Volume 3 ▪ Issue 5 ▪ December 2011

Editor-in-Chief
Dr. Min Song

INTERNATIONAL JOURNAL OF

COMPUTER NETWORKS (IJCN)

ISSN : 1985-4129

Publication Frequency: 6 Issues / Year

CSC PUBLISHERS
http://www.cscjournals.org

INTERNATIONAL JOURNAL OF COMPUTER NETWORKS (IJCN)

VOLUME 3, ISSUE 5, 2011

EDITED BY
DR. NABEEL TAHIR

ISSN (Online): 1985-4129

International Journal of Computer Networks (IJCN) is published both in traditional paper form and in Internet. This journal is published at the website http://www.cscjournals.org, maintained by Computer Science Journals (CSC Journals), Malaysia.

IJCN Journal is a part of CSC Publishers
Computer Science Journals
http://www.cscjournals.org

INTERNATIONAL JOURNAL OF COMPUTER NETWORKS (IJCN)

Book: Volume 3, Issue 5, December 2011
Publishing Date: 15-12-2011
ISSN (Online): 1985-4129

IJCN Journal is a part of CSC Publishers
http://www.cscjournals.org

Published in Malaysia

Typesetting: Camera-ready by author, data conversation by CSC Publishing Services – CSC Journals, Malaysia

CSC Publishers, 2011

EDITORIAL PREFACE

The International Journal of Computer Networks (IJCN) is an effective medium to interchange high quality theoretical and applied research in the field of computer networks from theoretical research to application development. This is the third issue of volume second of IJCN. The Journal is published bi-monthly, with papers being peer reviewed to high international standards. IJCN emphasizes on efficient and effective image technologies, and provides a central for a deeper understanding in the discipline by encouraging the quantitative comparison and performance evaluation of the emerging components of computer networks. Some of the important topics are ad-hoc wireless networks, congestion and flow control, cooperative networks, delay tolerant networks, mobile satellite networks, multicast and broadcast networks, multimedia networks, network architectures and protocols etc.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Starting with volume 3, 2011, IJCN appears in more focused issues. Besides normal publications, IJCN intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

IJCN give an opportunity to scientists, researchers, engineers and vendors to share the ideas, identify problems, investigate relevant issues, share common interests, explore new approaches, and initiate possible collaborative research and system development. This journal is helpful for the researchers and R&D engineers, scientists all those persons who are involve in computer networks in any shape.

Highly professional scholars give their efforts, valuable time, expertise and motivation to IJCN as Editorial board members. All submissions are evaluated by the International Editorial Board. The International Editorial Board ensures that significant developments in computer networks from around the world are reflected in the IJCN publications.

IJCN editors understand that how much it is important for authors and researchers to have their work published with a minimum delay after submission of their papers. They also strongly believe that the direct communication between the editors and authors are important for the welfare, quality and wellbeing of the journal and its readers. Therefore, all activities from paper submission to paper publication are controlled through electronic systems that include electronic submission, editorial panel and review system that ensures rapid decision with least delays in the publication processes.

To build its international reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJCN. We would like to remind you that the success of our journal depends directly on the number of quality articles submitted for review. Accordingly, we would like to request your participation by submitting quality manuscripts for review and encouraging your colleagues to submit quality manuscripts for review. One of the great benefits we can provide to our prospective authors is the mentoring nature of our review process. IJCN provides authors with high quality, helpful reviews that are shaped to assist authors in improving their manuscripts.

Editorial Board Members
International Journal of Computer Networks (IJCN)

EDITORIAL BOARD

TABLE OF CONTENTS

Volume 3, Issue 5, December 2011

Pages

Cloud Computing Security Issues and Challenges

Kuyoro S. O. *afolashadeng@gmail.com*
Department of Computer Science
Babcock University
Ilishan-Remo, 240001, Nigeria

Ibikunle F. faibikunle2*@yahoo.co.uk*
Department of Computer Science
Covenant University
Otta, 240001, Nigeria

Awodele O. *delealways@yahoo.com*
Department of Computer Science
Babcock University
Ilishan-Remo, 240001, Nigeria

Abstract

Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Usually cloud computing services are delivered by a third party provider who owns the infrastructure. It advantages to mention but a few include scalability, resilience, flexibility, efficiency and outsourcing non-core activities. Cloud computing offers an innovative business model for organizations to adopt IT services without upfront investment. Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hamper the growth of cloud. The idea of handing over important data to another company is worrisome; such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment. This paper introduces a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types.

Keywords: Cloud Computing, Scalability, Infrastructure, IT.

1. INTRODUCTION

For years the Internet has been represented on network diagrams by a cloud symbol until 2008 when a variety of new services started to emerge that permitted computing resources to be accessed over the Internet termed cloud computing. Cloud computing encompasses activities such as the use of social networking sites and other forms of interpersonal computing; however, most of the time cloud computing is concerned with accessing online software applications, data storage and processing power. 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. It extends Information Technology's (IT) existing capabilities. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, customers are still reluctant to deploy their business in the cloud. Security issues in cloud computing has played a major role in slowing down its acceptance, in fact security ranked first as the greatest challenge issue of cloud computing as depicted in figure 1.

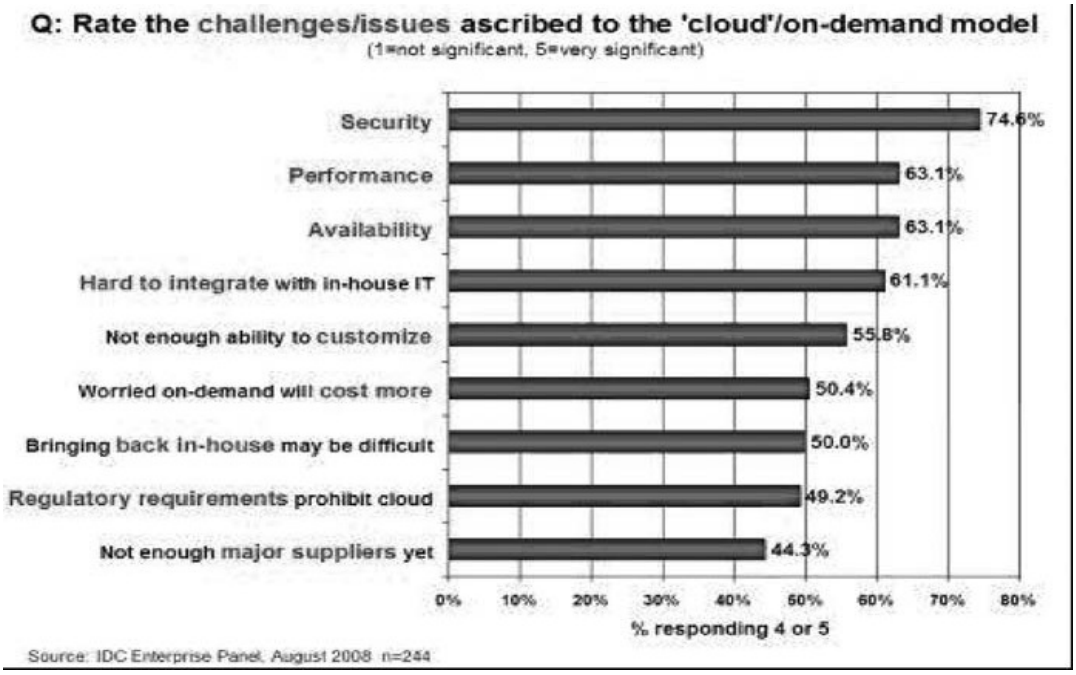

FIGURE 1: Results of IDC survey ranking security challenges, 2008 [1]

From one point of view, security could improve due to centralization of data and increased security-focused resources. On the other hand concerns persist about loss of control over certain sensitive data, and the lack of security for stored kernels entrusted to cloud providers. If those providers have not done good jobs securing their own environments, the consumers could be in trouble. Measuring the quality of cloud providers' approach to security is difficult because many cloud providers will not expose their infrastructure to customers. This work is a survey more specific to the different security issues and the associated challenges that has emanated in the cloud computing system. The following section highlights a brief review of literature on security issues in cloud computing and the remaining sections are organized as follows. Section 3.0 discusses security issues in cloud computing laying emphasis on SaaS, PaaS and IaaS; and cloud computing deployment methods. Section 4.0 deliberates on associated cloud computing challenges; and Section 5.0 presents the conclusion.

2. RELATED WORKS

Gartner 2008 identified seven security issues that need to be addressed before enterprises consider switching to the cloud computing model. They are as follows: (1) privileged user access - information transmitted from the client through the Internet poses a certain degree of risk, because of issues of data ownership; enterprises should spend time getting to know their providers and their regulations as much as possible before assigning some trivial applications first to test the water, (2) regulatory compliance - clients are accountable for the security of their solution, as they can choose between providers that allow to be audited by 3rd party organizations that check levels of security and providers that don't (3) data location - depending on contracts, some clients might never know what country or what jurisdiction their data is located (4) data segregation - encrypted information from multiple companies may be stored on the same hard disk, so a mechanism to separate data should be deployed by the provider. (5) recovery - every provider should have a disaster recovery protocol to protect user data (6) investigative support - if a client suspects faulty activity from the provider, it may not have many legal ways pursue an investigation (7) long-term viability - refers to the ability to retract a contract and all data if the current provider is bought out by another firm.[2] The Cloud Computing Use Case Discussion Group discusses the different Use Case scenarios and related requirements that may

exist in the cloud model. They consider use cases from different perspectives including customers, developers and security engineers.[3] ENISA investigated the different security risks related to adopting cloud computing along with the affected assets, the risks likelihood, impacts, and vulnerabilities in the cloud computing may lead to such risks.[4] Balachandra et al, 2009 discussed the security SLA's specification and objectives related to data locations, segregation and data recovery.[5] Kresimir et al, 2010 discussed high level security concerns in the cloud computing model such as data integrity, payment and privacy of sensitive information.[6] Bernd et al, 2010 discuss the security vulnerabilities existing in the cloud platform. The authors grouped the possible vulnerabilities into technology-related, cloud characteristics-related, security controls related.[7] Subashini et al discuss the security challenges of the cloud service delivery model, focusing on the SaaS model.[8] Ragovind et al, (2010) discussed the management of security in Cloud computing focusing on Gartner's list on cloud security issues and the findings from the International Data Corporation enterprise.[9] Morsy et al, 2010 investigated cloud computing problems from the cloud architecture, cloud offered characteristics, cloud stakeholders, and cloud service delivery models perspectives.[10] A recent survey by Cloud Security Alliance (CSA)&IEEE indicates that enterprises across sectors are eager to adopt cloud computing but that security are needed both to accelerate cloud adoption on a wide scale and to respond to regulatory drivers. It also details that cloud computing is shaping the future of IT but the absence of a compliance environment is having dramatic impact on cloud computing growth.[11] Several studies have been carried out relating to security issues in cloud computing but this work presents a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing deployment types and the service delivery types.

3. SECURITY ISSUES IN CLOUD COMPUTING

3.1 Cloud Deployments Models

In the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand as depicted in figure 2. The Cloud Computing model has three main deployment models which are:

3.1.1 Private cloud

Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization's internal enterprise datacenter. 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 organization itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud.[12]

3.1.2 Public cloud

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. It is 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 optimization.[13] 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.

3.1.3 Hybrid cloud

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 [14]. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Cloud provides 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. 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.

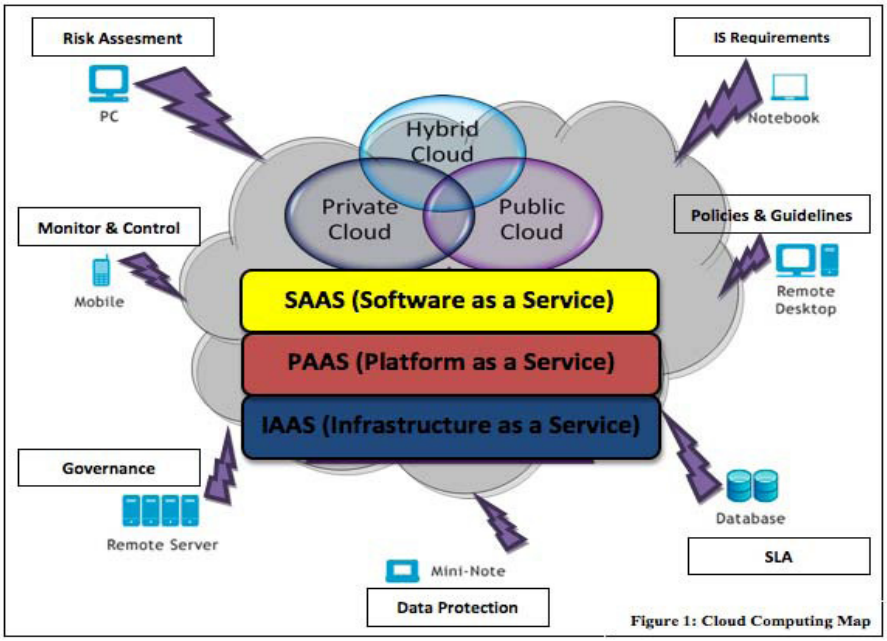

FIGURE 2: Cloud deployment model [13]

3.2 Cloud Computing Service Delivery Models

Following on the cloud deployment models, the next security consideration relates to the various cloud computing service delivery models. The three main cloud service delivery models are: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

3.2.1 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 collocation 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 [2]. IaaS and other associated services have enabled startups and other businesses focus on their core competencies without worrying much about the provisioning and management of infrastructure. IaaS completely abstracted the hardware beneath it and allowed users to consume infrastructure as a service without bothering anything about the underlying complexities. The cloud has a compelling value proposition in terms of cost, but 'out of the box' IaaS only provides basic security (perimeter firewall, load balancing, etc.) and applications moving into the cloud will need higher levels of security provided at the host.

3.2.2. Platform as a service (PaaS)

Platform-as-a-Service (PaaS) is a set of software and development tools hosted on the provider's servers. It is one layer above IaaS on the stack and abstracts away everything up to OS,

middleware, etc. This 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. It offers developers a service that provides a complete software development life cycle management, from planning to design to building applications to deployment to testing to maintenance. Everything else is abstracted away from the "view" of the developers. 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 [14]. 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.

3.2.3 Software as a Service

Software-as-a-Service is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support web services and service-oriented architecture (SOA) mature and new developmental approaches become popular. SaaS is also often associated with a pay-as-you-go subscription licensing model. Meanwhile, broadband service has become increasingly available to support user access from more areas around the world. 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. The architecture of SaaS-based applications is specifically designed to support many concurrent users (multitenancy) at once. 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.[8]

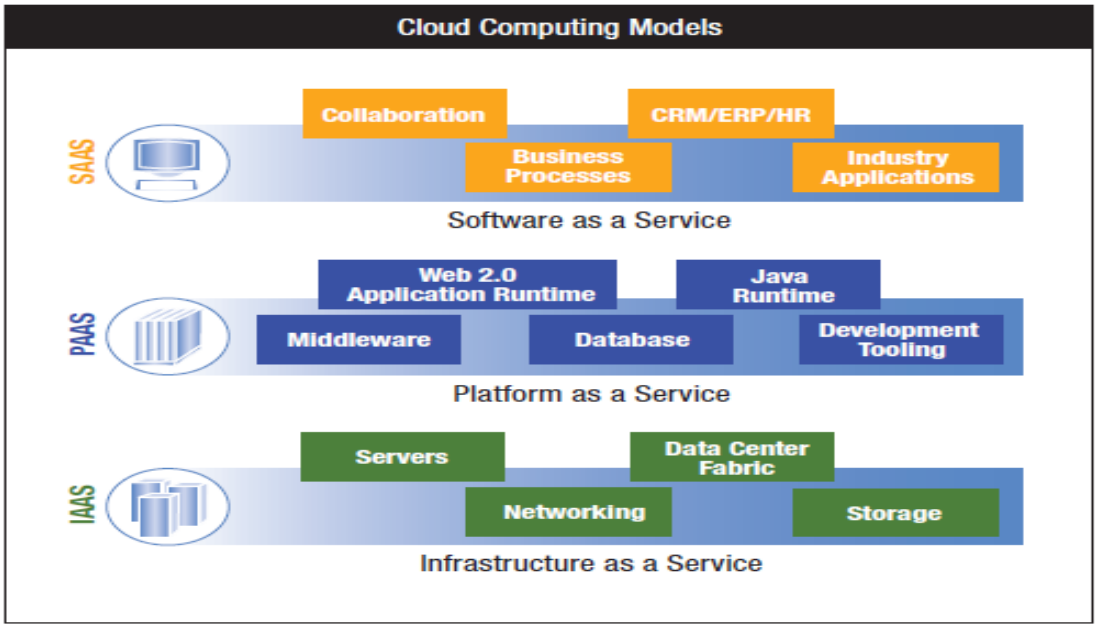

FIGURE 3: Cloud computing service delivery models [15]

Combining the three types of clouds with the delivery models we get a holistic cloud illustration as seen in Figure 3, 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 [15]. Cloud vendors and clients' need to maintain Cloud computing security at all interfaces. The next section of the paper introduces challenges faced in the Cloud computing domain.

4. CLOUD COMPUTING CHALLENGES

The current adoption of cloud computing is associated with numerous challenges because users are still skeptical about its authenticity. Based on a survey conducted by IDC in 2008, the major challenges that prevent Cloud Computing from being adopted are recognized by organizations are as follows:

A. Security: It is clear that the security issue has played the most important role in hindering Cloud computing acceptance. Without doubt, putting your data, running your software on someone else's hard disk using someone else's CPU appears daunting to many. Well-known security issues such as data loss, phishing, botnet (running remotely on a collection of machines) pose serious threats to organization's data and software. Moreover, the multi-tenancy model and the pooled computing resources in cloud computing has introduced new security challenges that require novel techniques to tackle with. For example, hackers can use Cloud to organize botnet as Cloud often provides more reliable infrastructure services at a relatively cheaper price for them to start an attack.[9]

B. Costing Model: Cloud consumers must consider the tradeoffs amongst computation, communication, and integration. While migrating to the Cloud can significantly reduce the infrastructure cost, it does raise the cost of data communication, i.e. the cost of transferring an organization's data to and from the public and community Cloud and the cost per unit of computing resource used is likely to be higher. This problem is particularly prominent if the consumer uses the hybrid cloud deployment model where the organization's data is distributed amongst a number of public/private (in-house IT infrastructure)/community clouds. Intuitively, on-demand computing makes sense only for CPU intensive jobs.[9]

C. Charging Model: The elastic resource pool has made the cost analysis a lot more complicated than regular data centers, which often calculates their cost based on consumptions of static computing. Moreover, an instantiated virtual machine has become the unit of cost analysis rather than the underlying physical server. For SaaS cloud providers, the cost of developing multitenancy within their offering can be very substantial. These include: re-design and re-development of the software that was originally used for single-tenancy, cost of providing new features that allow for intensive customization, performance and security enhancement for concurrent user access, and dealing with complexities induced by the above changes. Consequently, SaaS providers need to weigh up the trade-off between the provision of multi-tenancy and the cost-savings yielded by multi-tenancy such as reduced overhead through amortization, reduced number of on-site software licenses, etc. Therefore, a strategic and viable charging model for SaaS provider is crucial for the profitability and sustainability of SaaS cloud providers.[9]

D. Service Level Agreement (SLA): Although cloud consumers do not have control over the underlying computing resources, they do need to ensure the quality, availability, reliability, and performance of these resources when consumers have migrated their core business functions onto their entrusted cloud. In other words, it is vital for consumers to obtain guarantees from providers on service delivery. Typically, these are provided through Service Level Agreements (SLAs) negotiated between the providers and consumers. The very first issue is the definition of SLA specifications in such a way that has an appropriate level of granularity, namely the tradeoffs between expressiveness and complicatedness, so that they can cover most of the consumer expectations and is relatively simple to be weighted, verified, evaluated, and enforced by the

resource allocation mechanism on the cloud. In addition, different cloud offerings (IaaS, PaaS, and SaaS) will need to define different SLA metaspecifications. This also raises a number of implementation problems for the cloud providers. Furthermore, advanced SLA mechanisms need to constantly incorporate user feedback and customization features into the SLA evaluation framework.[16]

E. What to migrate: Based on a survey (Sample size = 244) conducted by IDC in 2008, the seven IT systems/applications being migrated to the cloud are: IT Management Applications (26.2%), Collaborative Applications (25.4%), Personal Applications (25%), Business Applications (23.4%), Applications Development and Deployment (16.8%), Server Capacity (15.6%), and Storage Capacity (15.5%). This result reveals that organizations still have security/privacy concerns in moving their data on to the Cloud. Currently, peripheral functions such as IT management and personal applications are the easiest IT systems to move. Organizations are conservative in employing IaaS compared to SaaS. This is partly because marginal functions are often outsourced to the Cloud, and core activities are kept in-house. The survey also shows that in three years time, 31.5% of the organization will move their Storage Capacity to the cloud. However this number is still relatively low compared to Collaborative Applications (46.3%) at that time.[1]

F. Cloud Interoperability Issue: Currently, each cloud offering has its own way on how cloud clients/applications/users interact with the cloud, leading to the "Hazy Cloud" phenomenon. This severely hinders the development of cloud ecosystems by forcing vendor locking, which prohibits the ability of users to choose from alternative vendors/offering simultaneously in order to optimize resources at different levels within an organization. More importantly, proprietary cloud APIs makes it very difficult to integrate cloud services with an organization's own existing legacy systems (e.g. an on-premise data centre for highly interactive modeling applications in a pharmaceutical company).The primary goal of interoperability is to realize the seamless fluid data across clouds and between cloud and local applications. There are a number of levels that interoperability is essential for cloud computing. First, to optimize the IT asset and computing resources, an organization often needs to keep in-house IT assets and capabilities associated with their core competencies while outsourcing marginal functions and activities (e.g. the human resource system) on to the cloud. Second, more often than not, for the purpose of optimization, an organization may need to outsource a number of marginal functions to cloud services offered by different vendors. Standardization appears to be a good solution to address the interoperability issue. However, as cloud computing just starts to take off, the interoperability problem has not appeared on the pressing agenda of major industry cloud vendors. [9]

5. 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 security risks and challenges 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 are highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.

6. REFERENCES

[1] 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].

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

[3] Cloud Computing Use Case Discussion Group. "Cloud Computing UseCases Version 3.0," 2010.

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

[5] R. K. Balachandra, P. V. Ramakrishna and A. Rakshit. "Cloud Security Issues." In PROC '09 IEEE International Conference on Services Computing, 2009, pp 517-520.

[6] P. Kresimir and H. Zeljko "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349.

[7] B. Grobauer, T. Walloschek and E. Stöcker, "Understanding Cloud Computing Vulnerabilities," *IEEE Security and Privacy*, vol. 99, 2010.

[8] 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.

[9] S. Ramgovind, M. M. Eloff, E. Smith. "The Management of Security in Cloud Computing" In PROC 2010 IEEE International Conference on Cloud Computing 2010.

[10] M. A. Morsy, J. Grundy and Müller I. "An Analysis of the Cloud Computing Security Problem" In PROC APSEC 2010 Cloud Workshop. 2010.

[11] Cloud Security Alliance (CSA). Available: http://www.cloudsecurityalliance.org [Mar.19, 2010]

[12] S. Arnold (2009, Jul.). "Cloud computing and the issue of privacy." *KM World*, pp14-22. Available: www.kmworld.com [Aug. 19, 2009].

[13] A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT." *Platform Computing*, pp6, 2010.

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

[15] M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. "What's Inside the Cloud? An Architectural Map of the Cloud Landscape." *IEEE Xplore*, pp 23-31, Jun. 2009.

[16] C. Weinhardt, A. Anandasivam, B. Blau, and J. Stosser. "Business Models in the Service World." *IT Professional*, vol. 11, pp. 28-33, 2009.

[17] N. Gruschka, L. L. Iancono, M. Jensen and J. Schwenk. "On Technical Security Issues in Cloud Computing" In PROC 09 IEEE International Conference on Cloud Computing, 2009 pp 110-112.

[18] N. Leavitt. "Is Cloud Computing Really Ready for Prime Time?" *Computer*, vol. 42, pp. 15-20, 2009.

[19] 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.

[20] 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: http://cyber.law.harvard.edu/publications [Aug.22, 2009].

Further Analysis Of A Framework To Analyze Network Performance Based On Information Quality

A Kazmierczak *akazmierczak@nwacc.edu*
Computer Information Systems
Northwest Arkansas Community College
One College Dr.
Bentonville, AR 72712 USA
Phone; 001.479.619.3126
FAX: 001.479.619.2670

Abstract

In [1], Geng and Li presented a framework to analyze network performance based on information quality. In that paper, the authors based their framework on the flow of information from a Base Station (BS) to clients. The theory they established can, and needs, to be extended to accommodate for the flow of information from the clients to the BS. In this work, we use that framework and study the case of client to BS data transmission. Our work closely parallels the work of Geng and Li, we use the same notation and liberally reference their work.

Keywords: Information Theory, Information Quality, Network Protocols, Network Performance

1. INTRODUCTION

The major contribution of Geng and Li's work was a framework that introduced information quality (IQ) as an additional attribute of information and further showed that information quality has an effect on network performance parameters, particularly system throughput. IQ reflects the degree of importance of information to the target network performance metric. The authors apply IQ to the quantitative analysis and design of network protocols.

To quantitatively measure the information efficiency (IE) of network protocols, the authors also present information efficiency and provide an approach to improve the information efficiency of protocols. Information efficiency (IE) is defined as improvement of a performance metric per bit od information as a metric as a metric of IE of network protocols [1] In their work, they study the effects of IQ and IE on network performance and show that using both IQ and IE the performance of a network can be improved. The authors base their analysis on the flow of information from a base station BS to a group of clients. In this work, we apply the concepts of IQ and IE to the analysis of the flow of information from a group of clients to the base station BS. Our results are the same as the authors and thus provides further validation to their framework.

2. PRELIMINARIES

The disciplines of information theory and networking have promised interesting connections and has received a great deal of attention from researches in both fields. One of the important early contributions by information theory was in the area of routing. Gallagher [2] provided an information theoretical analysis of minimum delay routing in packet-switched, store-and-forward networks. There have also been information theoretical analysis of multi-access communication [3], timing channel [4] and others. A summarization of this early work appears in a survey paper [5].Network information theory [6] deals with information capacity in multi-hop wireless networks and focuses on coding and channel information.

Another very active research topic is network coding [7], a research field of information theory and coding theory. Network coding is an approach derived from information theory. In [8], Chiang, et al, attempt to develop a uniform framework for network protocols.

3. FRAMEWORK AND DETAILS

3.1 Information Quality

The material in this section repeats much of the material in [1] to provide the proper background for our analysis.

IQ of information source x_i is defined using partial derivatives of the performance metric in the direction of x_i as:

$$Qual(x_i) = \frac{\partial U(Q(X^+))}{\partial x_i} \quad (1)$$

where $X^+ = \{ x_1, x_2, \ldots x_n\}$ represents information sources used by protocol Q and U(Q) is the performance of Q using information X^+.

The author's also define the idea of effective information quantity as:

$$I_{eff}(x_i) = I(x_i) \times Qual(x_i) \quad (2)$$

By multiplying information quantity by quality, where $I(x_i)$ is the quantity of information source x_i.

Effective information quality is really the original information weighted by the quality of the information. This particular parameter describes the effectiveness of the amount of information on the improvement in performance.

3.2 Fundamental Principles

The following theorems are proven in [1]. They are repeated here without proof.

Theorem 3.1: Marginal information change drives performance variation.

Comments: Given a performance metric U that is to be maximized, $Z = \{z_1, z_2, \ldots z_N\}$ the set of information sources used by Q and x an additional source, then

$$U(Q(Z, x)) \geq U(Q(Z)) \quad (3)$$

which means that additional information cannot increase uncertainty.

This result is because, with the current information, any additional information cannot increase uncertainty. If the added information is favorable, it can be used to enhance performance. If the added information is not favorable, it can simply be discarded.

Similarly,

$$U(Q (Z_{-i})) \leq U(Q(Z)) \quad (4)$$

Where Z_{-I} means that source Z_i is removed from the set.

*Theorem 3.2:*Increasing total information quantity does not necessarily mean better performance.

Comments: Even though

$$I(Z) > I(Y) \quad (5)$$

does not mean

$$U(Q(Z)) > U(Q(Y)) \quad (6)$$

Theorem 3.3: Information should be utilized as directly as possible to achieve better system performance.

Comments: Given the system performance function U, and available information sources X and Y and the relationship X -> Y -> U exists, which means Y is a more direct information source. Then, according to [9]

$$I(Y; U) \geq I(X: U) \quad (7)$$

and further

$$U(Q(Y)) \geq U(Q(X)) \quad (8)$$

This means that indirect information from source X reveals less about performance, U, than direct information from source Y. The system senses less uncertainty from X than from Y and consequently performs better.

Theorem 3.4: Performance variations due to marginal change of information of different qualities will differ.

Comment: Using higher quality information helps increase performance more effectively than using information of lower quality.

Theorem 3.5: Using different information jointly is at least as good as using them individually.

Comment: Given a performance function $U = U_1 + U_2$ and information source x with two sub-information sources x_1 and x_2

$$U_1(Q(x_1, x_2) \geq U_1(Q (x_1))$$

$$U_2(Q (x_1, x_2) \geq U_2(Q (x_2)) \quad (9)$$

Then

$$U_1(Q(x_1, x_2) + U_2(Q(x_1) \geq U_1(Q(x_1)) + U_2(Q (x_2)) \quad (10)$$

The performance, U, may not be the sum of U_1 and U_2. However, if we want to improve performance, using information jointly contributes more to improving performance using information singly.

3.3 Information Efficiency Of Network Protocols

In [1], the authors define Information Efficiency (IE) as the improvement of a performance metric per bit of information as a metric of information efficiency of protocols:

$$IE(Q(Z)) = \frac{U(Q (Z)}{\sum_{i=1}^{N} I(z_i)} \quad (11)$$

where $Z = \{ z_1, z_2, \ldots z_N\}$ is the set of information sources. IE can be used to evaluate how efficiently performance with an opportunistic protocol compared to the original protocol.

This last equation can be used to calculate information efficiency of a protocol. A useful application is to compare different opportunistic protocols for information efficiency. We can use IE in the next equation to

evaluate how the system performance efficiency has been improved with an opportunistically designed protocol.

$$IE\ (\ Q(\ X^{+},\ Z\ )\ ) = \frac{U(\ Q\ (\ X^{+},\ Z\ )\ ) - U(\ Q'(\ Z\ )\ )}{\sum_{i=1}^{N} I(\ x_i\ )} \qquad (12)$$

where Z is the set of information sources, Q' is the original protocol and $X^{+} = \{ x_1, x_2, \ldots x_n \}$ are the additional information sources used by the opportunistic protocol Q.

4. PERFORMANCE EVALUATION

In [1], the authors look at two opportunistic protocols. They look at the functionality of their framework and the impact of information quality on performance and they look at how to analyze and improve the information efficiency of the protocols using IE.

4.1 Information Quality

The network scenario used consistsof a base station (BS) serving four clients C_1, C_2, C_3, and C_4 in each time slot. Each client can have one of N discrete channel conditions. For simplicity, presume that each node is equally likely to have a "good" channel condition or a "bad" channel condition. Transmission rates on each channel are T_G = 1 Mb/slot and T_B = 0.5 Mb/slot, respectively.

Each client contains a transmission buffer of size k for outgoing messages. It's message availability is measured by dividing the message length by the empty buffer size k. If the message availability is greater than or equal 50%, it's transmission success probability is P_H, otherwise it's transmission success probability is P_L. As the authors in [1], we set P_H = 0.8 and P_L = 0.2. Each client is equally likely to have high or low message availability. The performance metric under consideration is the average system throughput per slot.

4.2 Channel Condition Information

If the BS has no information about each clients channel condition, the BS serves the clients in random order. The entropy of channel condition information, the number of bits necessary to encode channel condition information for four clients is:

$$G_{rand} = (1 / 4)\ (\ T_G \times P_H + T_G \times P_L + T_B \times P_H + T_B \times P_L\ ) \qquad (13)$$

$$= 0.375 \text{ Mb/slot}$$

Now presume the BS gets channel condition information from only one of its clients while the others remain unknown. This single bit may indicate either "good" or "bad" with equal probability. If the bit indicates "good", the BS will schedule a transmission from this client. If the bit indicates "bad", the BS will select one of the other clients for transmission. In this case, the expected average throughput becomes:

$$G = (1 / 2) \times (\ (1 / 2) \times P_H + (1 / 2) \times P_L\ ) + (1 / 2) \times G_{rand} \qquad (14)$$

$$= 0.4375 \text{ Mb/slot}$$

Presume the BS gets channel condition information from two clients. These two bits can be one of four combinations with equal probability 1 / 4. The expected average throughput becomes G = 0.4688 Mb/slot. System throughput can also be calculated with three and four bits of channel condition information.

4.3 Message Availability Information

We also consider message availability information and its effect on performance. We follow the same logic used previously and derive results and the quantitative performance variations with message availability information. The results are shown in Table I.

Info	Entropy	G (channel)	G (message)
Nil	4 bits	0.375 MB/slot	0.375 Mb/slot
1 bit	3 bits	0.4375 Mb/slot	0.4875 Mb/slot
2 bits	2 bits	0.4688 MB/slot	0.5438 Mb/slot
3 bits	1 bit	0.4844 Mb/slot	0.5719 Mb/slot
4 bits	Nil	0.4844 Mb/slot	0.5719 Mb/slot

TABLE: IPerformance Variation Due to Information Availability

Looking at columns three and four, it is apparent that with more information available, performance is improved. A close examination shows that less information, as indicated by entropy, generates better performance. This is counterintuitive and is due to the fact that higher quality information is used to more efficiently improve performance.

We note that different information does have a different affect on performance, In particular, message availability information has a more significant impact on performance than channel condition information. Message availability information has higher information quality.

We compare our results for client to BS communication to the results obtained by Geng and Li [1] for BS to client communication. The results obtained by Geng and Li are shown in Table 2 [1].

Info	Entropy	G (channel)	G (message)
Nil	4 bits	0.375 MB/slot	0.375 Mb/slot
1 bit	3 bits	0.4375 Mb/slot	0.4875 Mb/slot
2 bits	2 bits	0.4688 MB/slot	0.5438 Mb/slot
3 bits	1 bit	0.4844 Mb/slot	0.5719 Mb/slot
4 bits	Nil	0.4844 Mb/slot	0.5719 Mb/slot

TABLE 2 Results of Geng and Li

A close comparison shows that our results for client to BS communication exactly mathes the results of Geng and Li for BS to client communication. This serves to show that communication in both directions show equal performance improvements by applying the concepts of information quality and information efficiency

4.4 Information Efficiency

In this scenario we consider time slotted opportunistic scheduling. The network scenario of a BS serving three clients. Each client has two possible channel conditions, s_1 and s_2, and performance values, throughput G_1 and G_2 with $G_1 > G_2$. In any slot, each client is equally likely to be in states s_1 or s_2. As the authors in [1], we look at the temporal fairness requirement in [9] and set $r_1 = r_2 = r_3 = 1 / 3$, each user should be allocated one-third of the transmission time.
Using non-opportunistic scheduling, with no channel condition information, the average performance is:

$$E[U_{Q'(u)}] = \sum_{i=1}^{3} r_i \times E[U_i] \quad (15)$$

$$= (G_1 + G_2) / 2$$

where $Q'(U)$ is a non-opportunistic schedule and $E[U_i]$ is the expected performance of client i, and $E[U_{Q'(U)}]$ is the average performance. With no channel condition information, the BS chooses clients randomly.

Now, with opportunistic scheduling used with channel condition information available from each client, the BS can choose the most favorable client and the average system performance becomes:

$$E[U_{Q(s1, s2 u)}] = \sum_{i=1}^{3} r_i \times E[U_i] \quad (16)$$

$$= (7\, G_1 + G_2) / 8$$

The IE of the opportunistic scheduling protocol $Q(s_1, s_2, U)$ is:

$$IE(Q(s_1, s_2, U)) = \frac{E[U_{Q(s1, s2, U)}] - E[U_{Q'(U)}]}{3 \text{ bits per slot}} \quad (17)$$

$$= (G_1 - G_2) / 8$$

We also ask if all possible information is necessary. We presume that only clients with "good" channel condition information report their channel condition s_1. Indeed, using only s_1 as the information available, the IE improves to:

$$IE(Q(s_1, U) = \frac{E[U_{Q(s1, s2, U)}] - E[U_{Q'(U)}]}{1.5 \text{ bits/slot}} \quad (18)$$

$$= (G_1 - G_2) / 4$$

5. CONCLUSION

Geng and Li [1] presented an information theoretic framework to analyze network performance. In that work, the authors considered only the transmission from the BS to the clients. In this paper, we used the framework to analyze network performance when transmitting from the clients to the BS. Using the same scenarios as used in [1], we generate the same results. The quality of information available does affect system performance for the better. Our results provide further validation to the theory of an information theoretic framework for analyzing protocols and network performance.

6. BIBLIOGRAPHY

[1] Y. Geng and V. O. K. Li."A framework to analyze network performance based on information quality", *Proc. IEEE ICC '10*,2010, pp 148-152

[2] R. Gallagher."A minimum delay routing algorithm using distributed computation", *IEEE Transactions on Communications*, Vol 25, pp 73-85, Jan 1977

[3] N. Abramson."The Aloha system – another alternative for computer communications", *Proc AFIPS '70*, 1970, pp 281-285

[4] R. Gallagher."Basic limits on protocol information in data communications networks", *IEEE Transactions on Information Theory*, Vol 22, pp 385-398 Jul 1996

[5] A. Ephremides and B. Hajek."Information theory and communication networks: an unconsummated union", *IEEE Transactions on Information Theory*, Vol 44, pp 2416-2434, Oct 1988

[6] L.-L. Xie and P. Kumar."A network information theory for wireless communication: scaling laws and optimal operation", *IEEE Transactions on Information Theory*, Vol 50, pp 748-767, May 2004

[7] R. Ahlswede, N. Cai, S.-Y. Li, and R. Yeung."Network information flow", *IEEE Transactions on Information Theory*, Vol 46, pp 1204-1216, Jul 2000

[8] M.Chiang, S. Low, A Culderbank, and J. Doyle.“Layering as optimization decomposition: a mathematical theory of network architectures”, *Proc IEEE*, 2007, pp 255-312

[9] X. Liu, E. K. P. Chong and N. B. Shroff.“A framework for opportunistic scheduling in wireless networks”, *Computer Networks*, Vol 41, pp 451-474, 2003

INSTRUCTIONS TO CONTRIBUTORS

The International Journal of Computer Networks (IJCN) is an archival, bimonthly journal committed to the timely publications of peer-reviewed and original papers that advance the state-of-the-art and practical applications of computer networks. It provides a publication vehicle for complete coverage of all topics of interest to network professionals and brings to its readers the latest and most important findings in computer networks.

To build its International reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJCN.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Starting with volume 3, 2011, IJCN appears in more focused issues. Besides normal publications, IJCN intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

We are open to contributions, proposals for any topic as well as for editors and reviewers. We understand that it is through the effort of volunteers that CSC Journals continues to grow and flourish.

IJCN LIST OF TOPICS

The realm of International Journal of Computer Networks (IJCN) extends, but not limited, to the following:

- Algorithms, Systems and Applications
- ATM Networks
- Cellular Networks
- Congestion and Flow Control
- Delay Tolerant Networks
- Information Theory
- Metropolitan Area Networks
- Mobile Computing
- Multicast and Broadcast Networks
- Network Architectures and Protocols
- Network Modeling and Performance Analysis Network
- Network Security and Privacy
- Optical Networks
- Personal Area Networks
- Telecommunication Networks
- Ubiquitous Computing
- Wide Area Networks
- Wireless Mesh Networks
- Ad-hoc Wireless Networks
- Body Sensor Networks
- Cognitive Radio Networks
- Cooperative Networks
- Fault Tolerant Networks
- Local Area Networks
- MIMO Networks
- Mobile Satellite Networks
- Multimedia Networks
- Network Coding
- Network Operation and Management
- Network Services and Applications
- Peer-to-Peer Networks
- Switching and Routing
- Trust Worth Computing
- Web-based Services
- Wireless Local Area Networks
- Wireless Sensor Networks

CALL FOR PAPERS

Volume: 4 - **Issue:** 2 – April 2012

i. Paper Submission: January 31, 2012 **ii. Author Notification:** March 15, 2012

iii. Issue Publication: April 2012

CONTACT INFORMATION

Computer Science Journals Sdn BhD
B-5-8 Plaza Mont Kiara, Mont Kiara
50480, Kuala Lumpur, MALAYSIA
Phone: 006 03 6207 1607
006 03 2782 6991

Fax: 006 03 6207 1697

Email: cscpress@cscjournals.org

CSC PUBLISHERS © 2011
COMPUTER SCIENCE JOURNALS SDN BHD
M-3-19, PLAZA DAMAS
SRI HARTAMAS
50480, KUALA LUMPUR
MALAYSIA

PHONE: 006 03 6207 1607
006 03 2782 6991

FAX: 006 03 6207 1697
EMAIL: cscpress@cscjournals.org