ISSN No. 0976-5697

Volume 3, No. 4, July- August 2012

International Journal of Advanced Research in Computer Science

REVIEW ARTICAL

Available Online at www.ijarcs.info

Towards Building a Secure Cloud Computing Environment

Kuyoro Shade O.*
Department of Computer Science
Babcock University
Ilishan-Remo, Nigeria
afolashadeng@gmail.com

Omotunde Ayokunle A.
Department of Computer Science
Babcock University
Ilishan-Remo, Nigeria
ayo_omotunde@yahoo.com

Ajaegbu Chigozirim
Department of Computer Science
Babcock University Ilishan-Remo, Nigeria
chigozirim.ajaegbu@yahoo.com

Ibikunle Frank A
Department of Computer Science
Covenant University Otta, Nigeria
faibikunle2@yahoo.co.uk

Abstract: Cloud computing is the deployment of software, platform and infrastructure as a service by a third-party provider to consumers on a pay-as-you-go basis with the opportunity of expanding and contracting their service requirements as needed. It allows business organizations to utilize models that allow them to focus more on competence which improves their productivity. Cloud computing offers numerous advantages which include pervasiveness, scalability, flexibility, and automated provisioning of resources to name a few. In spite of the numerous advantages attributed to cloud computing, many organizations still exhibit a level of doubtfulness in cloud services because of the security challenges associated with it. This paper examines the security challenges being faced by the different deployment methods and describes how to build a secure cloud.

Keywords: deployment, cloud computing, IPSec, infrastructure, platform and provider

I. INTRODUCTION

According to a recent technical report published by the University of California, Berkley, there is no common theme that unifies the definition of cloud computing, it is defined according to changes in services rendered by different organizations that provide cloud solutions. In addition, there are many shades of cloud computing, each of which can be mapped into a multidimensional space with the dimensions being characteristics, service models, and deployment models.[1] Cloud computing is the delivery of computing and storage capacity as a service to a heterogeneous community of end-recipients.[2] Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software.[3] Cloud computing is 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.[1] The entire concept of cloud computing is not completely new, rather it is a collection of old technologies that are packaged, sold and delivered in a new way since its services combine virtualization (one computer hosting several virtual servers), automated provisioning (servers have software installed automatically), and internet connectivity technologies to provide service.[4].

According to [1], there are five key cloud characteristics, three delivery models and four deployment models.

A. *Key characteristics of the Cloud:*

a. On-demand self-service. Cloud computing resources can be procured and disposed of by the consumer without human interaction with the cloud service provider. This automated process reduces the personnel overhead of the cloud provider, cutting costs and lowering the price at which the services can be offered.

b. Resource pooling. By using a technique called "virtualization," the cloud provider pools his computing resources. This resource pool enables the sharing of virtual and physical resources by multiple consumers, "dynamically assigning and releasing resources according to consumer demand.[1] The consumer has no explicit knowledge of the physical location of the resources being used, except when the consumer requests to limit the physical location of his data to meet legal requirements.

c. Broad network access. Cloud services are accessible over the network via standardized interfaces, enabling access to the service not only by complex devices such as personal computers, but also by light weight devices such as smart phones.

d. Rapid elasticity. The available cloud computing resources are rapidly matched to the actual demand, quickly increasing the cloud capabilities for a service if the demand rises, and quickly releasing the capabilities when the need for drops. This automated process decreases the procurement time for new computing capabilities when the need is there, while preventing an abundance of unused computing power when the need has subsided.

e. Measured service. Cloud computing enables the measuring of used resources, as is the case in utility computing. The measurements can be used to provide resource efficiency information to the cloud provider, and can be used to provide the consumer a payment model based on "pay-per-use." For example, the consumer may be billed for the data transfer volumes,

the number of hours a service is running, or the volume of the data stored per month.

B. Service Delivery Methods in Cloud Computing:

The services offered by cloud computing vendors are available to customers on a pay-as-you-go basis, that is, services are provided on demand and customers are charged as these services are used. Also, users need not have prior knowledge about the administration of the resources involved and the physical infrastructures are not owned by customers, thus increasing the level of risk involved. These services are categorized into three main groups:

a. Software as a Service (SaaS). This is a service delivery method in which the cloud vendors make software applications available to customers over a network, more often than not, the internet on a pay-as-you-go basis. These software applications are accessed by customers using a thin client via a web browser. SaaS is most often implemented to provide business software functionality to enterprise customers at a low cost while allowing those customers to obtain the same benefits of commercially licensed, internally operated software without the associated complexity of installation, management, support, licensing, and high initial cost.[3] The multi-tenant architecture of this delivery model allows vendors to apply a single version of the application using a single hardware, network, and operating system across a large pool of users thereby sharing the cost.

b. Platform as a Service (PaaS). This service delivery method is one layer above IaaS. The cloud vendors provide software and tools for building application to customers. It offers developers a service that provides a complete software development life cycle management, from planning, design building applications, deployment, testing to maintenance without having to worry about maintaining the operating systems, server hardware, load balancing or computing capacity.[6] Everything else is abstracted away from the "view" of the developers. 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.[7,8]

c. Infrastructure as a Service (IaaS). This is the foundation of all cloud services in which the cloud vendors provide the basic infrastructure which includes (virtual) platforms, raw storages, firewalls, networking, etc. on which applications can be placed thereby drastically reducing the enormous initial investment faced by business organizations. This service delivery model allows business organizations to focus more on areas of competence which will in-turn improve level of productivity since the burden of provisioning and management of infrastructure has been taken care of by cloud service providers by completely abstracting the hardware beneath and allowing users to consume infrastructure as a service without bothering about anything about the underlying complexity.

C. Deployment Model in Cloud Computing:

The following are the various methods by which cloud computing can be implemented (Figure 1):

a. Private Cloud. This model is deployed to meet the need of a single organization. Scalable resources are assembled together and hosted internally or externally and managed either internally by the organization or a third party. Since this model is deployed for a single organization, its operation is more secure than public cloud.

b. Public Cloud. This is the most ubiquitous of all the models. Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. [3]

c. Community Cloud. This model is deployed for several organizations that have a common theme. This can also be managed internally or by third-party and hosted internally or externally. The costs are spread over fewer users than a public cloud (but more costly than a private cloud), so only some of the cost savings potential of cloud computing are realized.[1]

d. Hybrid Cloud. This is composed of a private cloud linked together with two or more clouds (public or community). Each of these clouds remain distinctive entities but are bound together thereby presenting the benefits of multiple deployment models. Hybrid cloud can describe configuration combining a local device, such as a Plug computer with cloud services. It can also describe configurations combining virtual and physical, collocated assets -for example, a mostly virtualized environment that requires physical servers, routers, or other hardware such as a network appliance acting as a firewall or spam filter.[3]

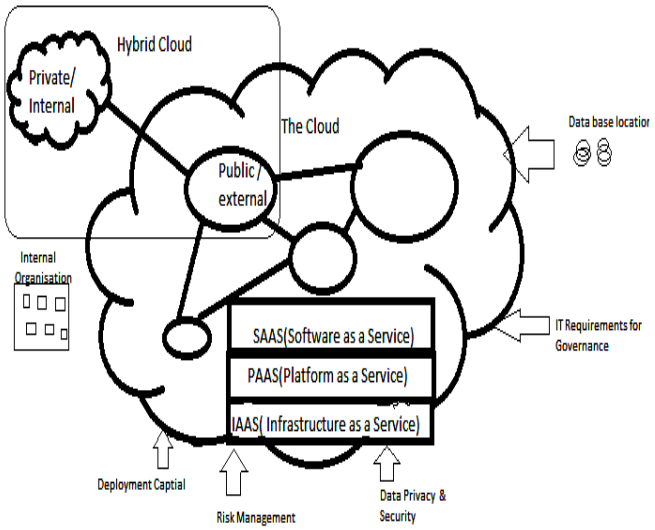

Figure 1. Cloud Computing Deployment Architecture [10]

II. CLOUD COMPUTING SECURITY

Figure 2 depicts IDC Enterprise Panel survey which outlines the benefits of cloud computing. In spite of these great advantages ranging from scalability to pay-per-use, many business organizations exhibit a level of doubtfulness in buying into cloud computing services mainly because their data resides on the service provider's server(s) which

they have no control over.[4] Users of cloud services need assurance that the cloud services and infrastructure provide appropriate functionality so they can have confidence that their data will be protected and its integrity maintained.

Concerns over the security of information in cloud infrastructures continue to stifle adoption of cloud services and restraints many organizations to traditional approaches of providing business IT services. Fundamentally, the concerns over cloud security fall into various category: concerns over security, privacy, availability, confidentiality and integrity.[10] Ensuring the security and integrity of information in the cloud becomes an issue as the management and ownership of the hosting platforms is removed from the consolidated control of a single facility and a single owner. Many organizations such as financial institutions, health care providers, and government agencies are legally required to protect their data from compromise due to the sensitivity of their information. Ideally, these organizations are required to manage and maintain their own datacenters with stringent physical and logical protection mechanisms ensuring that their data remains protected. They simply cannot utilize cloud computing in a generic manner due to the inherent risk of data compromise from systems they do not control. [12] Figure 3 shows that security ranked tops among the challenges facing cloud computing.

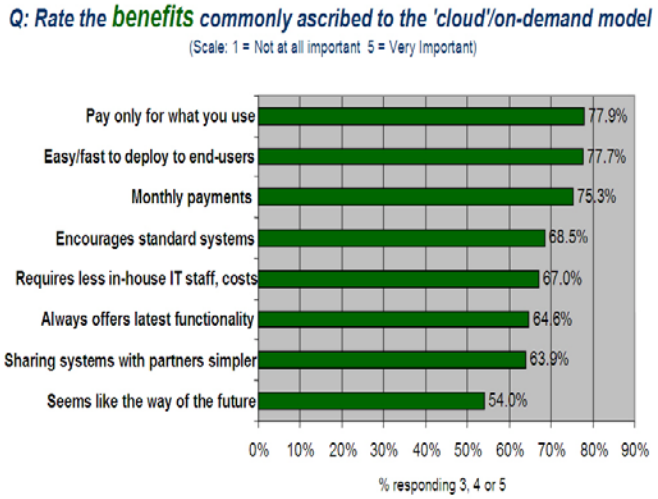

Figure 2. Survey rating the benefits of cloud computing [5]

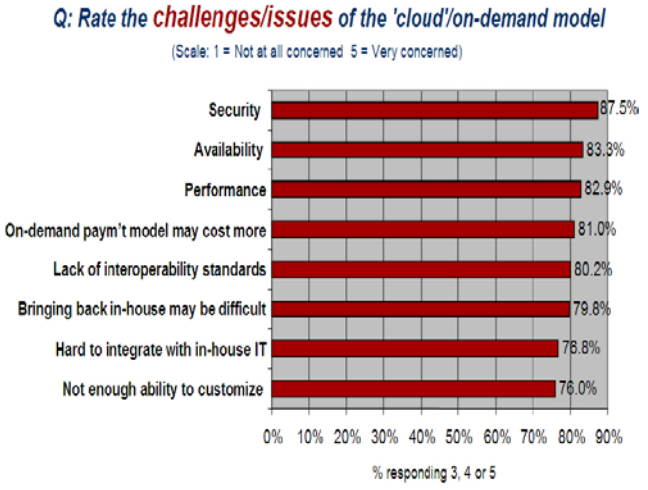

Figure 3. Survey rating the challenges of cloud computing [5]

A. Cloud Security Issues at Deployment Levels:

There are numerous security issues associated with cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction and management, load balancing, concurrency control and memory management.[13] Thus, it is expedient for organizations to apply security measures that will cater for the delivery method they adopt since the security threats differ depending on the layer they are engaging. Figure 4 depicts different security concerns in cloud deployments.

a. SaaS focuses on accessing software applications from service providers through a web browser and the customers worry less about management of network, servers, operating system, storage or even the capabilities of individual application. In a scenario where the service provider does not encrypt data, it is not encrypted. There is also a strong apprehension about insider breaches, along with vulnerabilities in the applications and systems' availability that could lead to loss of sensitive data and money. Such challenges can dissuade enterprises from adopting SaaS applications within the cloud.[6] The following should be considered when deploying SaaS:
   a) Data Security
   b) Data Integrity
   c) Authentication and Authorization

b. The primary focus of PaaS is to offers an integrated set of developer environment that a developer can tap to build their applications without having any clue about what is going on underneath the service by using virtual machines. Protection of data is therefore needed before sending any private information to the cloud. Encryption of data whilst in transit and while stored on a third party platform and awareness of the regulation issues that may apply to data availability in different geographies is another issue that must be duly considered.

c. Iaas pertains to the hardware where data is processed and stored. It also applies to the path through which data is being transmitted. Transmission of data will be done from source to destination through countless number of third-party infrastructure devices thereby increasing the possibility of data being routed through an intruder's infrastructure.[14]

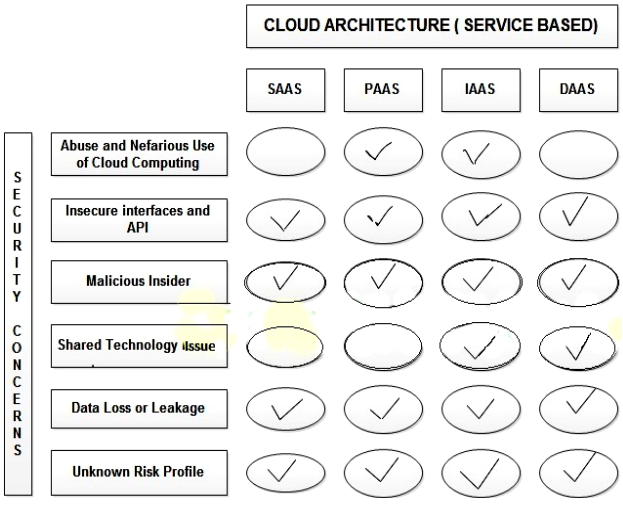

Figure 4 Security concerns in cloud deployments [10]

III. BUILDING A SECURE CLOUD

A. General Overview:

Gartner, Inc., the world's leading information technology research and advisory company, has identified seven security concerns that an enterprise cloud computing user should address with cloud computing providers [15] before adopting:

a. User Access. Ask providers for specific information on the hiring and oversight of privileged administrators and the controls over their access to information. Major companies should demand and enforce their own hiring criteria for personnel that will operate their cloud computing environments.
b. Regulatory Compliance. Make sure your provider is willing to submit to external audits and security certifications.
c. Data location. Enterprises should require that the cloud computing provider store and process data in specific jurisdictions and should obey the privacy rules of those jurisdictions.
d. Data Segregation. Find out what is done to segregate your data, and ask for proof that encryption schemes are deployed and are effective.
e. Disaster Recovery Verification. Know what will happen if disaster strikes by asking whether your provider will be able to completely restore your data and service, and find out how long it will take.
f. Disaster Recovery. Ask the provider for a contractual commitment to support specific types of investigations, such as the research involved in the discovery phase of a lawsuit, and verify that the provider has successfully supported such activities in the past. Without evidence, don't assume that it can do so.
g. Long-term Viability. Ask prospective providers how you would get your data back if they were to fail or be acquired, and find out if the data would be in a format that you could easily import into a replacement application.[16]

Cloud computing guidelines and policies should be clearly placed in an effort to protect the cloud from unauthorized and illegal access. A cloud computing system has capability in providing redundancy to enhance the high availability of the systems in nature.[10]

B. Encrypting the cloud:

In a traditional setting, encryption can be used when passing data from one point to another. This encryption is generally implemented through Internet Protocol Security (IPSec), a traditional type of encryption that uses standards created by the Internet Engineering Task force (IETF) and is based on network architecture.[17] Cloud computing has always used different security measures to protect data, applications and connections. Encryption is already being used in the cloud, but is costly and resource intensive; for example, in Amazon Web Services one can use a private VPN from within the system to cloud resources without opening the system to the outside.[18]

Additionally, improved cloud encryption techniques are also being researched. At Trend Micro work is being done about an encryption scheme for public cloud computing in order to apply encryption agents to every virtual computing instance. As a result, every virtual machine will have its own resident manager to ensure that the encryption security resources are properly applied.[18]

Another interesting research is underway at IBM on homomorphic encryption scheme, which is a scheme that allows one to evaluate circuits over encrypted data without being able to decrypt. Such a scheme allows one to compute arbitrary functions over encrypted data without the decryption key.[19] If this becomes a reality, it will allow users to send data in encrypted form throughout the cloud, manipulate it anyhow they want, and then still be able to decrypt it. As a result, one will be able to work on encrypted data as long as you want without having to change it back to its visible form. This will also minimize having to manage encryption keys, or be concerned about providing those keys to users that cannot be trusted. [20]

C. IPSec as a means of securing the cloud:

Security issues in the cloud can be addressed by implementing IPSec, a bundle of protocols and algorithms defining a flexible framework in which it is the user who selects the actual parameters of the algorithms and methods to be used. These selected parameters provide access authentication (for customers buying into SaaS), data encryption (for customers buying into SaaS and PaaS), and automated key exchange between source and destination IPs (for customers buying into IaaS).

IPSec (IP security) is an operational framework of protocols and algorithms for securing communication over a network at the packet processing layer, which is the network layer of the OSI model, in which the users select the parameters of the algorithms and methods to be used which provides address authentication, data encryption and automated key exchange between source and destination IPs. It is a standardized framework for securing Internet Protocol (IP) communications by encrypting and/or authenticating each IP packet in a data stream. There are two modes of IPsec operation: transport mode and tunnel mode.

In transport mode only the payload (message) of the IP packet is encrypted. It is fully-routable since the IP header is sent as plain text; however, it cannot cross NAT interfaces, as this will invalidate its hash value. In tunnel mode, the entire IP packet is encrypted. It must then be encapsulated into a new IP packet for routing to work.[21] Figure 5 depicts the marking process in IPSec. When the user computer is the one marking the transmitted packets, it is said that IPsec is used in “transport mode”. When the ingress router is doing the job on behalf of the user (acting as a proxy IPsec entity), it is said that IPsec is used in “tunnel mode”.[22]

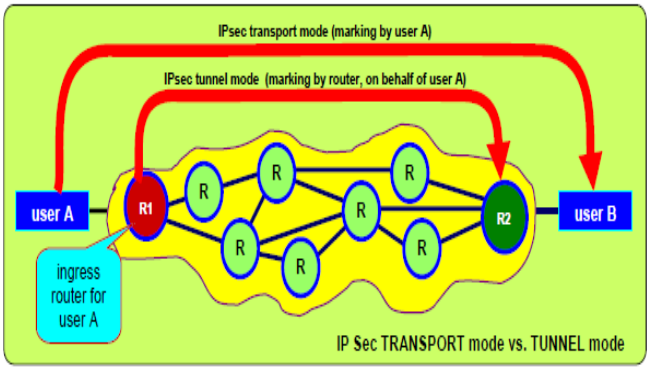

Figure 5: IPSec marking process[22]

IPSec is a suite of protocols that allow secure, encrypted communication between two computers over an insecure network. The encryption is applied at the IP network layer which means that it is transparent to most applications that use specific protocols for network communication. IPSec provides end-to-end security, meaning that the IP packets are encrypted by the sending computer, are unreadable en route, and can be decrypted only by the recipient computer. Due to a special algorithm for generating the same shared encryption key at both ends of the connection, the key does not need to be passed over the network.[23]

IPSec addresses the most essential security issues in a communications network by 'tagging' packets before they are sent into the network. The tag on the packet is used at the receiving end of the network to authenticate whether the packet is from the correct source; to confirm the integrity by checking to see whether the packet content is exactly the one generated from source without any alterations; to reject already received data; to encrypt the packet to ensure that they are not understood in case they are intercepted in transit by unintended recipients.[24]

IPSec is important to strategies of data confidentiality, data integrity, and non-repudiation. It provides security against data manipulation, data interception, and replay attacks. IPSec provides encryption of outgoing and incoming packets, and will be greatly beneficiary to cloud service providers.[22]

IV. CONCLUSION

Cloud computing is becoming appreciable because of its primary benefits. It can reduce both capital expenditures on infrastructure, as well as operational expenditures on infrastructure maintenance and engineering. Cloud computing is a combination of several key technologies that have evolved and matured over the years**.** Since the cloud incorporates resources such as routers, firewalls, gateway, proxy and storage servers etc, the interaction among these entities needs to occur in a secure fashion. Various cloud computing models and their security concerns and what can make the world of cloud computing more secure, reliable and admirable is an important aspect to look into. Cloud security concern is still a challenge and has supreme importance as many flaws and concerns are yet to be identified.

V. REFERENCES

[1] P. Mell & T. Grance, 2009 The NIST Definition of Cloud Computing. Recommendation of the US Department of Commerce's National Institute of Standards and Technology (Draft), available: csrc.nist.gov/group/SNS/cloud-computing/cloud-def-v15.doc

[2] http://en.wikipedia.org/wiki/Cloud_computing

[3] S.O. Kuyoro, F. Ibikunle, O. Awodele. "Cloud Computing Security Issues and Challenges". International Journal of Computer Networks (IJCN), 3(5):2011 pp 247-255

[4] D. Burford, "Cloud Computing: A Brief Introduction". LAD Enterprizes, Inc. (2010)

[5] F. Gens. (2009, Feb.). "New IDC IT Cloud Services Survey: Top Benefits and Challenges", IDC eXchange, Available: <http://blogs.idc.com/ie/?p=730> [Feb. 18, 2010].

[6] S. Subashini, and V. Kavitha. (2010) "A survey on security issues in service delivery models of cloud computing." J Network Comput Appl doi:10.1016/j.jnca.2010.07.006. Jul.,2010.

[7] A Platform Computing White Paper. "Enterprise Cloud Computing: Transforming IT." Platform Computing, pp 6, 2010.

[8] A. Grigoriu. "The Cloud Enterprise". BP Trends, Adrian Grigoriu, 2009

[9] M. R. Nelson, Building an Open Cloud, Science 324, 1656 (2009); www.sciencemag.org [October 20, 2011]

[10] Ashish Kumar, World of Cloud Computing & Security IJ-CLOSER Vol. 1, No. 2, June 2012: 53-58

[11] E. Grosse, "Security at Scale," invited talk, ACM Cloud Security Workshop (CCSW), 2010; http://wn.com/2010_Google_Faculty_Summit_Security_at_Scale.

[12] F. J. Krautheim "Building Trust Into Utility Cloud Computing", an unpublished PhD thesis submitted to the department of computer science and electrical engineering, University of Maryland, Baltimore County, Baltimore, MD

[13] K. Hamlen, M. Kantarcioglu, L. Khan, B. Thuraisingham. "Security Issues for Cloud Computing" International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010

[14] T. Ristenpart, E. Tromer, H. Shacham and S. Savage, "Hey, You Get Off my Cloud: Exploring Information Leakage in Third-party Compute Clouds", Computer and Communication Security CSS 2009

[15] J. Edwards (2009). Cutting through the fog of cloud security. Computerworld. Framingham: Feb 23, 2009. Vol. 43, Iss. 8; pg. 26, 3 pgs.

[16] A. Bisong, S. Shawon, M. Rahman "An Overview Of The Security Concerns In Enterprise Cloud Computing", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011 pp30-45

[17] Search Security: Network Encryption. February 2001. [11 March 2012].

[18] A. Wolfe. "Encryption Is Cloud Computing Security Savior." Network Computing for IT by IT. November 2009. http://www.networkcomputing.com/security/229502349

[19] C. Gentry. Fully Homomorphic Encryption using ideal lattices. In the 41st ACM symposium on theory of computing (STOC), 2009

[20] M. Moghadam and W. Sterkel, Cloud Computing vs Traditional Internet Setting: Which One is More Secure IT-4444 Cameron University Spring 2012

[21] http://research.cloudtweaks.com/technology/security/ipsec 30th June 2012 [20th July, 2012]

[22] S. M. Schwartz "IPsec basics" sorin m. schwartz seminars www.sorin-schwartz.com

[23] http://technet.microsoft.com/library/Cc960637 31st May 2012 [20th July. 2012]

[24] O. Adeyinka "Analysis of IPSec VPNS Performance in a Multimedia Environment School of Computing and Technology", University of East London

[25] B. Michael and G. Dinolt. "Establishing Trust in Cloud Computing". Cloud Computing: Silver Lining or Storm Ahead? Information Assurance Newsletter. vol. 13(2). Spring, 2010.

[26] C. Almond, "A Practical Guide to Cloud Computing Security: What you need to know about your business and cloud security." Avnade Perspective (2009)

[27] C. Soghoian. "Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era" The Berkman Center for Internet & Society Research Publication Series. Available at: http://cyber.law.harvard.edu/publications [Aug.22, 2009].

[28] ENISA. (2009, Feb) "Cloud computing: benefits, risks and recommendations for information security." Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingrisk-assessment [Jul. 10, 2010].

[29] Global Netoptex Incorporated. "Demystifying the cloud. Important opportunities, crucial choices." pp4-14. Available: http://www.gni.com [Dec. 13, 2009].

[30] I. Stoica, M. Zaharia. "Above the Clouds: A Berkley View of Cloud Computing" Electrical Engineering and Computer Sciences University of California at Berkeley (2009)

[31] J. Brodkin. (2008, Jun.). "Gartner: Seven cloud-computing security risks." Infoworld, Available: <http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputingsecurity-risks-853?page=0,1> [Mar. 13, 2009].

[32] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, M. Jensen, J. Schwenk, N. Gruschka and L. L. Iacono, "On Technical Security Issues in Cloud Computing." in PROC IEEE ICCC, Bangalore 2009, pp. 109-116.

[33] Progress Software Corporation Whitepaper. "SaaS Security and privacy." Progress Software, 2008.

[34] R. Vamosi. "Implementing IPSec for Embedded Devices" ECN Magazine.

[35] Sun Microsystems White Paper. "Building Customer Trust in Cloud Computing with Transparent Security." Sun Microsystems, 2009.

