Evaluating Security and Privacy in Cloud Computing Services:A Stakeholder's Perspective

Abdullah Abuhussein, Harkeerat Bedi, Sajjan Shiva
Computer Science Department
The University of Memphis
Memphis, USA
bhussein@memphis.edu, hsbedi@memphis.edu, sshiva@memphis.edu

Abstract— **The cloud computing paradigm is now adopted in many organizations in various fields because of its low cost, high availability and scalability features. Healthcare, education, business, and many other domains look at cloud computing as an endeavor to solve the continuous shortage in volume, infrastructure, accessibility, and monitoring potency. However, moving data to the cloud implies shifting control of the customer's data to the cloud service provider indefinitely. Hence, the security and privacy of the customer's information becomes an important issue. Being an emerging field, there is a lack of experience in cloud security and lack of consensus on security and privacy. Assessing and comparing among potential cloud computing services, poses an issue for novice customers interested to move their work to the cloud to choose security options that are sufficient and robust at the same time. This paper attempts to identify and categorize a list of attributes which reflect the various aspects of cloud security and privacy. These attributes can be used to assess and compare cloud computing services so that consumers can make well educated choices. Cloud service providers can use them to build and/or offer better cloud solutions.**

Keywords-component; (Cloud Computing, Security, Privacy Standardization, Legal Aspect.)

I. Introduction

The emerging success of cloud computing in the current Internet commercial landscape has opened new doors for attackers to exploit potential business and industries. This can largely be credited to the ubiquitous connectivity provided by cloud computing platforms where an attacker can inflict damage from almost any geographical location independent of where the cloud service itself is located. Thus, establishing a secured cloud computing infrastructure has been a matter of significant importance to the cloud computing providers and consumers since its inception. However, a key problem in the current landscape is a lack of consensus on a systematic approach for evaluating the security and privacy of such cloud computing services.

In this paper we aim to identify and categorize the attributes which highlight the security and privacy provided by cloud computing services. Then we proceed to present how one can use these attributes for assessing and comparing potential cloud computing services both from a provider and a consumer stand point.

The importance of such an evaluation resides in that it will: (1) increase consumers' awareness of the cloud computing security and privacy issues, (2) increase consumers' knowledge level in the recent cloud computing technologies that are available in market, (3) increase the provider willingness to make these technologies available for their clients in various options based on the consumer needs, (4) makes it easier for consumers to decide and sort of assess the amount of security that is deployed based on the system domain and the consumer needs, and (5) confirms who of the stake holders is responsible for what of the security aspects in the cloud computing environment.

The process of identifying vulnerabilities should include an analysis of the system's security attributes and the security controls used to protect the cloud environment [2]. Therefore, it is essential for cloud computing providers to be able to enumerate these security and privacy attributes in the provided service. In section II we enumerate the potential security and privacy attributes that we believe are sufficient to fulfill the consumers' and cloud service providers' (CSPs) security requirements based on their needs. In section III we demonstrate how such attributes are used to compare and assess the security and privacy offered by Amazon's EC2, Microsoft's Azure and Google's AppEngine. In section IV we highlight some recent work and solutions offered by others towards assessing and comparing the security and privacy of cloud computing services. In section V we provide a brief discussion on certain aspects of security and privacy which are harder to categorize and measure. In section VI we discuss ways in which this approach and be evolved and highlight our future work and conclude.

II. Security and privacy Attributes

A. *Stakeholders' Perspectives of Cloud Computing Security*

Cloud computing consumers lose the most when a cloud service is breached. Stakeholder's perspective must not be neglected when talking about cloud security [4]. In this paper we focus on two major stakeholders, which are the cloud computing service providers and consumers. Paying a penalty for service outage or losing business image once the cloud service consumer's privacy is breached will not make customers come back. Therefore, cloud providers need to carefully choose and customize the security options for their cloud services. Additionally, cloud computing consumers need to have more knowledge and control on how their cloud service is secured to be able to prepare a risk management plan (as an example) and to have more trust with the service provider.

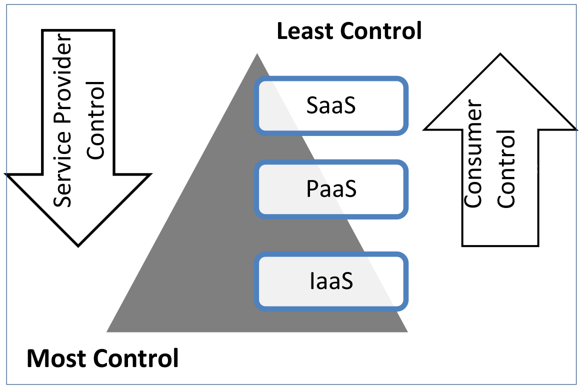

Figure1. Cloud computing security control

Fig. 1 shows the different cloud service models and amount of control the cloud service consumer and provider have for each of them model. We observe that as the cloud service model changes from SaaS to PaaS, to IaaS, the consumer control on security and privacy reduces; however, the provider's control increases.

According to NIST consumers feel more comfortable with the risk when they have more control over the processes and equipment [1]. However, expecting consumer expertise in security and privacy on such emerging domains is not always possible and using attributes for comparing and assessing the security and privacy can be an effective approach towards picking a safer cloud computing service.

A published quantitative analysis of current security concerns and solutions for cloud computing has identified the main problems in the area of cloud computing security and groups them into a model composed of seven categories aiming to organize information related to cloud security and to facilitate future studies [3]. We followed that model to distribute organize our list of security attributes of public cloud computing services. The reason behind adopting that model is because it is closer to what cloud consumers see and deal with in real life cloud computing environments. We enumerated our list of security and privacy attributes under each category of the seven so that it can be easily comprehended by the cloud consumers and covered by cloud service providers in as shown in Table I. Fig. 2 shows how these categories are related in terms of the security aspects that should be considered under each category.

TABLE I. OUR ATTRIBUTES OF SECURITY AND PRIVACY CATAGORIES

Category	**Attributes**
Network security attributes	Encryption
Interface security attributes:	Authentication, Access Control, Client side Protection
Data security attributes	Backup, Encryption, Data Isolation, and Disaster Recovery
Virtualization security attributes	Dedicated hardware, and Hypervisor Security, Encryption
Governance security attributes	Monitoring
Compliance security attributes	SLA Conformity, Standards and certification, and Nested Services
Legal issues security attributes	Data Storage location, and Data Sanitization

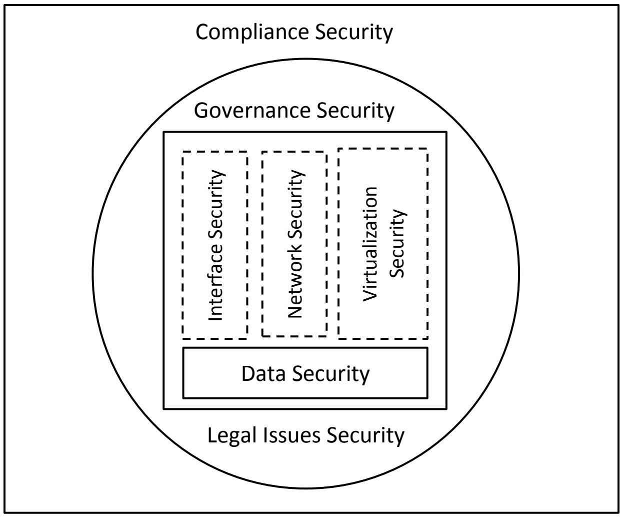

Figure2. The relationship between the different Cloud Computing Security Categories

B. *Explanation of Security and Privacy Attributes:*

In this section we discuss the above mentioned cloud computing security and privacy attributes in brief and explain their importance. We also highlight aspects that should matters to consumers when researching for different CSPs for each attribute.

Backup

Backup service is usually provided by cloud computing providers. It is essential for data protection, recovery, resiliency of data center and data availability.

The most important factors that consumers should care about when researching different CSPs for the backup attribute are (1) what is the size of the backup facility?, (2) how secured is the backup facility itself? [5], (3) compatibility of the backup service with the cloud computing environment in case the backup service was provided by a third party?, (4) what is the restoration bandwidth limitations?, and (5) is an automated backup service offered?

Encryption

Dropbox allowed anyone in the world to access any one of its 25 million customers' online storage lockers simply by typing in any password in 2011[9]. This raise up the necessity of encryption for data that is stored in the cloud and not only data that transfers from and to the cloud.

Consumers need to ensure that (1) are their transactions transferred to and from the cloud service encrypted by default? (2) Is the data that resides on cloud servers encrypted by default? [6] and, (3) what kinds of encryption services are offered by the cloud provider?

Authentication and Access Controls

While authentication provides proof of identity, it does not limit the actions or operations that a legitimate user of a computer system can perform. So, the cloud computing consumer needs to decide who can access what?

A set of questions that can be asked by a consumer to the provider would be: (1) do you provide policies for access control? (2) Who manages these policies? (3) how much control do you have?, and (4) how secured is the authentication system?

Dedicated hardware and Data Isolation

The multi-tenancy property of the cloud computing service put the consumer data under risk of being accesses.

Targeting more customers, Amazon's cloud new offered dedicated hardware in 2011 [8]. Some cloud service consumers tends to request to have their data on a dedicated machine just because they feel it is safer to isolate their data from other's data and transactions.

Dedicated machines address security issues like; some organization's regulations enforce that data has to be in an isolated machine. Also, dedicated physical machine indicates more security for data and transactions plus a better availability for the system which also applies to security.

A consumer should ask the CSP (1) whether they offer dedicated machines to a single consumer; (2) how does a CSP protect dedicated machines from DoS attack? And (3) how do you guarantee that our data is isolated and protected from other customer's data and only privileged personnel are allowed to?

Monitoring

It is necessary after having all the security attributes deployed, to have a monitoring technique to follow up and pull the trigger once an undesired action is noticed. Consumers may want to know the current security status of their systems on the cloud.

To assess this attribute, consumer may want to ask service providers: (1) how quickly you learn about any possible threats? (2) What is your mitigation procedure? Is security monitoring automated? (3) What information you collect to monitor the service for possible threats? And, (4) where all that monitoring information saved?

Data Storage Location

Location of the server where the consumer data resides makes that server exposed to more danger. Consumers should make sure that their service providers will not expose information about the storage location. A Consumer may ask the service provider whether that information about the exact location of the data center will be exposed to the public.

Security Standards and Certifications

Convincing potential customers to trust you with their data can be irrational and time consuming task. Certified CSPs put less effort in convincing their clients about the services they offer since they won't get these certificates unless they follow standards and the best security practices. Consumers might need to ask CSPs whether their service is certified or not?

Data Sanitization

Sanitization is serious data threat in cloud computing environments in several ways. When a cloud service is terminated, what happens to the customer's data?

Some service providers will not erase any of the customer's content as a result of the termination; a consumer may retrieve content from the services only if post-termination fees are paid. This might overhang a consumer security and/or privacy when this data is accessed by attackers.

Consumer should care about: (1) what happens to their original data when the service is terminated? (2) What happens to their cached or back-up copies? And, (3) whether the data will be purged within a certain time of the end of the retention period?

SLA Conformity

The authors of [3] shows that the number of citations for Legal and governance issues represents 73% of security concern citations.

Consumer should ask questions like; if performance doesn't guarantees defines in SLA, how will consumer be compensated?

Disaster Recovery

Consumers need to have a disaster recovery plan for their business continuity. Disaster Recovery as a Service is also coming up these day to allow business owner to rapidly have come back online after a failure.

Some concerns in Disaster recovery that consumer needs to take care of are: (1) Do the service provider offer a disaster recovery plan? (2) Is the recovery process automated? And, (3) what is the downtime if a disaster occurred?

Performance and Scalability

Cloud service consumers might want to scale up their services. The issues that matters consumers the most here are (1) how will the cloud service behave during and after the scale up operation?, (2) How fast will the scale up operation be? (3) And what will happen to the service during the scale up action?

Hypervisor Security

The multi-tenancy property of the cloud computing created this serious cloud computing security and privacy issue. Hypervisors or virtual machines allow multiple operating systems, called guests, to run concurrently on a single physical machine.

Consumers should care about (1) how do CSPs manage hypervisor defense against network/data vulnerabilities which can be caused by sharing of physical resources? (2) Can they identify and defend against side-channel attacks?

Client Side Protection

Although the location of most of the transactions and the final destination of the data or service journey is outside the end user side, but the end user cannot be neglected. They share some amount of the responsibility once an attack takes place. There many forms of connections (wired and wireless) that can be used by end users to connect to your cloud service. Likewise, end users can use many devices to connect to the cloud (Personal computers, smartphones, etc.) each of which can have its own security weaknesses. For instance, a spyware was sent to an end user that was used to send more than 1,000 screen captures of confidential information about 62 Ohio hospital patients in 2008 [7].

Consumers need to know (1) how CSPs manage to catch malicious access to the cloud coming from the end user's side? (2) Do you use secure protocols like SSL, HTTPS to connect to your clients?

Nested Services

Nested or composite service can become a vulnerability when a consumer gets different services from different vendors. For example, a consumer is purchasing the infrastructure from an IaaS service provider and SaaS from another service provider or, a public SaaS provider could build its services upon those of a PaaS or IaaS cloud. Of course, this will shift the security responsibility to the service provider but, SaaS security and availability will be Infrastructure dependent.

To be able to overcome similar problems; a consumer must be aware of these situations and make sure that (1) both purchased services are compatible with each other's and, (2) SLA covers all the aspects of security when there is a third party providing other services.

III. Assessing Security and Privacy of Cloud Computing Services

After briefly explaining our list of attributes in the previous section, we now explain how these attributes can be used to assess and compare potential cloud computing services. We consider three prominent commercial CSPs, namely, Amazon EC2, Microsoft Azure, and Google AppEngine. We assess and compare these CSPs in a tabular form, as shown in Table II. Here, the first column enumerates our attributes, the second column highlights a common concern a customer may have regarding the attribute, and the remaining columns explain how these CSP address the customer's concern based on the corresponding attribute. All CSP information used for this comparison was obtained from their official and publicly available documentation [14, 15, 16, 17, 18, 19].

TABLE II. A comparison between three cloud service providers based on our cloud computing security/privacy attributes

Security and Privacy Attributes	***Consumer Concern***	***Amazon EC2***	***Microsoft Azure***	***Google AppEngine***
Backup	Do you offer automated backup services?	Amazon has the compute cloud EC2 and the data repository S3 . By default one can back up from EC2 to S3 using simple Amazon provided scripts like ec2-bundle-vol and ec2-upload-bundle. One can either run them manually or use scheduling tools like cron.	It is advised that customers create a second Storage Account to provide hot-failover capability. In such a scenario, customers can create custom roles to replicate and synchronize data between Microsoft facilities.	Not offered. It is the responsibility of the user to perform this operation. Example: Google App Engine Backup and Restore (or Gaebar, for short).
Encryption	Do you offer encryption services for protecting user or system data?	No. If encryption is important, then they recommend that one runs an encrypted file system on top of your Amazon EBS (Elastic Block Storage) volume.	Encryption is used internally within Windows Azure for protecting control channels. SSL encryption is used for this purpose. It is also provided optionally for customers who need rigorous data protection capabilities. At the customer's discretion, the Windows Azure SDK extends the core .NET libraries to allow developers to integrate the .NET Cryptographic Service Providers within Windows Azure.	No. The user has to implement it manually using the "javax.crypto.*" classes.
Authentication and Access Controls	(1) do you provide policies for access control? (2) who manages these policies? (3) how much control do you have? (4) how secured is the authentication system?	AWS Identity and Access Management (IAM) enable secure control access to AWS services and resources for your users. EC2 had Roles for EC2 instances is a new feature that makes it easier for you to securely access AWS	Azure Access Control Service (ACS) to authenticate users from identity providers like Windows Live, Google, or Facebook Integration with Windows Identity Foundation. Support for popular web identity providers (IPs) Support for Active Directory Federation Services An Open Data Protocol (OData)-based management service	Google Accounts is Google's unified sign-in system. The option for restricting an application's authentication settings can only be set at app creation time
Dedicated hardware and Data Isolation	Can we run hardware dedicated to a single customer.	Dedicated Instances run on Dedicated Hardware	No dedicated hardware Isolation of Hypervisor, Packet Filtering, and VLAN Isolation	No, however data isolation can be manually implemented
Monitoring	(1) how quickly you learn about any possible threats? (2) What is your	AWS utilizes automated monitoring systems to provide a high level of service performance and	Security is monitored with the aid of centralized monitoring, correlation, and analysis systems that manage the large amount of	App Engine System Status Dashboard monitors performance, and review error logs

Security and Privacy Attributes	***Consumer Concern***	***Amazon EC2***	***Microsoft Azure***	***Google AppEngine***
	mitigation procedure? Is security monitoring automated? (3) What information you collect to monitor the service for possible threats? (4) where all that monitoring information saved?	availability. Alert Logic Threat Manager for EC2 is the first Network Intrusion Detection (IDS) service specifically designed for Amazon Web Services.	information generated by devices within the environment, providing pertinent and timely monitoring and alerts. Customers can optionally choose to run more sophisticated health monitoring processes	
Data Storage Location	Is the information about the exact location of the data center exposed to the public?	Publically available regions and availability zones. Consumers may specify the region.	Customers may specify the geographic region(s) of the Microsoft datacenters in which Customer Data will be stored. At present, the available major regions are Asia, Europe, and the United States.	Google AppEngine provides SaaS and PaaS. Consumers Applications are and run across multiple servers.
Security Standards and Certifications	Is your environment certified?	EC2 has the following certifications SAS70 Type II, PCI DSS Level 1, ISO 27001, and FISMA	(The Microsoft cloud has obtained ISO/IEC 27001:2005 certification and SAS 70 Type 1 and II attestations)	Google has received a SSAE 16 certification for both the Google Apps cloud productivity and collaboration suite and the Google App Engine platform. (SSAE-16 is an evolution of the SAS 70 Type II audit)
Data Sanitization	If I terminate service, what happens to your copy of my data?	Amazon EC2 will not erase any content as a result of the termination; consumer may retrieve Content from the Services only if any charges for any post-termination use of the Service Offerings and all other amounts due is paid Amazon EC2 will provide consumer with the same post-termination data retrieval assistance that we generally make available to all customers"	contact Microsoft and tell whether to: (1) disable your account and then delete your customer data; or (2) Retain your customer data stored in the online service in a limited function account for at least 90 days after for extraction of the data. Following the expiration of the retention period, we will disable your account and then delete your customer data. Cached or back-up copies will be purged within 30 days of the end of the retention period."	Google will provide Customer access to, and the ability to export, the Application and any Customer Content for at least 15 days; Customer will delete the Software and any Application (including any Customer Content) Following a commercially reasonable period of time, Google will delete the Account and Upon request, each party will use commercially reasonable efforts to return or destroy all other Confidential Information of the other party.
SLA Conformity	If performance doesn't guarantees defines in SLA, how will I be compensted?	10% credit, if the Annual Uptime Percentage for a customer drops below 99.95% for the Service Year.	If the monthly connectivity uptime service levels drops below 99.95%, consumer gets 10% credit on next month’s bill. If the monthly connectivity uptime service levels drops below 99%, consumer gets 25% credit on next month’s bill.	If the monthly connectivity uptime service levels drops is between 99.95%,- 99.00% consumer gets 10% credit on future bill. If the monthly connectivity uptime service levels drops is less than 99.00 and more than or equal 95.00% consumer gets 25% credit on future bill. If the monthly connectivity uptime service levels drops is less than 95.00 consumers gets 50% credit on future bill.
Disaster Recovery	Can we recover the data if there is a disaster in the cloud infrastructure? How to recover the user's data/application-processes in case of a disaster in the cloud? (This is a data-availability issue.)	CloudArray used by Amazon offers data copy policies that replicate data across local storage and a variety of third party storage cloud providers to ensure high data availability. CloudArray also enables replication between service	Azure also has its own internal disaster management measures. Security services ensure token federation, claims transformation. These services are built on open standards, WS-Security, WS-Trust, WS-Federation, SAML protocols and OpenID. With the information consumers/users get through these standards about the operation, the Azure encourage configuring their	Data is replicated at multiple datacenters for redundancy and consistent availability.

Security and Privacy Attributes	***Consumer Concern***	***Amazon EC2***	***Microsoft Azure***	***Google AppEngine***
		providers.	cloud usage for data/applications for high availability and disaster management.	
Performance and Scalability	Can we scale our operations, in terms of both data stored and processes run, with still performing at the optimum level of operation? How is it taken care of?	The cloud infrastructures are tuned to eliminate barriers and streamline IT operational processes (that range) that exist in most mid-sized enterprises today.	Agents monitor each VM instance for failure conditions and collect metrics regarding failures Performance measures and usage metrics. Azure Fabric automates the provisioning and management aspect with limited human input. Applications run in a partial-trust sandbox, requests are load balanced and failure conditions are automatically managed.	User provisioning utility and API connect Google Apps to your existing user directory encourages the users deep handles to customize to tune up the performance during scaling of operations.
Hypervisor Security	(1) How do CSPs manage hypervisor defense against network/data vulnerabilities which can be caused by sharing of physical resources? (2) Can they identify and defend against side-channel attacks?	Privileged access to hypervisors through paravirtualization Instance Isolation Firewall resides within the hypervisor layer	Isolation of Hypervisor, Root OS, and Guest VMs. Hypervisor Packet Filtering VLANs partition a network such that no communication is possible between VLANs without passing through a router, which prevents a compromised node from faking traffic from outside its VLAN except to other nodes on its VLAN	Google AppEngine provides SaaS and PaaS. There is no hypervisor
Client Side Protection	(1) How CSPs manage to catch malicious access to the cloud coming from the end user's side? (2) Do you use secure protocols like SSL, HTTPS to connect to your clients?	Any support or services to End Users unless we have a separate agreement with you or an End User obligating us to provide support or services. EC2 users can now use Symantec's Endpoint Protection.	Least Privilege Customer Software to protect the customer's service from attack by its own end users. End users are by design not trusted by the Windows Azure infrastructure or by our default customer configuration, and so Azure infrastructure provides mechanisms to protect against end users and for our customers to secure their services against them.	Consumer responsibility
Nested Services	(1)Are the purchased services compatible with each other's (2) Does SLA cover all the aspects of security when there is a third party providing other services.	Amazon EC2 SLA excludes unavailability, suspension or termination of Amazon EC2 that result from any actions or inactions of you or any third party that result from consumer equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control)	Microsoft Azure SLA excludes any performance or availability issue result from third party hardware or software. Third Party Offering will be governed by the applicable privacy statement and policies from the third party.	Google AppEngine SLA does not cover to any errors caused by factors outside of Google's reasonable control that resulted from third party software or hardware that are result of abuses or other behaviors that violate the Agreement.

IV. RELATED WORK

In late 2011, NIST came up with a list of public cloud computing security and privacy issues [1]. In Table III below we show how our list of cloud computing security and privacy attributes are mapped to those of NIST. Our security attributes cover all the nine security and privacy issues. Thus, by using our list of attributes consumers will have a service that is equipped against the well-known cloud computing security issues. Numbers beside the NIST Security and Privacy Issues corresponds to NIST “Guidelines on Security and Privacy in Public Cloud Computing” document [1].

TABLE III. OUR CLOUD COMPUTING SECURITY/PRIVACY ATTRIBUTES MAPPED TO NIST STANDARD SECURITY AND PRIVACY GUIDELINES [1]

Security/ privacy attribute	NIST Security and Privacy Issues
Backup	7.Data Protection 8.Availability
Encryption	9. Data Protection 8.Availability
Cloud Employee Trust	1. Governance 2.Complience (Law and regulation) 3. Trust (Insider Access)
External Network Security	9. Incident Response (Incident Analysis and Resolution)
Access Controls	5. Identity and Access Management (Acess Control)
Dedicated Hardware and Data Isolation	4. Architecture 7. Availability 2.Compliance (Data Location) 3.Trust (Data Ownership) 3. Trust (Composite Services)
Authentication Management	5. Identity and Access Management (Authentication)
Monitoring	9. Incident Response (Incident Analysis and Resolution)
Storage Location	2. Compliance (Data Location)
Security Standards and Certifications	1. Governance 2.Complience (Law and regulation)
Data Sanitization	2.Compliance (Electronic Discovery) 3. Trust (Data Ownership) 3.Trust (Ancillary Data) 7. Data Protection (Data Sanitization) 7. Data Protection (Value Concentration)
SLA Conformity	1. Governance 2. Compliance 3. Trust 4. Architecture 5. Identity and Access Management 6.Software Isolation 7. Data Protection 8. Availability 9.Incedint Responce
Disaster Recovery	3. Trust (Risk Management) 8. Availability (Denail of Service) 8. Availability (Tempopary outage) 8. Availability (Permenant Outage) 9. Incident Response (Incident Analysis and Resolution)
Performance Over Scalability	4. Architecture 8. Availability 9. Incident Response (Incident Analysis and Resolution)
Hypervisor Security	4.Software Isolation (Hypervisor Complexity) 4.Software Isolation (Attack Vectors)
Client Side Protection	3.Trust (Insider Access) 6.Software Isolation
Nested Services	1. Governance 3.Trust (Composite Services)

There has been a lot of work on trying to differentiate between different CSPs in terms of performance, response time, etc. [11, 12]. Our work is significantly different in the sense that we do not only research a specific attribute like availability, but we went beyond that to provide the consumer with 17 attributes to make the decision on how safe the data will be in the providers’ hands.

V. CONCLUSION

Securing the cloud is not an easy task especially after vulnerable incidents we see and hear every day. One problem that consumer cannot really get a true answer when researching CSP for a service is the inside trust. Cloud-related insider threat lays in three groups; the cloud provider administrator, the employee in the victim organization that exploits cloud weaknesses for unauthorized access, and the insider who uses cloud resources to carry out attacks against the company’s local IT infrastructure [10]. Although we in this paper care about the first group that is a cloud provider administrator who uses the administrator account to threaten the consumer’s cloud security and/or privacy however, CSP tends not to publish information about such incidents. This is a challenging research area and is open for researchers to investigate [10].

Another issue that remains open is the emergence of new dimensions in securing parts of the cloud. New attributes for securing the different parts of a cloud computing environment that are not mentioned in this paper may be needed. To the best of our knowledge, this is perhaps the first work that aims to evaluate the amount of security that is applied to a cloud computing service. Our goal is to provide hesitant consumers who are still thinking about moving their work or parts of it to cloud or current cloud computing consumers who are curious about how secured is their data with a set of evaluating criteria to end their confusion.

We have demonstrated in this paper that our set of attributes conforms to those from NIST. We have also demonstrated that the different security aspects of three well known cloud computing providers (Amazon EC2, Microsoft Azure, and Google AppEngine) can be evaluated to give cloud computing consumers a better view of their security features. We are now working on developing metrics that aid in quantifying these attributes.

VI. REFERENCES

[1] NITS, “Guidelines on Security and Privacy in Public Cloud Computing”, http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf, retrieved on Sep 29, 2012.

[2] NIST, “Risk Management Guide for Information Technology Systems” , SP 800-30, NIST, July 2002, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, retrieved on Sep 29, 2012.

[3] Gonzalez N., Miers C., "A quantitative analysis of current security concerns and solutions for cloud computing", Third IEEE International conference on Cloud Computing Technology and Science, pp 231-238, 2011.

[4] Shandilya V., Shiva S., “Security in the cloud: a stake holder's perspective, SAM'12, July 2012

[5] Florence G., “why is there a need for cloud computing backup?”, Cloudtweaks.com from: http://www.cloudtweaks.com/2012/03/why-is-there-a-need-for-cloud-computing-backup/ , on March 20, 2012

[6] Heels E.,“Is Encryption the Solution to Cloud Computing Security and Privacy?”, Enterprise Cloud Computing Blog, reteived from:

http://www.cloudswitch.com/page/is-encryption-the-solution-to-cloud-computing-security-and-privacy , Aug 04, 2011.

[7] McMillan R., “Misdirected Spyware Infects Ohio Hospital”, PC Magazine, IDG News Service September 17, 2009,retrieved from: http://www.pcworld.com/businesscenter/article/172185/misdirected_spyware_infects_ohio_hospital.html

[8] Ricknas M., Amazon's cloud new offers dedicated hardware, infoworld, Cloud Computing, March 28, 2011 From: http://www.infoworld.com/d/cloud-computing/amazons-cloud-new-offers-dedicated-hardware-910

[9] Singel R. , “Dropbox Left User Accounts Unlocked for 4 Hours Sunday”, June 2011 retrieved from: http://www.wired.com/threatlevel/2011/06/dropbox/

[10] Claycomb W., Nicoll A. , “Insider Threats to Cloud Computing: Directions for New Research Challenges”, CERT Program. Software Engineering Institute, Carnegie Mellon University, 2012 Global

[11] Provider View, https://cloudsleuth.net/global-provider-view, retrieved on Sep 29, 2012.

[12] Cloud Harmonsy Speed Test, http://cloudharmony.com/speedtest, retrieved on Sep, 29, 2012.

[13] Google App Engine, http://code.google.com/appengine/articles/gae_backup_and_restore.htm, retrieved on Sep 29, 2012.

[14] Amazon EC2 FAQs:, http://aws.amazon.com/ec2/faqs/, retrieved on Sep 29, 2012.

[15] Microsoft, “Technical Overview of the Security Features in the Windows Azure Platform”, http://www.microsoft.com/online/legal/?langid=en-us&docid=11, retrieved on Sep 29, 2012.

[16] Google App Engine Service Level Agreement retrieved on Sep 29, 2012 from: https://developers.google.com/appengine/sla

[17] Amazon EC2 Service Level Agreement, retrieved on Sep 29, 2012 from: http://aws.amazon.com/ec2-sla/

[18] Microsoft Azure Service Level Agreement , retrieved on Sep 29, 2012 from: http://www.windowsazure.com/en-us/support/legal/sla/