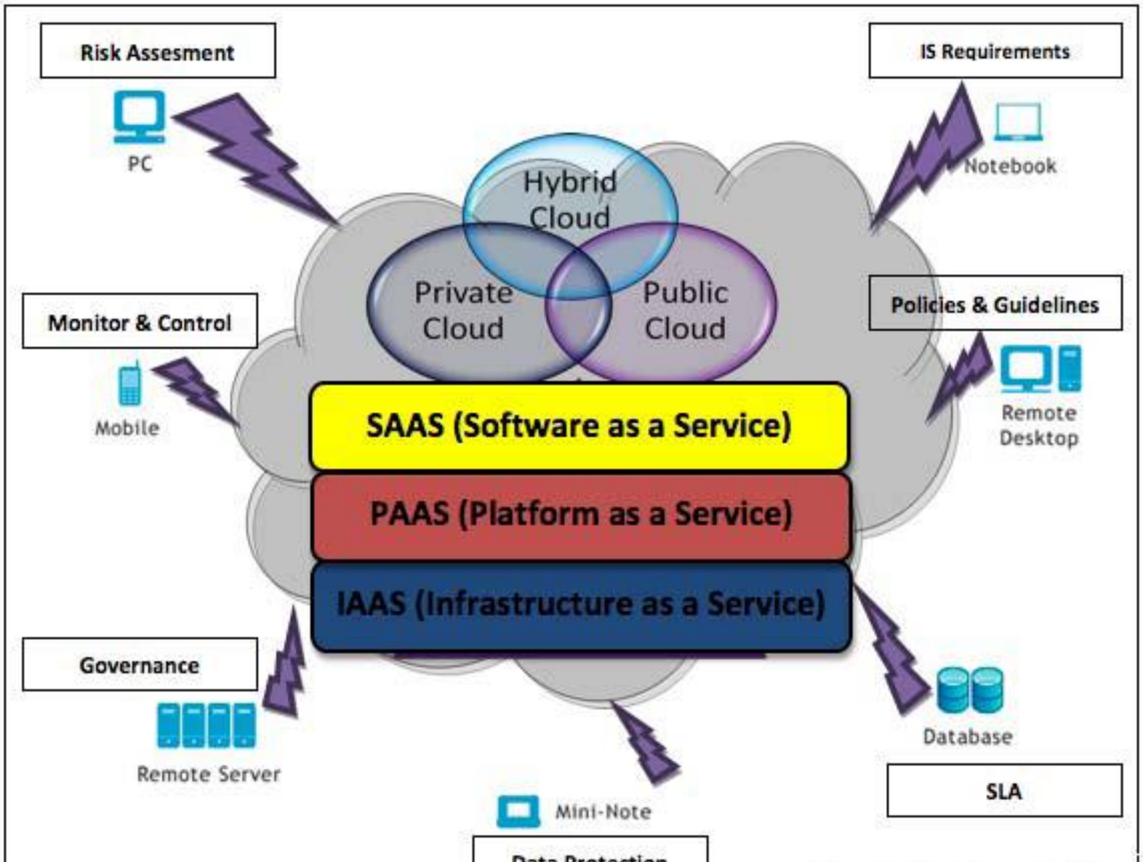

Figure 1: Cloud Computing Map

B. Private Cloud

A private cloud is set up within an organisation's internal enterprise datacenter. It is easier to align with security, compliance, and regulatory requirements, and provides more enterprise control over deployment and use. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organisation itself, similar to Intranet functionality. Utilisation on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organisation and designated stakeholders may have access to operate on a specific Private cloud [5].

C. Hybrid Cloud

A hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network [6]. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Clouds provide more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems. To summarise, in the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand [7]. In deciding which type of Cloud to deploy, business managers' needs to holistically assess the security considerations from an enterprise architectural point of view, taking into account the information security differences of each Cloud deployment model mentioned above.

III. CLOUD COMPUTING DELIVERY MODELS

Following on the cloud deployment models, the next security consideration that business management must unpack relates to the various cloud delivery models. Due to the payper-use economy model that pertains to Cloud delivery models, the degree of information security is directed towards adhering to industry standards and legislations among cloud shareholders. The architecture of Cloud computing can be categorised according to the three types of delivery models, namely Infrastructure as a service (IaaS), Software as a service (SaaS) and Platform as a service (PaaS).

A. Infrastructure as a Service (IaaS)

Infrastructure as a Service is a single tenant cloud layer where the Cloud computing vendor's dedicated resources are only shared with contracted clients at a pay-per-use fee. This greatly minimizes the need for huge initial investment in computing hardware such as servers, networking devices and processing power. They also allow varying degrees of financial and functional flexibility not found in internal data centers or with co-location services, because computing resources can be added or released much more quickly and cost-effectively than in an internal data center or with a collocation service [9]. However, corporate decision makers must
be aware of the capital outlay shift from a periodic fixed expense payment reflected on the income statement to an operational expense increase.

B. Software as a Service (SaaS)

Software as a Service also operates on the virtualised and pay-per-use costing model whereby software applications are leased out to contracted organisations by specialised SaaS vendors. This is traditionally accessed remotely using a web browser via the Internet. The software has limited functionality and its core pack can be expanded and contracted allowing of easy customisation which is billed accordingly. SaaS providers may host the software in their own data centers or with co-location providers, or may themselves be outsourced to IaaS providers. The availability of IaaS services is a key enabler of the SaaS model [10]. Software as a service applications are accessed using web browsers over the Internet therefore web browser security is vitally important. Information security officers will need to consider various methods of securing SaaS applications. Web Services (WS) security, Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL) and available options which are used in enforcing data protection transmitted over the Internet.

*C. **Platform as a Service (PaaS)***

Platform as a service cloud layer works like IaaS but it provides an additional level of "rented" functionality. Clients using PaaS services transfer even more costs from capital investment to operational expenses but must acknowledge the additional constraints and possibly some degree of lock-in posed by the additional functionality layers [6]. The use of virtual machines act as a catalyst in the PaaS layer in Cloud computing. Virtual machines must be protected against malicious attacks such as cloud malware. Therefore maintaining the integrity of applications and well enforcing accurate authentication checks during the transfer of data across the entire networking channels is fundamental. Combining the three types of clouds with the delivery models we get a holistic cloud illustration as seen in Figure 1, surrounded by connectivity devices coupled with information security themes. Virtualized physical resources, virtualized infrastructure, as well as virtualized middleware platforms and business applications are being provided and consumed as services in the Cloud [11]. Cloud vendors and clients' need to maintain Cloud computing security at all interfaces. The next section of the paper will introduce current concerns faced in the Cloud computing domain.

IV. CLOUD COMPUTING CONCERNS

Upon strategically deciding on the appropriate cloud delivery and deployment models to explore, security officers should be aware of the current Cloud computing concerns experienced in the Cloud environment. Gartner has conducted an investigation regarding the information security issues that should be considered when dealing with Cloud computing. The following list contains several security issues highlighted by Gartner that organizations and key decision makers, as a prerequisite, should unpack with Cloud computing vendors [9]:

- Privileged access: Who has specialized/privileged access to data? Who decides about the hiring and management of such administrators?
- Regulatory compliance: Is the cloud vendor willing to undergo external audits and/or security certifications?
- Data location: Does the cloud vendor allow for any control over the location of data?
- Data segregation: Is encryption available at all stages, and were these encryption schemes designed and tested by experienced professionals?
- Recovery: What happens to data in the case of a disaster, and does the vendor offer complete restoration, and, if so, how long does that process take?

• Investigative Support: Does the vendor have the ability to investigate any inappropriate or illegal activity?
• Long-term viability: What happens to data if the cloud vendor goes out of business, is clients' data returned and in what format?
• Data availability: Can the cloud vendor move all their clients' data onto a different environment should the existing environment become compromised or unavailable?

By considering the above mentioned cloud issues, executives can gain a comprehensive understanding as well as measure the feasibility of employing Cloud computing solutions to best match their Cloud strategy. The next section follows on from the concerns mentioned above and is aimed at assisting IT managers assess business critical needs in terms of information security requirements.

V. INFORMATION SECURITY REQUIREMENTS

In the ISO 7498-2 standard [10], produced by The International Standards Organisation (ISO), Information Security should cover a number of suggested themes. Cloud computing security should also be guided in this regard in order to become an effective and secure technology solution. Figure 2, illustrating the information security requirements coupled with the Cloud computing deployment model and delivery models has been adapted from Eloff et al [12]. In Figure 2, the different cloud delivery models and deployment models are matched up against the information security requirements with an "X" denoting mandatory requirements and an asterisk (*) denoting optional requirements. However future work is needed in investigating the optimal balance required in securing Cloud computing. Figure 2 should be viewed in context as a guideline in assessing the security level. Each of the security requirements will be highlighted below in context of Cloud computing.

A. Identification & authentication

In Cloud computing, depending on the type of cloud as well as the delivery model, specified users must firstly be established and supplementary access priorities and permissions may be granted accordingly. This process is targeting at verifying and validating individual cloud users by employing usernames and passwords protections to their cloud profiles.

B. Authorisation

Authorisation is an important information security requirement in Cloud computing to ensure referential integrity is maintained. It follows on in exerting control and privileges over process flows within Cloud computing. Authorisation is maintained by the system administrator in a Private cloud.

C. Confidentiality

In Cloud computing, confidentiality plays a major part especially in maintaining control over organisations' data situated across multiple distributed databases. It is a must when employing a Public cloud due to public clouds accessibility nature. Asserting confidentiality of users' profiles and protecting their data, that is virtually accessed, allows for information security protocols to be enforced at various different layers of cloud applications.

D. Integrity

The integrity requirement lies in applying the due diligence within the cloud domain mainly when accessing data. Therefore ACID (atomicity, consistency, isolation and durability) properties of the cloud's data should without a doubt be robustly imposed across all Cloud computing deliver models

E. Non-repudiation

Non-repudiation in Cloud computing can be obtained by applying the traditional e-commerce security protocols and token provisioning to data transmission within cloud applications such as digital signatures, timestamps and confirmation receipts services (digital receipting of messages confirming data sent/received).

F. Availability

Availability is one of the most critical information security requirements in Cloud computing because it is a key decision factor when deciding among private, public or hybrid cloud vendors as well as in the delivery models. The service level agreement is the most important document which highlights the trepidation of availability in cloud services and resources between the cloud provider and client. Therefore by exploring the information security requirements at each of the various cloud deployment and delivery models set out by the ISO, vendors and organizations can become confident in promoting a highly protected safe and sound cloud framework.

VI. CLOUD SHORTFALLS

From the survey done by the International Data Corporation (IDC), we can learn enormous lessons from past and present cloud players. The reference to the International Data Corporation, is important because it highlights the shortfalls of Cloud computing as well as users' security expectations in Cloud computing. In the Cloud Computing Services Survey conducted during August 08/09 by IDC IT group (www.idc.com) [3], users were asked to rate their issues and challenges experienced with Cloud computing. The results shown in Figure 3 illustrate that security is the biggest concern. Information security, availability and performance issues still remain in the top 3 for both years the survey was done. Security is the main issue users are concerned with when considering Cloud computing solutions. Selecting and implementing the suitable cloud security architecture is not as simple as it might seem as shown from the survey above. Some of the most important issues for companies to consider before engaging in Cloud computing, highlighted from the survey above, are the providers' terms of service, as well as the location and data restrictions on information stored in the cloud. Down-time of cloud services is another growing concern. Cloud providers have the right to read and make public information that is put in the cloud.

There needs to be a subtle balance between cost effectiveness and a smooth running of secure operations with the selected cloud environment. From the cloud shortfalls presented above and by exploring the information security concerns, prospective users will become more familiar and aware of its potential and how Cloud computing can be used to better improve the way we do things whilst pushing the boundaries of traditional norms adapted by society. The biggest challenge in implementing successful Cloud computing technologies is managing the security. As with any new technology enhancements, criticisms are driven by fear of unknown variables and changes to current control procedures of Cloud computing? By focusing more on information security awareness, cloud privacy and by ensuring appropriate policies and procedures are initially put in place, Cloud computing can become the most viable information technology solution. Cloud security polices, cloud transparency and its security impact are the core themes in analysing the strategic information security of Cloud computing which will covered in the next section. These themes, once fully understood and explored by potential endusers can provide the strategic intelligence in guiding the successful implementation of a secure cloud solution.

VII. MANAGING CLOUD COMPUTING SECURITY

In order to effectively manage and control the use of cloud technology in an organisation, business and strategic decision makers need to begin with assessing the potential impact of Cloud computing on their competitive edge. Secondly, business critical security questions of implementing cloud technologies will then need to be evaluated. Managing and controlling Cloud issues will need to address but not limited to the following:

- How the organisation will deal with new and current Cloud compliance risks. This will deal with the potential impact which Cloud computing may have on the business concerning governance and legislation.
- How Cloud computing may affect the organization in terms of its business intelligence and intellectual property by potentially influencing its market differentiation. In setting up a Cloud framework that specifically addresses, organisations' information security, senior professionals and management may look to adapt and incorporate current data protection, trust and privacy policies in formulating a comprehensive set of Cloud computing guidelines. These guidelines may include:
- Establishing an overall business Cloud computing policy that highlights the organisations stance on information protection.
- Govern the installation and communication of Cloud computing when IT decisions are made.
- Leverage of current IT audit and TAX processes with the in embedding cloud security disclosure and Cloud audit practices. Cloud computing guidelines should be seen as the cornerstone of the Cloud strategy with Cloud governance and transparency forming part of the security perspective.

A. Cloud Govenance

Cloud computing policies and procedures should be put in place in an effort to protect the cloud from potential of threats, hacks and the loss of information. We must understand that it is necessary to design privacy within the Cloud right from the outset. The privacy challenge for software engineers is to design cloud services in such a way so as to decrease privacy risks and to ensure legal compliance. There are threats associated with the data being stored, processed remotely and an increased usage of virtualisation and sharing of platforms between users. Concerns arise when it is not clear to individuals why their personal information is requested or how it will be used or passed on to other parties. This lack of control leads to suspicion and ultimately distrust. The protection of data in the cloud is a key consumer concern particularly for committing fraudulent activities and financial exploitation. With governance and security in place, Cloud computing can be used safely and with confidence.

B. Cloud Transparency

Transparent security would entail cloud providers disclosing adequate information about their security policies, design, and practices, including disclosing relevant security measures in daily operations [9]. Public clouds are more likely to be seen as having a greater degree of transparency as compared to the Hybrid or Private Cloud models. This is due to public cloud vendors having a "standardised" cloud offering thereby targeting a wider client base. Private clouds are usually built for specific organisations having more attention focused on offering customization and personalisation cloud functionality. One of the most important protocols in ensuring transparency within Cloud computing is the SLA. The SLA is the only legal agreement between the service provider and client and its importance is greatly discussed in the article titled "Cloud Security Issues" [13]. The only means that the cloud provider can gain the trust of clients is through the SLA, therefore the SLA has to be standardised. The main aspects as a guideline, which the SLA contains, are:

- Services to be delivered, performance,
- Tracking and Reporting
- Problem Management
- Legal Compliance
- Resolution of Disputes Customer Duties
- Security responsibility
- Confidential Information Termination.

One of the main challenges of Cloud computing is that the software vendor should assume responsibility for maintaining the application and ensuring quality of service [14].

C. Cloud Computing's Security Impact

As computer manufacturers, employers and universities deploy cloud based tools on desktops, many users may fail to realize that they are in fact using an Internet based service. This risk of confusion will likely increase when cloud based applications lack any recognizable browser branding, and continue to function when the user is not connected to the Internet. The use of HTTPS together with WS Security should be a bare minimum when logging on to access data using Cloud computing. But providing a HTTPS encrypted connection takes significantly more processing power and memory for a Web server to provide than a normal web connection [15]. WS-Security assists with SOAP messages by defining the header that carries the WS-Security extensions. Additionally, it defines how existing XML security standards like XML Signature and XML Encryption are applied to SOAP messages [16]. Thus far there has been four service failures identified between Amazon and Google in 2008, ranging from 1.5 to 8 hours downtime. Organisations must decide whether proper security measures are in place (to secure their data and applications) or do they share a joint responsibility with service providers when engaging in the cloud environment [17]. The shift to Cloud computing moved much of a user's normal activity to the Web browser. Web browsers generally store all of a user's saved passwords, browsing history and other sensitive information in a single place.

As such it is possible for malicious websites to exploit browser vulnerabilities in order to steal information associated with other existing or previous browsing sessions, such as a logged in email account or online banking session. It is for this reason that some security experts recommend that consumers use one web browser for general surfing, and another for more sensitive tasks, such as online banking. Often, usernames and passwords are transmitted to remote servers via unencrypted network connections. In cases where encryption is used, it is typically only used to transmit the initial login information, while all other subsequent data is sent in the clear. This data can easily be snooped on by hackers. This exposes users to significant risks when they connect to the services using public wireless networks to any Cloud Service. In the book titled '*The Tower and the Cloud',* Richard Katz focuses on many areas where the cloud may impinge on education [18]. He advocates that because companies might be storing documents which should not be made public, there are reasons for concern about what can happen to the information. Potential Cloud organisations and vendors need to be aware that it may become easier for attackers to threaten clouds by moving towards a single cloud interface.

VIII. CONCLUSION

Although Cloud computing can be seen as a new phenomenon which is set to revolutionise the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However one must be very careful to understand the limitations and security risks posed in utilizing these technologies. Cloud computing is no exception. In this paper key security considerations and challenges which are currently faced in the Cloud computing industry are highlighted. While current offerings explore trail-and error control methods, a great deal of investment must be made in the managing security around this evolving technology. The Cloud Security Alliance [19] is one such organisation. It is a non-profit organization formed to promote the use of best practices for providing security assurance within Cloud computing, and provide education on the uses of Cloud computing to help secure all other forms of computing. By following guiding principles discussed in this paper, a great deal of insecurities may be easily expelled, saving business owners' valuable time and investment. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution and future work and progress lies in standardising Cloud computing security protocols.

REFERENCES

[1] Leavitt N, 2009, 'Is Cloud Computing Really Ready for Prime Time?', *Computer*, Vol. 42, pp. 15-20, 2009.
[2] Weinhardt C, Anandasivam A, Blau B, and Stosser J, 'Business Models in the Service World', *IT Professional*, vol. 11, pp. 28-33, 2009.
[3] Gens F, 2009,' New IDC IT Cloud Services Survey: Top Benefits and Challenges',*IDC eXchange*, viewed 18 February 2010, from <http://blogs.idc.com/ie/?p=730>.

[4] A Platform Computing Whitepaper, ‘Enterprise Cloud Computing:Transforming IT’, *Platform Computing*, pp6, viewed 13 March 2010.
[5] Dooley B, 2010, ‘Architectural Requirements Of The Hybrid Cloud’, *Information Management Online*, viewed 10 February 2010, from <http://www.information management.com/news/hybrid-cloudarchitectural- requirements-10017152-1.html>.
[6] Global Netoptex Incorporated , 2009, Demystifying the cloud. Important opportunities, crucial choices, http://www.gni.com, pp 4-14, viewed 13 December 2009.
[7] Lofstrand M, ‘The VeriScale Architecture: Elasticity and Efficiency for Private Clouds”, *Sun Microsystems*, Sun BluePrint, Online, Part No 821- 0248-11, Revision 1.1, 09/22/09
[8] ISO. ISO 7498-2:1989. *Information processing systems- Open Systems Interconnection*. ISO 7498-2
[9] Klems, M, Lenk, A, Nimis, J, Sandholm T and Tai S 2009, ‘What’s Inside the Cloud? An Architectural Map of the Cloud Landscape’, *IEEE Xplore*, pp 23-31, viewed 21 June 2009.
[10] Dlamini M T, Eloff M M and Eloff J H P, ‘Internet of People, Things and Services – The Convergence of Security, Trust and Privacy’, 2009.
[11] Balachandra R K, Ramakrishna P V, Dr. Rakshit A, ‘Cloud Security Issues’, *2009 IEEE International Conference on Services Computing*, viewed 26 October 2009, pp 517-520.
[12] S. Arnold, 2009,’ Cloud computing and the issue of privacy’, *KM World*, vol July/August 2008, *www.kmworld.com*, viewed 19 August 2009, pp 14-22.