State of the Art of Network Security Perspectives in Cloud Computing

Tae Hwan Oh[1], Shinyoung Lim[2], Young B.Choi[3],
Kwang-Roh Park[4], Heejo Lee[5], and Hyunsang Choi[5]

[1] Dept. of Networking, Security and Systems Adminstration
Rochester Institute of Technology
Rochester, NY, 14623 U.S.A
[2] Dept. of Rehab Sci & Tech
University of Pittsburgh
Pittsburgh, PA, 15260 U.S.A
[3] Dept. of Natural Science, Mathematics and Technology
Regent University
Virginia Beach, Virginia, 23464 U.S.A
[4] Electronics and Telecommunication Research Institute (ETRI)
138 Gajeongno, Yuseong-gu, Daejeon, 305-700
Rep. of Korea
[5] Korea University
Anam-dong Seongbuk-gu, Seoul, 136-701
Rep. of Korea

Abstract. Cloud computing is now regarded as one of social phenomenon that satisfy customers' needs. It is possible that the customers' needs and the primary principle of economy – gain maximum benefits from minimum investment – reflects realization of cloud computing. We are living in the connected society with flood of information and without connected computers to the Internet, our activities and work of daily living will be impossible. Cloud computing is able to provide customers with custom-tailored features of application software and user's environment based on the customer's needs by adopting on-demand outsourcing of computing resources through the Internet. It also provides cloud computing users with high-end computing power and expensive application software package, and accordingly the users will access their data and the application software where they are located at the remote system. As the cloud computing system is connected to the Internet, network security issues of cloud computing are considered as mandatory prior to real world service. In this paper, survey and issues on the network security in cloud computing are discussed from the perspective of real world service environments.

Keywords: Cloud computing, cloud security guidance, network security, risk analysis.

1 Introduction

When Google's Christophe Bisciglia proposed concept of cloud computing in 2006 [1], it has to wait until 2008 for most global enterprises' recognition of cloud

T.-h. Kim, A. Stoica, and R.-S. Chang (Eds.): SUComS 2010, CCIS 78, pp. 629–637, 2010.

computing as one of futuristic business services. Cloud computing provides customers with service in the form of virtualized computing resources [2][3]. Customers are able to acquire computing resources (i.e., software, storage, server, and network) based on their demands. Available cloud services are Software as a Service (SaaS) [4], Platform as a Service (PaaS) [5], and Infrastructure as a Service (IaaS) [6]. SaaS focuses on multiple leases of application software packages, PaaS focuses on providing software developer's environment, and IaaS focuses on providing service infrastructure such as storage or computing power over the Internet.

Although there are problems with the cloud security issues, there are a number of security benefits that comes with cloud computing. All security measures are cheaper if they are implemented on a large scale. Customers of cloud computing have security as their primary concern, and thus as the cloud provider provides more security, they will be more acceptable to customers as preferred suppliers. Large cloud providers are able to offer standardized interfaces for managing the clouds; this can help reduce the migration time, and also identifies certain problems. Having all the data on the same place is dangerous as it could be a single point of failure, but on the other hand, if all the data is on the same place this means it will be easier for monitoring. Cloud providers provide algorithms for hashes and checksums for saving files, thus any incident happens will produce a backup copy and will be provided instantly. You may have unaware of doing it yourself. Most companies (especially small ones) do not have a 24/7 or they can't provide them. Security advantages that come from virtualization also apply to cloud computing.

In this paper, we focus on network security perspectives in cloud computing. Section 2 discusses related work of technical aspects and commercially available cloud computing service, section 3, security threats of cloud computing, section 4, status of cloud computing security, and section 5, network security for cloud computing are discussed followed by conclusion in section 6.

2 Related Work

In this section, topics on deployment models of cloud computing and commercially available cloud computing are discussed to find out system architecture without or less security features.

2.1 Deployment Models of Cloud Computing

We can categorize clouds based on their visibility as follows: Public clouds, private clouds, hybrid clouds, and community cloud based on its customers and service policy.

Clouds have a five following unique characteristics.

Multi-tenancy (shared resources): In cloud computing environment, multiple users use the same resources in which resources are shared in network level, host level and application level, rather than dedicate to single host to server.

Massive scalability: Cloud computing provides the ability to scale thousands of systems, bandwidth and storage space.

Elasticity: The cloud computing provides the ability to increase or decrease their computing resource by their needs.

Pay as you go: This feature is to provide the user to pay for actual resource for their usage, which depends upon computing power, bandwidth and storage use.

Self–provisioning of resources: Having additional resources, like processing capability, software, storage network resources.

2.2 Commercially Available Cloud Computing Services

Currently there are a few companies that provide cloud computing services: Amazon, Google, Microsoft, Sales-force.com, IBM, HP, and VMware. In this paper, we summarize cloud computing services of Amazon and Google.

Amazon, known as one of world's largest online sellers, has the Internet online sale regarded as cloud services. Amazon provides cloud services in S3 and EC2 [7][8]. S3 stands for Simple Storage Services and users can access storage in stored objects in S3 from any place in the internet. EC2 is Elastic Computer Cloud. It's a virtual infrastructure that is able to run a lot of applications from web-hosting, emails, all the way to simulations. The control over the data is in the user's hands. Users can create their own virtual image to include customizable features such as OS, security and network access controls, and API. Some of their main security issues currently include availability. Another issue is the threat of attackers to leverage Amazon and their processors to a level that will be hard for detection (for example using multiple servers as a super computer to brute force encryption attack).

Google's App Engine (GAE) is the companies cloud services [9][10]. They give users possibility to build their own virtual application to run on web applications in either Java or Python. Resources used by applications are free up to 500MB in addition to the bandwidth. In Google's GAE, customers will not get any privileges as opposite to Amazon's services. Google's core business is in the cloud; all of its services like search, emails, online mapping, office productivity, and social networking are available in the clouds. Users can subscribe to those services for free or pay a little for more services and support. Google's Electronic Privacy Information Center (EPIC) has filed a complaint for the FTC about security standards in Google's Cloud computing services.

3 Security Threats in Cloud Computing

Among the requirements of disseminating the cloud computing services, acquiring reliability, availability, and compatibility are in active discussion in the community. As the cloud computing has different type of system architectural models and service models, the security risks are also different from other models. Cloud computing is about gracefully losing control while maintaining accountability even if the operational responsibility falls upon one or more third parties. But even though, as clouds do have benefits, they still have security concerns that need to be addressed. Some of security topics are being discussed by Gartner, European Network and Information Security Agency (ENISA) [14], and Cloud Security Alliance (CSA) [11].

Gartner announced seven cloud-computing security risks [19] and ENISA also announced 10 security risk assessments [20]. Gartner pointed out seven security risks in cloud computing as follows:

1. Privileged user access: Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the 'physical, logical and personnel controls' IT shops exert over in-house programs. Get as much information as you can about the people who manage your data. As providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access, customers should know as much as they know about how is their data being processed and handled so sensitive data should not be exposed to un-privileged users.

2. Regulatory compliance: Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are signaling that customers can only use them for the most trivial functions. It is also necessary for the customers to pay precautious attention to the terms and conditions that service providers should give the services of customer compliance according to their policies.

3. Data location: Service provider will be responsible for storing sensitive data and whole process for customer but the customer or client not aware of process are running and where the data are stored. Cloud service providers might commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers. Customer should inquiry the service provider about commitment for protects their sensitive data on behalf the customer and should obey their policies.

4. Data segregation: Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. It should find out what is done to segregate data at rest. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists. Encryption accidents can make data totally unusable, and even normal encryption can complicate availability.

5. Recovery in the case of disaster: Even if customers do not know where their data is, a cloud provider should tell the customers what will happen to their data and service in case of a disaster. Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure. Customers should ask their provider if it has the ability of a complete restoration, and how long it will take.

6. Investigative support: Investigating inappropriate or illegal activity should be impossible in cloud computing if these investigation or activities are against of user service and policy. Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If customers are unable to get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then their safe assumption is that investigation and discovery requests will be impossible.

7. Long-term viability: Ideally, cloud computing provider will never go broke or get acquired and swallowed up by a larger organization. But customers must be sure their data will remain available even after such an event. It is required to make an inquiry to the potential providers how customers would get their data back and if it would be in a format that the customers could import into a replacement application.

The ENSIA security risk assessments are summarized as follows: When in using cloud infrastructures, the client necessarily cedes control to the Cloud Provider, thus leaving a gap in security defenses. There are no standards those are available so, it will be hard for customers to migrate data between providers as well moving them back to in-house IT departments. This risk category covers the failure of mechanisms separating storage, memory, routing between different tenants. However, the attacks on resource isolation mechanisms are much more difficult for an attacker compared on traditional operating systems. An investment in achieving certification or certain compliance regulations may be put at stake due to migration to the cloud, and sometimes the use of a public cloud infrastructure implies that certain kinds of compliance cannot be achieved. Customer management interfaces of a public cloud provider are doing so using the internet, and thus this is a more risk as it's publically available. It can be difficult for the customer to check the data handling correctly, and thus if it's a lawful way or not. As customers may not be sure of the way the cloud providers get rid of the data, this can be a security risk if they are not deleted in a lawful manner.

4 Improving of Cloud Computing Security

To improve security in cloud computing, companies and academia joined together and formed several groups and alliances to address the security issues for cloud computing.

The common goals for those groups and alliances are to enhance and improve security for cloud computing through education and by encouraging the use of best practices for providing security for clouding computing. The following list describes the different security organization for cloud computing.

Cloud Security Alliance (CSA): This is a non-profit organization and promotes best practices of security assurance for clouding computing. Also, this alliance allocates resources for awareness campaigns and education programs to encourage appropriate use clouding computing security solutions. Additionally, strong research activities are encouraged as well [11].

Open Cloud Consortium (OCC): This consortium supports standard development for cloud computing as well as framework development to address interoperable between different clouds. Additionally, the bench marks for cloud computing are supported as well as the reference implementations. Lastly, the consortium sponsors events that related to cloud computing [12].

Storage Networking Industry Association (SNIA): This non-profit organization assists members to store and manage large amount of information. This is important for cloud computing to address the storage issues including the security issues related to storage [13].

European Network and Information Security Agency (ENISA)**:** This organization is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard for information on good practices. The ENISA has presented few recommendations for providing security in the clouds and the cloud customers need assurance that providers are providing good security practices for cloud computing [14]. Therefore, following action items are check to ensure the security between the customers and providers.

- Assess the risk of adopting cloud services
- Compare different cloud provider offerings
- Obtain assurance from selected cloud providers
- Reduce the assurance burden on cloud providers.

National Institute for Standards and Technology (NIST):
NIST mission is promoting technical guidance and standards to provide effective and secure use of cloud computing technology. NIST wants to promote cloud security standards by proposing roadmaps for needed standard as well as catalysts to help industry to formulate their own standards. Also, NIST encourage government and industry to adopt the cloud standards [15]. The goals of NIST Cloud standards are fungible clouds that have following features:

- Mutual substitution of services
- Data and customer application portability
- Common interfaces, semantics, programming models
- Federated security services
- Vendors compete on effective implementations

Also, enable and foster values add on services for advanced technology and vendors compete on innovative capabilities.

5 Network Security for Cloud Computing

There are some recommend priority areas of research to improve the security of cloud computing. The following are the categories being considered [16]:

Building Trust in the Cloud

- Effects of different forms of breach reporting on security
- End-to-end data confidentiality in the cloud and beyond
- Higher assurance clouds, virtual private clouds etc

Data protection in large scale cross-organizational systems

- Forensics and evidence gathering mechanisms.
- Incident handling - monitoring and traceability
- International differences in relevant regulations including data protection and privacy

Large scale computer systems engineering:

- Resource isolation mechanisms, data, processing, memory, logs etc
- Interoperability between cloud providers
- Resilience of cloud computing

The Open Cloud Consortium (OCC) [12] is a group formed by universities and IT companies looking to investigate new ways of improving computing and storage costs across various cloud platforms and integrate communication standards among different providers. This is a relatively new group formed in the mid-2008, which confirms the novelty of the field. The OCC has undertaken the following goals:

- Development of standards for cloud computing and frameworks for interoperating between clouds
- Develop benchmarks for cloud computing
- Support reference implementations for cloud computing, preferably open source reference implementations.
- Manage a test bed for cloud computing - the Open Cloud Testbed
- Sponsor workshops and other events related to cloud computing

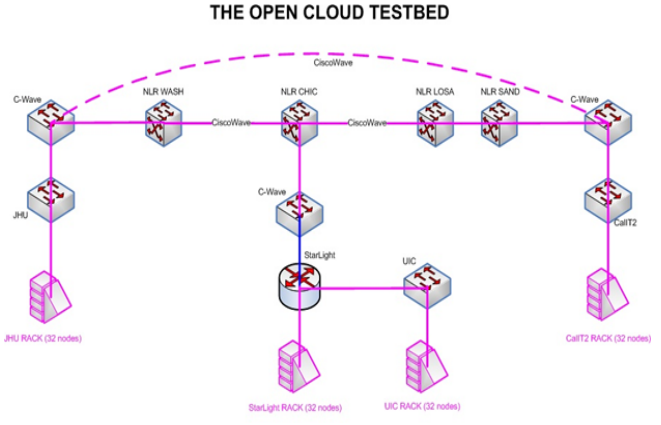

Fig. 1. OCC Network Testbed

The architecture in the Figure 1 above shows the OCC network and the connection among server racks at University of Illinois at Chicago, StarLight in Chicago, Calit2 in La Jolla and John Hopkins University in Baltimore to the switches, routers and wide area routers in between [12]. Using the aforementioned architecture, the OCC published has worked towards implementing high traffic flow design and protocols among several locations [12]."

According to the 'Security Guidance for Critical Areas of Focus in Cloud Computing V2.1' published by Cloud Security Alliance (CSA) in December 2009,

CSA focused on operating in the cloud and identified the following as the factors to consider in network security aspects in cloud computing [17]:

- 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
- Virtualization

Another view about the network security aspects in cloud computing can be found in the research performed by RSA on the role of security in trustworthy cloud computing. First, they identified the challenges of the cloud security and found that security is the big question mark because of the factors such as changing relationships, standards, portability between public clouds, confidentiality and privacy, viable access controls, compliance, and security service levels. Bay analyzing those factors RSA suggested the three principles for securing the cloud computing as 1) Identity security, 2) information security, and 3) infrastructure security [18].

6 Conclusion

To satisfy increasing needs of customers' about security in cloud computing, it is important to identify the outstanding issues, existing technologies, and future directions of network security in cloud computing.

In this paper, we surveyed the state of the art of network security perspectives in cloud computing. We researched related work in development models of cloud computing and commercially available cloud computing services. Considering security threats in cloud computing identified by Gartner, efforts to improve cloud computing security by various organizations including CSA, OCC, SNIA, ENISA, and NIST were explained respectively as major technical development efforts. Finally, major network security paradigms for cloud computing by OCC, CSA, and RSA were introduced to forecast future directions of network security perspectives for cloud computing.

References

1. Kimball, A., Michels-Slettvet, S., Biscigilia, C.: Cluster Computing for Web-Scale Data Processing. In: SIGCSE 2008, Portland, Oregon, pp. 116–120 (2008)
2. Wikipedia, http://en.wikipedia.org/wiki/Cloud_computing
3. Vision, Hype, and Reliability for Delivering IT Services as Computing Utilities, HPCC 2008 Keynote (2008)
4. Thomas, D.: Enabling Application Agility-Software as a Service, Cloud Computing and Dynamic Languages. Journal of Object Technology 17(4) (May-June 2008)

5. Lawton, G.: Developing Software Online with Platform-as-a-Service Technology. Computer (June 2008)
6. Armbrust, M., et al.: Above the Clouds: A Berkeley View of Cloud Computing (February 2009), http://radlab.cs.berkeley.edu
7. Amazon Elastic Compute Cloud (Amazon EC2), http://aws.amazon.com/ec2
8. Amazon Simple Storage Service (Amazon S3), http://aws.amazon.com/s3
9. Valdes, R.: Google App Engine Goes Up Against Amazon Web Services. Gartners (April 2008)
10. Mitchell, A.: Google Apps: Education Edition Overview Webinar, http://www.google.com
11. Cloud Security Alliance, http://cloudsecurityalliance.org/
12. Open Cloud Consortium, http://opencloudconsortium.org/
13. Storage Networking Industry Association, http://www.snia.org/home/
14. European Network & Information Security Agency (ENISA), http://www.enisa.europa.eu/
15. National Institute of Standards and Technology, Computer Security Resource Center, http://csrc.nist.gov/groups/SNS/cloud-computing/
16. Andrei, T., Jain, R.: Cloud Computing Challenges and Related Security Issues. Project report, Washington University in St. Louis (April 2009)
17. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, Cloud Computing Alliance (December 2009)
18. The Role of Security in Trustworthy Cloud Computing, White Paper, RSA
19. Brodkin, J.: Gartner: Seven cloud-computing security risks (July 2, 2008), http://www.infoworld.com
20. European Network and Information Security Agency (ENISA), Cloud Computing: benefits, risks and recommendations for information security (November 2009)