Security Dynamics of Cloud Computing

Khaled M. Khan
Department of Computer Science and Engineering
Qatar University
Email: k.khan@qu.edu.qa

Abstract

This paper explores various dimensions of cloud computing security. It argues that security concerns of cloud computing need to be addressed from the perspective of individual stakeholder. Security focuses of cloud computing are essentially different in terms of its characteristics and business model. Conventional way of viewing as well as addressing security such as 'bolting-in' on the top of cloud computing may not work well. The paper attempts to portray the security spectrum necessary for enterprizes to understand the dynamics of cloud computing security, the relationships between security requirements of different stakeholders at different levels of abstraction, and the challenges it poses. The paper is expected to shed some lights on concerns as well as dynamics of cloud computing security.

1 Introduction

The main idea of cloud computing has evolved from cluster computing, grid computing, component based composition, and lately, service oriented architecture (SOA) and Web services. In cloud computing, everything is considered service such as hardware, software, CPU power, storage, platform, application software etc. Many leading enterprizes have enough reasons to believe that cloud computing is not mere hype. Main cloud computing providers include Microsofts Azure, GoGrid, Google Apps, XCalibre Communications, Amazon Web Services, Salesforce.com, AppNexus, GridLayer, Mosso and so on. Cloud computing provides a blending of application-deployment speed, fast prototyping capabilities, cost savings, virtually infinite computing power and capacity as well as great unknown and uncertainty about security. It is not entirely a new technology, rather it is a paradigm shift to a new enterprize distributed computing. Cloud computing is considered a computing paradigm shift from mainframe computers to cloud computing over the past decades [7].

Cloud computing is expected to provide an illusion of simplicity and convenience to the enterprizes. If an enterprize needs more storage space, more CPU power, intensive computation and high volume of data processing, or a couple of database servers, cloud computing can provide these capabilities without the enterprize having to install new servers, buy powerful computer with huge storage capacity, and of course the related application software [3]. When the enterprize no longer needs those extra capacity and computing power, it can decide to discontinue the services at any time, and switch it off. The question is: does it that simple? Not really, as long as its security is concerned. The complexities and security concerns of services delivered by cloud computing are not entirely negligible. There is no shortage of published literature on the benefits that the cloud computing could bring to enterprizes. One can easily find plenty of materials explaining what a cloud computing is and its numerous benefits. On the contrary, whenever someone wanders to find out any real insights of security issues of this paradigm, there are hardly many. There are two possible explanations for this. Firstly, many probably think that the cloud

computing security is not much different than existing security practices, therefore nothing to worry about. Secondly, we are not sure yet about the actual security concerns that need to be tackled in cloud computing. This paper attempts to explore these.

Most cloud providers try to satisfy potential cloud consumers by stating that they use SSL for all communications to protect network traffic, they use encryption, they designed trusted virtual domains, cloud specific access control technology in place in their cloud domains, etc. The main concerns of CIOs are possibly more than technological issue of traditional security and threats of cloud computing. Their central worries include possible data breaches, accidental intermixing of their data assets with other consumers of the cloud provider, great uncertainty about data privacy and vulnerability issues, and lack of control on their data assets while these residing in third-party hardware-software infrastructure. These concerns are partly due to the unique characteristics of cloud computing and the great unknown about its security issues. Cloud computing themselves unlikely cause the security problems as most of us are too worried about. Security issues of cloud computing are not the technology, rather it is the issue of reliability, confidence, lack of clear and enough information about cloud security.

In order to understand the right issues in cloud computing security, we need to understand the entire spectrum of its stakeholders and their security concerns. Sensitive data processed by a third party in a remote machine as well application would undoubtedly introduce inherent level of security risk, because such third party services may take away the very controls of cloud computing consumers on their data assets. Cloud consumers may demand transparency such as detailed information on security functions and assurances provided by cloud computing providers. In general, a cloud computing consumer can believe that the password based security is reasonably protecting her desktop browser. However, when her application is using a cloud service, browser security becomes a critical organizational security factor [6]. A consumer may like to know where her data is stored, who owns and control the sites, what data manipulation accesses are available to third party employees, any audit trail is available, how to invoke the data manipulation access remotely and so on [1].

Cloud computing security is increasingly getting importance. As a result, National Institute of Standards and Technology (NIST) has announced to create a Cloud Computing Security Group. The group is to oversee the cloud computing security issue, securing cloud infrastructure, security cloud applications, enabling forensics in the cloud, security monitoring in a cloud, security compliances etc. The usual practice of putting a mere security tag such as ‘secure’ on the cloud computing marketing slogan does not help much to boost cloud consumers confidence in the cloud computing. The term ‘secure’ is over used and somehow misleading because it does not state the specific type of security ensured.

This paper makes an attempt to unfold the specific security problems that cloud computing suffers from. In order to understand the security dynamics of this issue, section 2 identifies various levels of abstractions in cloud computing and their associated stakeholders. Section 3 discusses security concerns of each stakeholder group, and maps out the existing security practices. Section 4 outlines the challenges to address the security issues identified in section 3. Finally, section 5 closes with some concluding remarks.

2 Cloud stakeholders

Cloud computing can have various types of stakeholder at different levels of its abstraction. We can identify three different levels of abstraction in cloud computing: *cloud infrastructure providers*, *cloud service providers*, and *cloud consumers*. At the back-end, the cloud infrastructure providers typically own and manage cloud computing resources such as hardware, networks, systems software etc. Cloud service providers serve the front-end cloud consumers by offering services such as on-demand computing, utility computing, data processing, software services and platform for developing application software. Cloud consumers at the front-end of cloud computing can be classified into two major groups: (i) *end-users* who use on-demand computing, software services as well as utility services; and (ii) *application developers* who need software development platform as well as hardware software infrastructure to construct software on the fly. This classification represents entire cloud computing into three levels of abstraction with four different major stakeholders as depicted in Fig. 1.

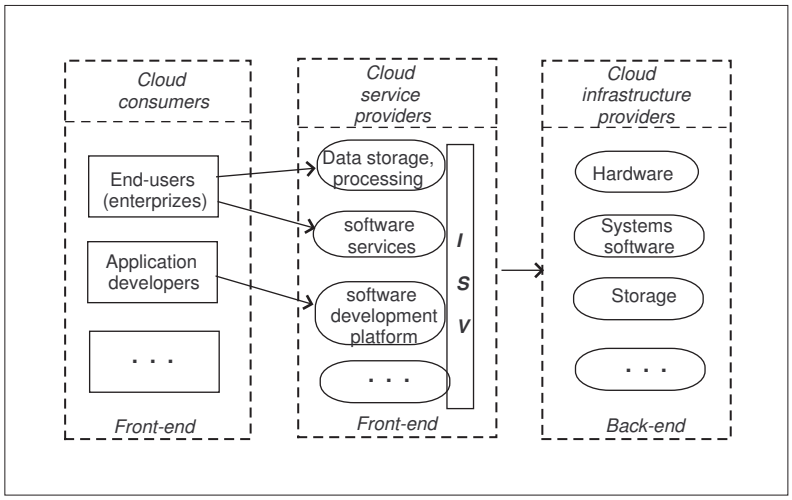

Figure 1. Three Levels of Abstractions and Stakeholders of Cloud Computing

- At the back-end of cloud computing, *cloud infrastructure providers* own, manage, and maintain hardware and systems software required for generating the cloud computing power. The infrastructure is based on Internet-connected servers, storage, virtualization, grid of distributed servers, multiple blade servers, APIs with Web services, XML-based protocols to connect users over the Internet, multiple nodes of processor etc. Amazon, IBM, Sun Microsystem offer infrastructure supports such as storage, processors, and virtual servers. IBM's Research Compute Cloud provides an on-demand globally accessible set of computing resources which are distributed across its several labs.

- At the front-end of cloud computing, *cloud service providers* offer services such as high volume computation, virus scanning, anti-spam services, desktop management services, email services, databases, software development platform, and data storage. Providers are the ISVs who offer various computing services directly to cloud consumers. For services, cloud service providers use software running on hardware-software resources managed by back-end cloud infrastructure providers. Companies like Salesforce.com, Amazon.com, and Google have developed various on-demand services to enterprizes. A cloud provider could also play the role of cloud infrastructure. Everything goes on behind the scenes of the services such as the server, operating system, the programming language services, software tools, utility programs used are abstracted away from the cloud consumers.

- *End-users* are the front-end stakeholders of the service level abstraction. They consume services provided by cloud service and infrastructure providers. End-users usually use Web browsers or other user interface software to access cloud services. The services include from data storage to high volume computation. End-users use the services and 'pay as they go'. The business enterprizes or corporations are the main end-users of cloud services.

- *Application developers* can build software on the fly without investing in additional software and hardware devices. A large scale application software sometimes needs to increase its computing capacity or add more functionalities. Cloud infrastructure providers offer real-time computing resources, and cloud service providers offer development environment as a service over the Internet to cloud application developers who do not control the development infrastructure. The vendors provide the platform, the application developers decide what development tools such as compiler, libraries, components, hardware will be used for their applications. Examples of this type of application development platforms include Sun Grid, Amazon Elastic Compute Cloud (EC2), Salesforce.com's Force.com, GRIDS Lab, Aneka, Coghead, Google App Engine, Yahoo Pipes, Dapper.net etc. The idea behind platform as a service is that resources

are made available for building whole applications as components, rather than programs to be written. Widgets, web editors, pre-built shopping carts, whatever pieces application developers need could be offered by a single ISV for the application developer to match and compose at will.

Cloud computing potentially raises various types of security concerns at different levels of abstraction to different stakeholders as discussed in the next section.

3 Cloud Computing Security

Security of cloud computing can be viewed through numerous lenses. One of the leses is the perspective of stakeholders. Each of the stakeholders has its own security concerns and objectives. These security objectives are associated with specific services that they provide or consume. We note that a cloud is not a single entity, it can consist of one or more open clouds, internal clouds or external clouds. There is no doubt that new security risks arise from the communication that goes on between cloud consumers and cloud providers; and between cloud providers and cloud infrastructure providers. The cloud security promotes de-perimeterization of the enterprize data security boundary, and extends it to greater mobility and collaboration with third party enterprizes [2]. In order to understand this phenomena as well as the cloud computing security concerns, consider the following three scenarios.

1. **Scenario 1**: A medical practitioner $MediScan$, a cloud end-user, consumes computing services offered by a cloud service provider $CloudX$. The service is to process the patients' digital medical images such as CT scan, MRI, ultrasound. The confidentiality and integrity of images are very important for $MediScan$, but are beyond its control, rather $CloudX$ is responsible for all these. It goes further. The huge volume of images are finally stored in several physical storage facilities owned and managed by a cloud infrastructure provider $CloudBon$. $MediScan$ likes to know from $CloudX$ about its specific security concerns: How (i) *confidentiality* of images is kept, (ii) *integrity* is preserved, and (iii) *to control read-write access of others to its data*. How these are ensured at different levels of abstraction in relation to the service it consumes from $CloudX$.

2. **Scenario 2**: A second cloud end-user, a media company $NewsMedia$, uses the same cloud service provider $CloudX$'s computing services to process various images such as news clips and pictures of its clients. The confidentiality of the images is not important for $NewsMedia$ because all images are publicly available. However, the integrity of images is very important for $NewsMedia$ but beyond its control, rather $CloudX$ is responsible for protecting the images. $CloudX$ stores some of the images in the devices owned and managed by the cloud infrastructure provider $CloudBon$. $NewsMedia$ does not care who can see and copy its images, but it wants to know from $CloudX$ about its specific security requirements: How (i) *integrity* of its images is preserved; (ii) *authentication* of $CloudX$ is maintained, and (iii) *non-repudiation* is ensured for all communications between $NewsMedia$ and $CloudX$. In other words, the images should not be allowed to be tampered or modified by any unauthorized entities (integrity), and $CloudX$ cannot deny later that it did not perform the operation to $CloudX$ (non repudiation).

3. **Scenario 3**: $SofTech$, an application developer, uses software development platform offered by $CloudX$. $SofTech$ basically composes software with some of its existing software components, new components and utilities provided by $CloudX$. The main two concerns of $SofTech$ are: (i) how the *security requirements of its application software are complied* with the security assurances of the new components and utilities available from $CloudX$'s platform. It also likes to know how the security properties of its existing software components are supported by the security provisions offered by $CloudX$; (ii) what are the *assurances* that the claimed security of the software components and utilities provided by $CloudX$ will always hold; and (iii) an assurance that the software components do not have problems of *information leakage* and *buffer overflows*.

Fig. 2 shows these scenarios with the security objectives of the stakeholders. In the following sub-sections, we discuss the main security concerns of each stakeholder in these three scenarios.

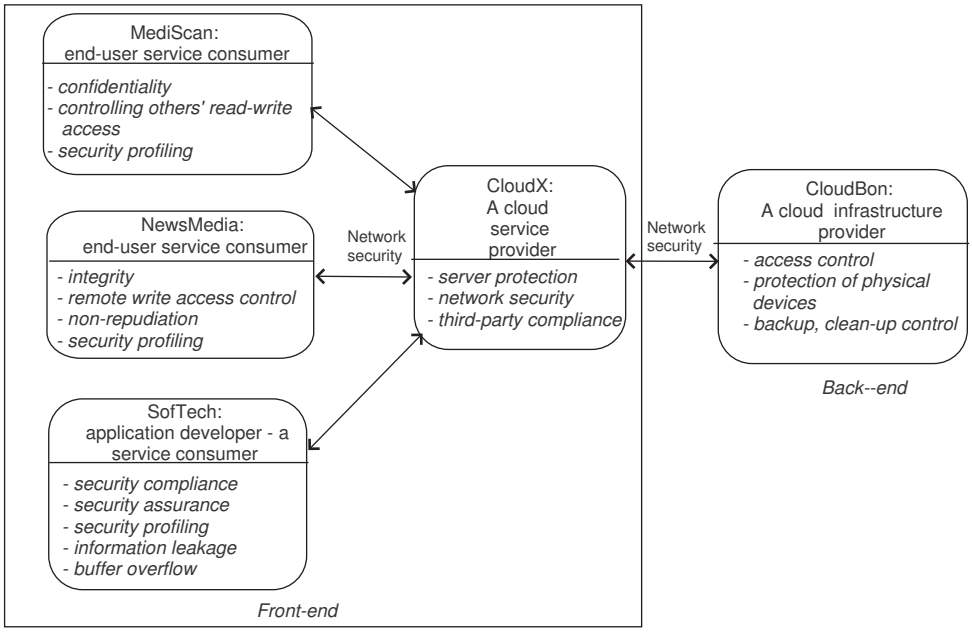

Figure 2. Security objectives of different stakeholders

3.1 Security concerns of end-users

The scenarios suggest that the main security concerns of the stakeholder $MediScan$ are confidentiality, lose of control on their digital images, and unknown security profiles of third part providers such as $CloudX$ and $CloudBon$. $MediScan$ sees that its images are hosted and stored on someone else like $CloudX$'s servers and $CloudBon$'s hardware-software infrastructure. It finds losing its control over its data assets. $MediScan$ has also no control to check the security assurances a prior to the service of $CloudX$ and $CloudBon$. The problem is compounded with the fact that the service adds additional communication links in the chain, that is, $CloudBon$ in this case. This third party inclusion in the service introduces an additional vectors of attack [4]. This additional link includes entrusting third party such as $CloudBon$ in the chain. The $MediScan$'s data are not only transmitted to $CloudX$, and further to $CloudBon$, rather they are persistently stored there. In such cases, data might not be adequately protected while they are being moved within the systems or across multiple sites owned by multiple ISVs [5]. $MediScan$ and $NewsMedia$ may wonder: are data persistently encrypted, or only encrypted while being moved over the network? How to control the access of others to their own data? How to manage the images split across multiple third party ISV providers?

In first two scenarios, we can find that two different end-users namely $MediScan$ and $NewsMedia$ have two different sets of security requirements for the same service offered by the same cloud service provider $CloudX$. It signifies the fact that in cloud computing one security does not fit all. This scenario also suggests that the security assurances associated with a cloud service could be customized according to the needs of the consumers. At the lowest level of the abstraction, these requirements are to be complied such as cloud infrastructure provider should synchronize and ensure the different sets of security requirements surfaced at the front-end level of cloud computing. Similarly, the application software must support various security needs requested for the same cloud service. $MediScan$ and $NewsMedia$ need to be ensured by $CloudX$

that $CloudBon$ provides same level of security standards as $CloudX$.

3.2 Security concerns of application developer

The cloud application developer $SofTech$ is more interested in the compositional impact and conformity of security properties of their application running on infrastructure managed by $CloudBon$. $SofTech$ should know specific security assurances provided by $CloudX$ and $CloudBon$. In a highly fluid distributed environment such as cloud computing, $SofTech$ develops applications on platform and infrastructure provided by $CloudX$ and $CloudBon$ respectively of which they have only partial or no knowledge about the underlying security properties. Their concerns may include: does the application software built on the $SofTech$'s platform somehow leaks information to other devices? How is the buffer overflow controlled? How is the security policies defined by the $CloudX$ and $CloudBon$ preserved and honored at the application level?

3.3 Security concerns of cloud service provider

The cloud service provider $CloudX$'s main concern of safeguarding the $MediScan$'s and $NewsMedia$'s data is transferring images from devices and servers within the control of $MediScan$ and $NewsMedia$ to its devices, and subsequently images stored in $CloudBon$. It requires $CloudX$ a kind of remote management of $MediScan$'s images and ensuring security. Images stored in cloud provider $CloudX$'s devices are not located on a single machine, rather, these are saved across the entire virtual layer. The data are also hosted on devices that belong to third party ISV $CloudBon$. $CloudX$ needs to ensure its consumers $MediScan$ and $NewsMedia$ on how the security issues of images are addressed between the partners: does $CloudBon$ ensure similar level of security of $CloudX$? How is the clean-up of outdated images managed at its site and the site of $CloudBon$?

3.4 Security concerns of cloud infrastructure provider

For $CloudBon$, the cloud infrastructure provider, the security concerns are undoubtedly not less than $MediScan$, $NewsMedia$, or $CloudX$. $CloudBon$ knows that a single point of failure in its infrastructure security mechanisms would let the hackers take out thousands of images owned by $MediScan$ and $NewsMedia$, probably also images owned by other enterprizes. Their concerns are: how are the data stored in its physical devices protected? How is the backup of images managed, cleaned up, and controlled at its site? How to ensure the access control to the physical devices and images stored on its devices?

4 Cloud computing challenges

The existing security technologies can take care of most of the security concerns unfolded in the previous section.

- *Network security*: The communication between $MediScan$ and $CloudX$ should be secure. The current security technology provides plenty of security protocols and provisions for network security. There is no new or unique network security problem in cloud computing in this case.
- *Confidentiality and integrity*: Encrypting a data file before it's sent to cloud computing services can secure the images of $MediScan$ and $NewsMedia$. The existing security techniques can scramble the image file such a way that it can only be accessed with a password. However, encrypted images can only be accessed by the user –regardless of where the file is stored. The stored images could be protected by using encryption. A cloud provider can protect data in transit by encrypting it in the pipe between the provider and the service consumers system.
- *Non-repudiation and authenticity*: These security aspects can be well managed with existing techniques such as digital signature, PKI, encryption etc.

Encryption, digital signature, network security, all are important for cloud computing, but these won't make cloud computing more reliable to the consumers. It needs something more in addition to conventional security mechanisms. Cloud consumers may wonder: what is the actual problem in cloud computing security when the network is secure, the password appears to be working, the encryption is working, and keys seem to be strong? The answer to this question probably lies with some new technical as well as some non-technical challenges of cloud security.

4.1 Technical challenges

The technical issues include non-disclosing specific security assurances of a service as opposed to claiming 'secure' service, lack of control of data owner, and absence of security compliances between service level functions of service consumers and cloud providers. A lack of control on data assets triggers the issue of confidence and reliability. The following specific technical challenges need to be addressed in order to make cloud computing viable to consumers:

- Security profiling of services which could be available to end-users and verifiable.
- Consumers have the capability of controlling others' access to data remotely irrespective of locations and systems. Consumers like to have fine grained access control on their own data irrespective where its data assets are located and processed.
- Security compliances between consumers systems and cloud providers systems, and
- Security assurances of software-hardware as claimed, better certification is to be provided.

Our further work on this paper is expected to address the above four challenges in near future.

4.2 Non-technical challenges

The three scenarios also suggest that in addition to these technical challenges, the cloud computing probably is to address some non-technical aspects of the identified security concerns, mostly the psychological one. The great unknown about cloud security and its service dynamics are the driving instrument for the psychological issue of uncertainty and confidence problem in cloud computing. In security field, it is known that to make a data asset secure, one must separate the asset from the threat. On the contrary, data assets are taken closer to their threats in cloud computing because the assets are transmitted to, stored, and manipulated in remote devices by third parties, not by the owner of the data asset. When a cloud computing consumer finds that she does not have clear idea in where her enterprize data is processed, how her persistent as well as transient data are protected while being processed, transmitted and stored by machines controlled by others not related to her enterprize, she has valid reason to be concerned about cloud computing. By computer security definition, a remote location not controlled by the asset owner may usually be associated with multiple threat scenarios. This is one of the reasons for why the psychological aspect of cloud security is so strong among the cloud consumers. The end-users license agreement (EULA) or some privacy policies may not solve this psychological issue.

In this brief discussion we can see that no one-size security fits for all stakeholders. The security requirements of cloud consumers need to be ensured by the cloud provider's security assurances. Similarly, the cloud providers' security promises to consumers must be guaranteed by the infrastructure providers. The security requirements of four different stakeholders of cloud computing are interdependent and need to be integrated in a business model.

5 Conclusion

Cloud computing provides consumers the choices of software, hardware, and computing environment. This choice provision could be extended further to include security assurances. The ultimate cost for a service could be well based on the

choice of service as well as the choice of security assurances. In order to mature the cloud services, service level agreement (SLA) needs to specify the preferred specific security assurances in details. The security concerns of cloud computing are very much based on consumers' concerns. The characteristics of cloud computing security are somehow different than the conventional software systems in several ways. In this new design paradigm, change of mind is crucial because data belongs to end-users, therefore, they need to control it. Nowadays, cloud consumers are more security-aware than before. They make the service consuming decision not only on cost and functionality of the service, but they like to see the real credible security that cloud providers ensure. Cloud consumers may demand the proof of security assurance and certificate of the services before they lock in any deal in cloud services. Generally speaking, it is somehow unrealistic to tell cloud consumers whether a cloud system is secure or not; it is better to expose the security profiles of specific service to them. Based on this, end-users could map out which tasks could be consigned to the cloud and which should be kept under their control. This decision could be made based on the value of their data assets and the risks involved in cloud computing. Our repeated experiences suggest that just relying on security claims made by cloud providers, such as *secure cloud*, may not be very appealing to all cloud consumers. A blanket security assurance may not satisfy all types of cloud stakeholders. We need to do more to attain and sustain the consumers' confidence in cloud computing.

References

[1] Balding, Craig. "Security in the Cloud: Introducing Cloud Mashups", Cloud Security, 2008. http://cloudsecurity.org/2008/04/21

[2] Condon, Ron. "Cloud computing security framework due", Information Security Magazine, TechTarget IT Media, March 2009

[3] Erdogmus, Hakan. "Cloud Computing: Does Nirvana Hide behind the Nebula?", IEEE Software, March/April 2009, pp. 4-6.

[4] Greenberg, Andy. "Cloud Computing's Stormy Side", Forbes, February, 2008.

[5] Leavitt, Neal. "Is Cloud Computing Really Ready for Prime Time?", IEEE Computer, January 2009, pp. 15-20.

[6] Mills, Elinor. "Payment processor Heartland reports breach", CNET News, Security, January 2009.

[7] Voas, Jeffrey and Zhang, Jia. "Cloud Computing: New Wine or Just a new Bottle?", IEEE IT Professional, March/April 2009, pp. 15-17.

About the author: *Khaled M. Khan has been serving the department of computer science and engineering at Qatar University since 2006. He also holds an honorary Adjunct Fellow position in the School of Computing and Mathematics at the University of Western Sydney, Australia. Prior to these, Khaled served University of Western Sydney for seven years as an academic in computing. He held the position of head of programs for the postgraduate programs several years at the University of Western Sydney. He taught computing last twenty years at various universities in Asia, Europe, Africa and Australia. He received his PhD in computing from Monash University and a BS and an MS in computer science and informatics from the University of Trondheim, Norway. He also holds a second bachelors degree from the University of Dhaka. Khaled has published more than 50 refereed papers, and two books. He could be contacted at: k.khan@qu.edu.qa*