For Small and Medium Size Enterprises (SME) Deliberating Cloud Computing: A Proposed Approach

JANET L. KOURIK
Mathematics and Computer Science
Webster University
St. Louis, Missouri 63119, USA
kourikJL@webster.edu

Abstract: - Cloud computing is composed of complex systems using many different technologies, services, and delivery mechanisms and growing dramatically. Potential benefits of cloud computing include reducing IT capital expenditure, providing rapid dynamic scaling of resources on a metered basis, as well as transparency related to platforms, storage, transmission and processing of data. However, these benefits come with many potential problems. There is an urgent need to investigate and understand security assurance in cloud computing. Small to medium enterprises (SMEs) may be unable to dedicate specialized staff and other resources to this end. This paper argues that emerging taxonomies, frameworks and guidelines, collectively referred to as instruments in this paper, can facilitate SME enquiry into cloud computing. The instruments have been developed and refined by industry and government consortia. Yet, these instruments are rarely referenced in the academic literature, drawing attention to a continuing gap between industry and academia. The proposal is oriented in the context of a prevailing definition and model of cloud computing. Potential benefits and drawbacks in cloud computing are presented. Organizations responsible for developing the instruments are depicted followed by the systematic approach based upon the cloud instruments. Risk assessment and several of the cloud instruments are central to illuminating cloud computing for SMEs. Additionally, the proposal offers an opportunity for industry and academic collaboration.

Key-Words: - Cloud computing, risk assessment, risk management, information security and assurance.

1 Introduction

The adoption of cloud computing is growing rapidly. Nearly 69% of Americans use cloud computing services such as webmail, online backup, etc according to. India reports over 1,500 companies use blended cloud-based communication services (voice, chat, and data). The PEW Research Center conducted a survey on the "Future of Cloud Computing" in 2010 [10]. Findings include estimates that by 2020, over 70% of users will use internet-based (cloud) software to perform work.

The use of cloud computing is increasing, yet data breaches and other problems are reported in the news nearly every week. In fact, the largest barriers to adopting cloud computing are related to security, confidentiality and privacy [2] [6] [8].

Senior decision-makers in SMEs often are not aware of cloud computing. If the decision-makers are aware of cloud computing, they often report not understanding the technology. Some features of cloud computing would be particularly beneficial to SMEs such as reducing IT investment. SMEs often have fewer IT related resources to devote to security and to consider cloud computing [6][8]

This paper proposes a more accessible path for SMEs to use in their approach to cloud computing. Section 2 introduces the prevailing definition of cloud computing along with its widely accepted model. Section 3 describes some major advantages and disadvantages of cloud computing. Emerging taxonomies, frameworks and guidelines, collectively referred to as instruments in this paper, serve to communicate, direct and measure controls need for cloud computing. They progressively expose potential cloud consumers to the terminology of the cloud and risk and offer instruments to explore risk assessment in the cloud. Section 4 presents several of the key groups that are responsible for building the instruments. Section 5 presents a systematic approach to cloud computing for SMEs based on risk assessment (RA).

Section 6 summarizes important concepts, contributions, and future directions.

2 Cloud Computing

Cloud computing is nascent with publications appearing in the Institute of Electrical and Electronics Engineers (IEEE) and Association of

Computing Machinery (ACM) digital libraries in late 2007 to early 2008. A 2009 examination of Google search terms reported that 'cloud computing' starts to appear in the third quarter of 2007. Within a year, usage of cloud computing overtakes and replaces the search phrases 'grid computing', 'distributed computing' and 'utility computing'. An introduction cloud computing and the complexity of managing cloud risk is provided by [1] [7] [11].

2.1 NIST Definition of Cloud Computing

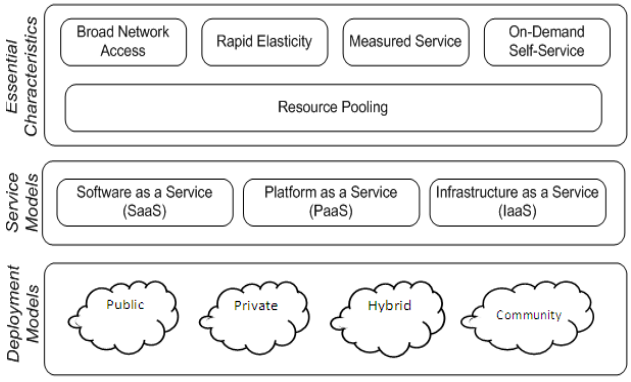
After contributions from many sources and much debate, a formal definition of cloud computing developed by the National Institute of Standards and Technology (NIST) was released in October of 2009. The current version (v26) follows:

> "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models. [9]"

The NIST definition has become an accepted standard by many in the field including European Network and Information Security Agency (ENISA).

The cloud computing definition offered by NIST organizes concepts around three major elements: A) characteristics, B) cloud service models, and C) cloud deployment models as shown in Figure 1.

Figure 1: NIST Cloud Computing Model [5].



Five characteristics (broad network access, rapid elasticity, measure service, on-demand self-service and resource pooling) are considered essential to cloud computing. The three cloud service models, perhaps the most recognized cloud topics terms, are: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). The SPI model represents SaaS, PaaS, and IaaS. Public, private, hybrid, and community are the four deployment models for cloud computing.

3 Potential Benefits and Drawbacks of Cloud Computing

3.1 Potential Benefits of Cloud Computing

Cloud computing offers many potential benefits that are distinct from many current information systems. Cloud computing extends the idea of resource pooling by an order of magnitude. Historic quantities of pooled resources, say servers, enables the cloud service provider (CSP) to achieve economies of scale. Using the rental model, cloud resources may be shared by any organization even competitors. The idea of multi-tenancy introduces significant challenges.

Measured service implements the idea of renting IT resources. The cloud consumer pays for only the resources consumed yet has access to many additional resources. This approach can dramatically reduce capital IT expenses. Those resources though, must be able to handle maximum loads.

Rapid elasticity is the ability for the consumer to almost instantly employ additional resources from the CSP. If an average load requires 100 web servers, a sudden, dramatic spike in demand would automatically allocate 1000 servers if needed.

The consumer must be able to procure additional resources as needed from the CSP. Typically this is called on-demand and self-service capability.

Security benefits are also possible, for example the cloud can reduce single points of failure through replication, multiple locations. CSPs are more likely to employee teams of security and assurance experts unlike many SMEs.

3.2 Potential Downside of Cloud Computing

Major disadvantages in cloud computing are found in areas such as organizational, technical and legal. Some of the major technical risks include: multi-tenant environment; internet as connection; system complexity; and loss of control. Legal issues include governance, compliance, and problems generated by data crossing national, legal, and regulatory boundaries [9] [11]. With resource pooling it may be difficult to recover data or unauthorized recovery of data may occur. Metering

ISBN: 978-960-474-297-4

offers the potential to bypass the meter or assign the usage to another tenant.

Traditional approaches to security and assurance often focus on system perimeters placing firewalls, and other barriers there. Perimeters are not as clear cut in the cloud particularly with multi-tenancy. The internet is a weak area as many internet protocols lack or limit security features.

New vulnerabilities inherent to cloud computing include breaches from one virtual computing space to another, misappropriation of session security from web protocols, and limited encryption capabilities in many protocols.

Cloud computing may also be used in support of malicious activities such as denial of service attacks or cracking encryption.

4 Organizations

Many organizations are working to enable the transition to cloud computing. ENISA and NIST represent governing bodies in the European Union and US respectively. The remaining groups are consortia of representatives from industry research & design, vendors, consumers, academia and in some cases government.

4.1 European Network & Information Security Agency (ENISA)

The European Network and Information Security Agency (ENISA) focuses on network and information security. ENISA investigates information security to address, respond to, and prevent security problems. ENISA coordinates the development and exchange of best practices and advice among business, industry, institutions, and EU Member States.

4.2 National Institute of Standards and Technology (NIST)

As described previous, the National Institute of Standards and Technology (NIST) is similar in nature to ENISA in that it is an agency of the US government. NIST houses the Information Technology Laboratory that guides the nation and federal agencies on matters related to information systems, security, and privacy.

4.3 Cloud Security Alliance (CSA)

Another strong presence in the field of cloud risk and security is the Cloud Security Alliance (CSA). The CSA was launched in April 2009 and is composed of information security experts and practitioners from some of the largest computing and technology companies such as Qualys, RSA Security, Barclays, and Visa. CSA membership consists of North America (47%), Europe (34%) with the remaining members representing the Middle East, Africa and Asia.

Focused on security assurance in cloud computing, the non-profit group works to develop best practices and consensus across many constituencies. CSA working groups highlight the breadth of concerns in cloud computing.

4.4 The Open Group (OG)

The Open Group is consortium with a goal to use open interfaces to achieve improved interoperability. Largely the goal is achieved by involving both suppliers and consumers to develop consensus about application programming interfaces (API), process models, and eventually standards. The Open Group is well known for its role in developing approaches to IT Architecture Framework in large enterprises under the name TOGAF. While consortium includes members from academia and other consortia, the governing board is composed of representatives from some of the largest technology consumers and providers. Many of the processes to design and develop interoperability are restricted to members only, however results of those efforts are freely available for use. The Open Group also has established certifications for standards such as CORBA, POSIX, UNIX as well as TOGAF. Cloud computing relies very heavily on interoperability in various service models such as SaaS, PaaS, and IaaS as well as various deployment models.

5 Risk Assessment Instruments

SMEs could benefit substantially from cloud computing with elasticity and metering being especially helpful to finances. SMEs may find it simpler and faster to turn complex IT requirements over to cloud service providers (CSP) than to build the specialized expertise in-house.

There are several barriers to the adoption of cloud computing. Security, privacy and control of data are significant barriers. SMEs often lack awareness or knowledge of cloud computing. SMEs are more likely to have limited technical resources available to toward cloud computing.

Emerging taxonomies, frameworks and guidelines, collectively referred to as instruments in

ISBN: 978-960-474-297-4

this paper, are being developed by industry and government communities. Several have adapted risk assessment as a viable way to examine the cloud computing environment. It is noteworthy that these instruments are rarely, if ever, mentioned in the IEEE or ACM literature.

In recognition of the growing need, limited resources, and availability of a range of cloud specific instruments a pathway to enable SME exploration of cloud computing is proposed. After examining of a wide range of cloud instruments, the following systematized approach is put forward. The first three instruments (Nos. 1-3) provide a plain language introduction to significant cloud computing and risk assessment concepts. The fourth (No. 4) provides very brief, high-level exposure to risk assessment. If the SME has a continued interest in cloud computing the next three instruments (Nos. 5-7) delineate very detailed approaches to risk assessment in the cloud.

5.1 Open Group-Risk Taxonomy

The risk taxonomy [12] is the place for SMEs to begin. Practitioners and researchers are faced with the need to master many different concepts in order to consider cloud computing and formal concepts about risk may be new to many in IT.

The Open Group (OG) leveraged its experience from work on interoperability to develop a formal taxonomy of security and risk terminology in 2009. OG's view is that precision is vital to measurement, and measurement is essential making decisions to manage risk.

The taxonomy specifies strict definitions for 13 terms with a formal hierarchy to describe the relationships between terms. Subtypes or scales are provided for security terms, e.g. six forms of loss are productivity, response, replacement, fines and judgments, competitive advantage, and reputation.

OG focused on the frequency of risks in combination with the magnitude of loss. Metrics, both quantitative and qualitative, are recommended to improve the accuracy and value of the risk assessment. Of particular value is a fully worked scenario specification of metrics to a complete matrix representing loss event frequency by probably level of magnitude.

The taxonomy is an indispensable, yet concise, introduction to risk analysis. As such, it should be studied, if possible, before proceeding to the remaining instruments on assurance in cloud computing.

5.2 CSA-Top Threats to Cloud Computing

This slim offering is the fast path to understanding potential problems in cloud computing. Along the way it also provides a light introduction to cloud computing. CSA and ENISA proposed, debated and ultimately distilled a list of seven top threats in cloud computing along with the estimated impact for each threat, remediation options and suggested resources. For each threat, the working group also specifies its relationship to the SPI service models (IaaS, PaaS, and SaaS) and the related domain(s) in the Security Guidance described below [www.cloudsecurityalliance.org].

5.3 NIST-Guidelines on Security and Privacy in Public Cloud Computing (Guidelines))

NIST published a new draft of the Guidelines on Security and Privacy in Public Cloud Computing in January 2011 [9]. Coverage in the Guidelines is quite broad. A brief explanation of service level agreements (SLA) in public cloud services is included along with a short summary of the positive and negative aspects of the public cloud. Nine security and privacy themes are each examined by highlighting three to six significant barriers or risks for the public cloud. At this point SMEs should have a high-level appreciation for critical topics and enough guidance to make more informed decisions on such topics.

An examination of cloud computing through the lens of IT outsourcing is distinctive. A limitation is that some sections are specific to US laws.

5.4 ENISA - Information Assurance Framework

This instrument provides an introductory and succinct guide to assessing cloud service providers (CSP). It is a tool for consumers to evaluate cloud service providers [4]. ENISA asserts the framework can also reduce work for CSPs. Further, the framework incorporates many previous information security standards such as ISO 27001/2 and BSI BS25999. Several significant contributions include:

- Suggested division of responsibilities and liabilities between the consumer and the CSP.
- Information assurance requirements for 10 areas of an entity.
- Cautions regarding the use of cloud computing in e-Government.

ISBN: 978-960-474-297-4

ENISA clearly states that risk can only be transferred to a limited degree. Even if a cloud service provider makes reparations following a problem, it will be the reputation of the cloud consumer that is damaged. In the end, true risk will always stay with the consumer.

5.5 CSA - Security Guidance for Critical Areas of Focus in Cloud Computing V2.1

Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 is tool to help SMEs decide if, as an organization, they are ready to use cloud computing for a specific asset and process. The instrument described in [3] can be used to "test the waters" before a transition is initiated. CSA clearly states that this is not exhaustive, is not a full risk assessment framework or a methodology for all needs.

All recommendations are organized in 13 domains, the "critical areas of focus" in the document's title. The 13 domains are divided to three categories: A) cloud computing architecture, B) governance, and C) operations. Governance includes the following domains: governance and enterprise risk management; legal and electronic discovery; information lifecycle management; compliance and audit; as well as portability and interoperability. The operations category includes eight domains: traditional security, business continuity and disaster recovery; data-center operations; incident response, notification and remediation; application security; encryption and key management; identity and access management; and virtualization. The substance of the guide rests on very detailed recommendations for each domain. Each of the 13 domains is described in condensed form, followed by subsets of recommendations. The recommendations have been revised over time to reflect field experience gained during use in industry.

5.6 ENISA-Cloud Computing: Benefits, Risks, and Recommendations for Information Security

A clear classification of cloud computing risks, vulnerabilities, and assets is presented in [5]. The relationships between each risk and the kind of assets and vulnerabilities involved are described explicitly. Thirty-five risks are identified, of which 24 risks are specific to cloud computing. Over 50 vulnerabilities and 20 assets are delineated. Moreover, for each risk an approximate rating for probability and impact is provided using a scale from very low to very high. The probability and impact ratings are used to chart each risk in a scatter plot. The scatter plot is overlaid with a grid to categorize each risk on the scale of 0 to 8 representing the no probability or impact up to very high probability and very high impact. The sections that describe risks, vulnerabilities and assets offer a very concise synopsis, based on the consensus of experts, about a complex topic.

An Information Assurance Framework is offered in the form of questions to ask a cloud provider. The questions are categorized by areas similar to those in existing ISO information security standards. Business organizations can then select appropriate groups of questions for the cloud project being considered. Responsibilities and liabilities for both customer and provider across the SPI service models (SaaS, PaaS, and IaaS) are identified.

Key legal issues and recommendations to ENISA are also included along with cases demonstrating the application of the framework.

5.7 CSA-Domain 12 Guidance for Identity and Access Management (IAM) V2.1

This Trusted Cloud Initiative focuses on secure and interoperable identity in cloud computing. Domain 12 Guidance was extensively revised and re-issued in April 2010. This version of Domain 12 will be most useful to specialists familiar with existing protocols and architecture. For other readers, Domain 12 illustrates the complexity of IAM [www.cloudsecurityalliance.org].

IAM for the cloud is organized into four functional areas: A) identity provisioning and deprovisioning B) authentication and federation, C) authorization and profile management, and D) support for compliance.

IAM for the cloud is organized into four functional areas: A) identity provisioning and deprovisioning B) authentication and federation, C) Authorization and user profile management, and D) support for compliance. The sections on identity provisioning and access control in IAM include considerable changes.

Each functional area includes an overview of requirements and challenges followed by an analysis of the area in relation to SaaS, PaaS, and IaaS. Detailed solutions and recommendations become

ISBN: 978-960-474-297-4

increasingly technical. However, key questions for cloud consumers to ask of cloud service provider would enable SMEs to start necessary discussions.

Most significantly, Identity as a Service (IDaaS) is introduced. IDaaS must support different types of users. Interactions for those users will differ by service module (SPI). IDaaS is its infancy; as a result recommendations include directions for further research and development.

6 Conclusion

Cloud computing is an exceedingly complex technology that has great potential benefits. For SMEs, cloud computing can lower the entry cost for powerful IT capabilities by reducing the need for hardware and software ownership costs and a large IT staff. The idea of metered services may minimize expenses for SMEs, particularly at startup. On-demand elasticity enables rapid scaling of resources as the SME grows and has the potential to provide a competitive advantage.

Cloud computing does come with many serious security and assurance challenges particularly in the areas of identity, authentication, data assurance, and compliance. Research projects investigating technology solutions are numerous but many security challenges are open issues.

The technical expertise required to implement cloud computing can be daunting to SMEs with limited IT resources. Risk assessment (RA) is proposed as a viable tool to security assurance in the cloud. While the research literature in cloud RA is just appearing, governments and industry consortia have crafted a variety of tools to address cloud RA.

This paper presented a way of applying cloud risk instruments in a systematic manner to assist SMEs in exploring cloud computing. The first instruments entail an orientation to this complex technology. SMEs can rapidly become acquainted with the fields of cloud computing and risk via the formal taxonomy of risk, cloud threats and fundamental cloud computing concepts.

The next step involves using a high-level instrument to assist cloud consumers in conducting an assessment of their prospective cloud service provider (CSP). If the SME proceeds, three additional instruments, specifically tailored to the cloud environment, provide guidance for very detailed risk assessments. The integrated view of recent initiatives that can assist SMEs in broadening their view of cloud computing and providing better data for decisions regarding cloud computing.

Future directions include studying SMEs to ascertain the benefits or problems with the proposal. Going forward, the use of industry and government-based cloud risk instruments presents an opportunity for industry and academia to collaborate. Research could examine the standard creation process itself for group design processes to better understand collaboration with external partners. The actual application of the cloud risk instruments may provide empirical evidence regarding effectiveness or revisions. Rapid changes will generate new opportunities for research in cloud computing.

References:

[1] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., et al, 2010. A view of cloud computing. *Commun. ACM* 53, 4 (April 2010), 50-58.

[2] Balboni, P. 2010. Security and privacy in cloud computing: The European regulatory approach. *The Conference Board, Executive action series.*

[3] Cloud Security Alliance, 2009. Security guidance for critical areas of focus in cloud computing V2.1.

[4] ENISA, 2009a. Cloud computing Information Assurance Framework.

[5] ENISA, 2009b. Cloud computing benefits, risks and recommendations for information security. November, 2009.

[6] ENISA, 2009c. An SME perspective on Cloud Computing.

[7] Hartig, K. 2009. What is Cloud Computing? *Cloud Computing Journal.*

[8] IDC Enterprise Panel, 2008. Rate the Challenges Ascribed to Cloud Computing.

[9] NIST, 2009. Effectively and Securely Using the Cloud Computing Paradigm v26.

[10] Pew Research Center, 2010. The future of cloud computing, *Pew Internet & American Life Project*. http://pewinternet.org

[11] Snead, D., 2010. Understanding, preparing for and developing compliance plans for regulatory issues governing cloud computing, *Second International Conference on Evolving Internet* (ICCGI 2010), Valencia, Spain.

[12] The Open Group, 2009a. Risk taxonomy technical standard, January 2009.