Cloud Computing: Securing without Losing Control

Mubarak S. Almutairi

1. INTRODUCTION

As early as 1960s, tremendous efforts have been made in the computing arena to separate end-users from computing-hardware requirements. These efforts have gone through different transitional phases starting from the concept of time-sharing resources, network computers, all the way to the recent cloud computing systems those days. Cloud computing has gained a lot of attention from academic scientist and business leaders in recent year. Cloud computing architecture reshaped the way we see Information System (IS), envisioned as the future driving computing technology, people started rethinking of the reality of operating systems, client server architectures, and web and mobile browsers. Cloud computing has leveraged end users from computing hardware requirements while reducing overall client-side requirements and complexity.

The evolution of cloud computing dates back to the early 1960s. Concepts like distributed computing and computer utility have emerged to what is known today as cloud computing [27]. Cloud computing in its simplest meaning is a set of computing infrastructure that can be accessed and scaled up or down as needed with minimal modification to the infrastructure itself [2].

Computing virtualization is the key technology in cloud computing as it can reduce the investment in the hardware component drastically. It enables the sharing of the same hardware even virtually dividing the hardware to serve multipurpose [3]. On the other side, the physical network components are not necessarily located on the same geographical area but yet are doing the necessary processing and storage. As such, cloud computing will be the driving force behind most of today's promising computing technologies.

2. LITERATURE REVIEW

The cloud model offers a lot of benefits which to be successfully utilized will need secure systems that protect data, privacy and resources. Security will be always an issue when talking about computing whether it is cloud or traditional one. The only difference is that cloud computing systems are not under your control. Being unaware about security procedures raises new questions and challenges that need to be solved before an enterprise decides to adopt this model. A recent study was done by *International Data Corporation* (IDC - http://www.idc.com/) and *CA Technology* (CA - http://www.ca.com/) on challenges associated with cloud model, security was found to be the number one concern for most of the survey respondents. The results from the surveys are show in Figure 1.

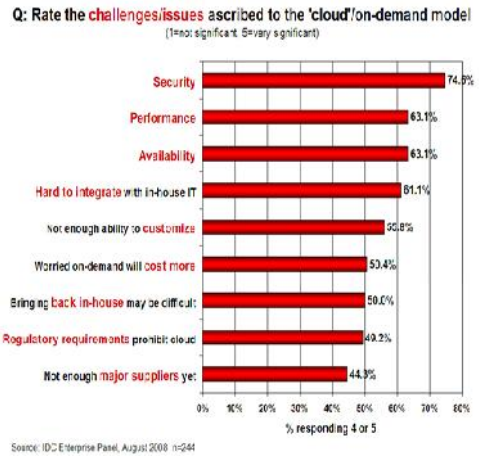

Fig 1a: IDC Survey Results

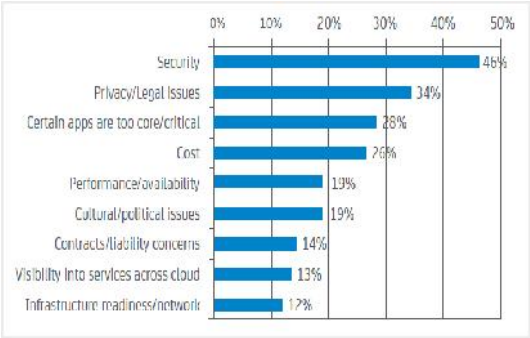

Fig 1b: CA Survey Results

(Source: http://www.ca.com/us/~/media/Files/whitepapers/techinsights-report-cloud-succeeds.pdf)

While the main advantage of cloud model is to provide clients with on-demand resources (as needed), it comes with some security issues as highlighted in Figures 2a and 2b above and also reported in [8]. Figure 2 displays the complexity level in cloud models.

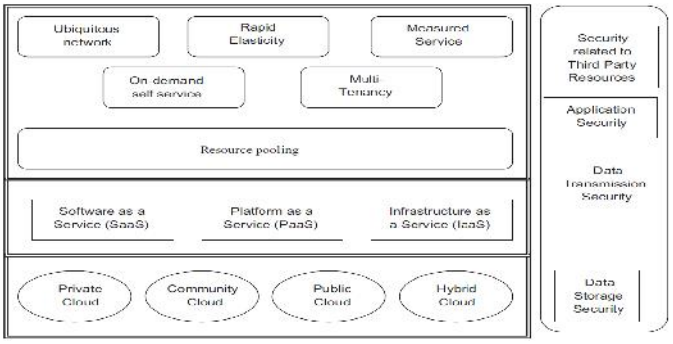

Fig. 2 Cloud Model Security Level and Complexity

In Figure 3, the bottom part differentiates the cloud and hybrid cloud architecture. Above the deployment layer, different representations for the delivery schemes being utilized within each specific deployment architecture. To Name some but not limited to: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) delivery schemes. These schemes together form the heart of the cloud and they mimic specific on-demand self-service characteristics, multi-redundant-tenancy, common networks, measured-service and rapid-elasticity which are shown in the top layer. These basic component of the cloud computing environment calls for security parameters which depend and at the same time varies depending on the deployment scheme in use. Some of the fundamental security challenges are data storage security, data transmission security, application security and security related to third-party resources.

3. KEY CHARACTERISTICS OF CLOUD COMPUTING

The main key components and characteristics of cloud computing have been identified as follows [4,5]:

3.1 Flexibility/Elasticity: users can quickly assign needed computing resources, without human interaction. The computing power and storage can be scaled up or down as required with minimal intervention and in some cases automatically.

3.2 Scalability of infrastructure: with zero or minimal modification to the physical infrastructure, new network-nodes can be added or dropped from the network. As a result, cloud-architecture can be scaled up or down (horizontally or vertically) upon demand.

3.3 Broad network access: making sure that cloud computing services can be made available and can simply and easily accessed by any device (e.g., smart phones, desktops, iPad, and laptops).

3.4 Location independence: what really matters is the service not the physical location. In that sense, the end user shall not worry about the exact location of the computing facility. The service and the location are detached from each other.

3.5 Reliability: is one of the top priorities for businesses. The use of multiple backup redundant webs can enhance the reliability beside disaster recovery plans that ensure business continuity 24/7.

3.6 Economies of scale and cost effectiveness: for cloud computing (regardless of the model being used) to be viable, it needs to be implemented in a large scale. The larger the scale, the lower the cost, and the higher the benefits given that the physical location is being chosen on economical basis.

In any cloud computing environment, security will be always an issue. It needs to be addresses at two different levels: front-end and back-end. By the front-end we mean the physical security of the infrastructure which also include the weakest link human user. On the other hand, the back-end incudes the software side which includes Platform and Infrastructure-as-a-Service via the cloud [6].

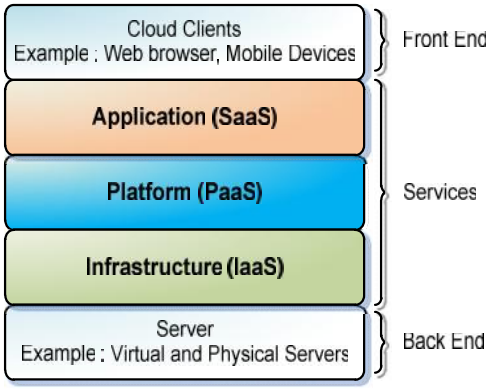

Fig. 3: Cloud Computing represented as a stack of service [7]

As shown in Figure 3, cloud services are offered in terms of Infrastructure-as-a- Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). It follows a bottom-up model in which at the infrastructure-level and computing power is provided as a ratio of CPU to memory consumption allocation. On top of it, lies the layer that delivers an environment in terms of framework for application development, termed as PaaS. At the top level resides the application layer, delivering software outsourced through the Internet, eliminating the need for in-house maintenance of sophisticated software. At the application layer, the end users can utilize software running at a remote site by Application Service Providers (ASPs). Here, customers need not buy and install costly software. They can pay for the usage and their concerns for maintenance are removed [7].

In a nutshell, cloud computing is hugely beneficial for the enterprise and while still evolving, will be around for the long-term. It is crucially important for those enterprises which will adopt the cloud computing model to put long-term security strategy in place. Although economically viable, cloud computing may turn into a very expensive venture for those who neglect to implement and maintain a solid security practice for their virtual environment. It is the time for researchers in this field to get together and think about how to address these issues.

4. FUNDAMENTAL SECURITY CHALLENGES

These issues have been tackled as shown below:

In [9] the main focus was on complex-technical concerns resulting from deploying cloud computing models. I ssues and concerns of the different type of attacks, failures, and risks have been addressed. Four main cloud computing indicators have been identified: 1- basic and frequent core-technology of cloud environments, 2) rooted NIST's intrinsic cloud characteristics, 3) New technologies in cloud environments causing security to go out of control, 4) up to date and modernized cloud systems. In [10] some fundamental security concerns have been addressed like, internal-threats, authentication, mobility, software-security, and hardware-security.

La'Quata Sumter et al. [11] introduced a new concept for a tracking system that will monitor and capture any processing or modification done to the information stored on the cloud. The main concern of the cloud users is to be assured that their data is safe and far from being compromised. The key contribution of this work is the end-to-end cloud security. On the other hand, this concept is not suitable for mega-scale cloud models. Meiko Jensen et al. [12] expanded the concept of cloud-security to include both the web-browsers and web-based services. In order to achieve this, the two concepts need to be integrated into each other. In a similar fashion, M.

Jensen et al. [13] paid special attention to a particular type of DoS attacks on web-based service that uses SYN message-flooding attacks.

Armbust M Fox et al. [14] recommended using virtualization technology to hide the computing resources. The research done by Wayne [15] focuses on both security and privacy issues. Among but not limited to main privacy-security issues are those related to end-user trust, verification & authentication, visibility & viability, risk assessment & management, front-end back-end protection. Similar security issues are explained in Rituik Dubey et al. [16]. Other similar findings are reported in ([17], [18], [19], [20], [21] and [22])

Knowledge of cloud architecture, technology, process, services, and deployment models is vital in specifying security models and identifying security concerns in cloud computing. As the providers and end users increase, standardization and security techniques will play an important role in helping organizations to reduce risks involved.

4.1 Vulnerabilities Identified in Cloud Computing

Recent incidents involving clouds have not helped the perception on cloud's security. This section outlines some recent incidents that shows and explain this issue in the arena of cloud computing. These vulnerabilities range from outages to hacking attempts that inconvenienced end users and organizations using the services. In order establish Cloud Computing reliability as reported in [23], more than 11,000 articles on cloud-computing outages were reviewed between 2008 and 2012. In that period, there were a drastic increase in the number of cloud vulnerability. For example, the number reported incidents doubled over a period of four years. Out of 172 cloud-computing outages, only 129 (75%) were of known cause(s) while the remaining 43 (25%) did not. It was declared and revealed that the most common three threats were insecure interfaces and APIs as 29% of all recorded threats. Followed by data loss and leakage as 25%. And finally, hardware failure as 10%. Together those three threats comprise 64% of all recorded cloud incidents. Upon a thorough and careful review of all reported cloud incidents, over 100 incidents were being grouped together in 8 different threats listed in the Top Threats Report. Close to 50 incidents were not falling in any category. As a result, the author proposes five new different categories to contain and accommodate the remaining incidents namely: hardware failure, natural disasters, cloud service closure, cloud malware, shortcomings of infrastructure design.

It is important to mention that the study only included the reported incidents. A considerable number of incidents went unreported. It is the role of regulators to compel cloud vendors to implement a more transparent reporting policy to make the cloud computing more reliable, trustable, and secure. Incident reporting platform could be a start.

As of now, over 50 online news archives related to cloud computing (1,000 to 10,000 articles) on the different areas of cloud computing. Just Google revealed almost 168,000,000 results on cloud-computing. Google search engine was the top one according to Experian Hitwise [25], the author used it to search for cloud vulnerability incidents. Due to a lack of documented reports on cloud vulnerabilities, all data was based on news published in online news archives and other sources.

4.2 Observation of Cloud Vulnerabilities

129 (75%) of the 172 reported cloud vulnerability incidents declared the cause(s) while 43 (25%) incidents did not. In Figure 4, cloud service providers: Amazon, Google, Microsoft, together accounted for more than 50% of non-transparent incidents of cloud incidents and vulnerabilities. In 2010, Amazon became more open about the causes of their incidents leading the other cloud service providers to be transparent too [26].

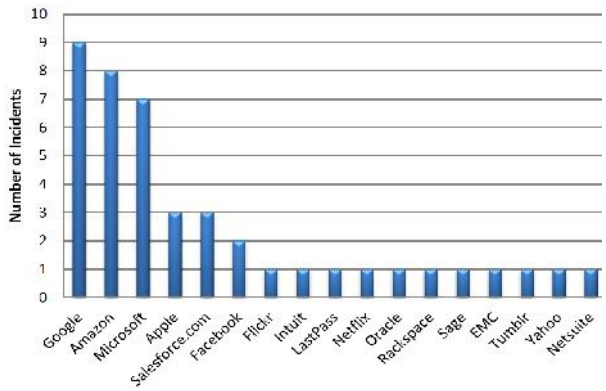

Fig. 4: Cloud break down due to unreported causes

A similar report was published by the *Open Security Foundation*, a non-profit organization providing security information and list of incidents. The incidents are depicted in table 1 below:

Table 1: Cloud Incidents

Type	Date	Organization	What Happened?
Hack	2012-01-21	DreamHost	DreamHost Database Hack Forces Mass Password Reset
outage	2011-04-21	Amazon Web Services	Businesses are totally knocked-out due to amazon-server problems in their data center
outage	2011-04-21	Sony	Play Station Network outages
outage	2011-03-25	Twitter, Inc.	Twitter Experiences Delays in Delivering to Facebook and SMS
outage	2011-03-25	Heroku	Heroku Users Experience HTTP 503 Errors
outage	2011-03-25	Twitter, Inc.	Twitter Experiences Tweet Delivery Delay
outage	2011-03-25	Heroku	Heroku Shared Database Experienced Hardware Failure
outage	2011-03-25	Heroku	Heroku Users Unable to Provision New Dedicated Databases

4.3 Security Analysis from Cloud Service Providers View

CA Technologies provides an executive summary of various surveys conducted over cloud services end-users and cloud-computing providers. It states how IT end-users and cloud computing service providers are addressing the needs to safeguard the data within the cloud. The report presents both the study of cloud computing service providers and the cloud computing end-users. The findings of the study are summarized below:

- The majority of cloud service providers do not have a sense of responsibility towards importance of cloud computing security to protect sensitive data of their users.
- On an average, cloud providers do not confirm or evaluate if their customers' security needs are being met.
- Cloud providers emphasize on cost and time of service deployment rather than focusing on security. This leads to security breaches and vulnerable systems.

5. CONCLUSION & FUTURE WORK

This research evaluates IT user experience and perceptions with regard to security towards existing or new cloud-based solutions by using survey methods. This research determines the IT users' acceptance and risk awareness rate in regard to cloud security. The above survey illustrates the view of cloud providers' actions and assessment of the cloud computing services provided by them to the IT users. Our future research work will carefully analyse some of the major security threats to the cloud services based on the security threat analysis produced by Cloud Security Alliance (CSA) such as:

1. Threat: Abuse and nefarious use of cloud computing.
2. Threat: Insecure application programming interfaces.
3. Threat: Malicious insiders.
4. Threat: Shared technology issues.
5. Threat: Data loss due to leakage.
6. Threat: Accounting of services (Hijacking)
7. Threat: Unknown/unidentified risk.

REFERENCES

[1] K. Stanoevska-Slabeva, T. Wozniak, Grid and Cloud Computing-A Business Perspective on Technology and Applications, Springer-Verlag, Berlin, Heidelberg, 2010.
[2] National Institute of Standards and Technology, The NIST Definition of Cloud Computing, Information Technology Laboratory, 2009.
[3] E. Naone, Technology overview, conjuring clouds, MIT Technology Review, July–August, 2009.

[4] G. Reese, Cloud Application Architectures: Building Applications and Infrastructure in the Cloud, in: Theory in Practice, O'Reilly Media, 2009.
[5] B. Rajkumar, C. Yeo, S. Venugopal, S. Malpani, Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems (2009).
[6] Philip Wik, Thunderclouds: Managing SOA-Cloud Risk,. Service Technology Magazine. 2011-10.
[7] M. Kashif andSellapan P, Security Threats\Attacks present in Cloud Environment,In International Journal of Computer Science and Network Security (IJCSNS) vol 12, No.12,December 2012, pp. 107-114,
[8] A. H. Seccombe, A, Meisel A, Windel A, Mohammed A, Licciardi A,, Security guidance for critical areas of focus in cloud computing, v2.1. CloudSecurityAlliance, 2009, 25 p.
[9] Armbrust ,M. ,Fox, A., Griffth, R., et al "Above the clouds: A Berkeley View of Cloud Computing" , UCB/EECS-2009-28,EECS Department University of California Berkeley, 2009 http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf
[10] Wayne A. Jansen, -Cloud Hooks: Security and Privacy Issues in Cloud Computing‖, 44th Hawaii International Conference on System Sciesnces 2011.
[11] M. Okuhara et al., "Security Architecture for Cloud Computing", www.fujitsu.com/downloads/MAG/vol46-4/paper09.pdf
[12] "A Security Analysis of Cloud Computing" http://cloudcomputing.sys- con.com/node/1203943
[13] "Cloud Security Questions? Here are some answers"http://cloudcomputing.sys-con.com/node/1330353
[14] Cloud Computing and Security –A Natural Match, Trusted Computing Group(TCG) http://www.trustedcomputinggroup.org
[15] "Controlling Data in the Cloud:Outsourcing Computation without outsourcing Control http://www.parc.com/content/attachments/ControllingDataInTheCloud- CCSW-09.pdf
[16] Rituik Dubey et al., "Addressing Security issues in Cloud Computing"http://www.contrib.andrew.cmu.edu/~rdubey/index_files/cloud%20com puting.pdf
[17] M. Okuhara et al., "Security Architecture for Cloud Computing", www.fujitsu.com/downloads/MAG/vol46-4/paper09.pdf
[18] "A Security Analysis of Cloud Computing" http://cloudcomputing.sys- con.com/node/1203943
[19] "Cloud Security Questions? Here are some answers"http://cloudcomputing.sys-con.com/node/1330353
[20] Cloud Computing and Security –A Natural Match, Trusted Computing Group(TCG) http://www.trustedcomputinggroup.org
[21] "Controlling Data in the Cloud:Outsourcing Computation without outsourcing Control http://www.parc.com/content/attachments/ControllingDataInTheCloud- CCSW-09.pdf
[22] "Amazon Web services: Overview of Security processes " September 2008 http://aws.amazon.com
[23] R. K. L. Ko, "Cloud computing in plain English," *ACM Crossroads,* vol. 16 (3), pp. 5-6, 2010.
[24] Cloud Security Alliance. (2010). *Top Threats to Cloud Computing (V1.0).* Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
[25] A. Banks. (2011, 7th April 2012). *Microsoft's Bing regains position as UK's 2nd favourite search engine. YouTube accounts for 1 in every 35 UK Internet visits.* Available: http://www.hitwise.com/uk/press-centre/press-releases/bing-uks-second-favourite-search-engine/
[26] C. Brooks. (2010, 7th April 2012). *IT shops cheer new openness at Amazon following outage.* Available: http://searchcloudcomputing.techtarget.com/news/1507837/IT-shops-cheer-new-openness-at-Amazon-following-outage
[27] Dimitrios Zissis, Dimitrios Lekkas, "Addressing Cloud Computing Security Issues" Future Generation Computer Systems, 28 (2012)583-592.