AN INTEGRATED MODEL FOR SECURE ON DEMAND RESOURCE PROVISIONING BASED ON SERVICE LEVEL AGREEMENT (SLA) IN CLOUD COMPUTING

[1]ADNAN ABDULWAHED HASSAN, [2]BASMA MOHAMADHASHIM BAI, [3]TAGHI JAVDANI GANDOMANI

[1]Universiti Putra Malaysia, Faculty of Computer Science and Information Technology, Serdang, Malaysia
[2]Tenga National University, College of IT, Department of Information Systems, Kajang, Malaysia
[3]Department of Computer Engineering, Boroujen Branch, Islamic Azad University, Boroujen, Iran
E-mail: [1]adn518@yahoo.com, [2]basma@hotmail.com, [3]tjavdani@yahoo.com

ABSTRACT

Cloud computing, as new paradigm of new century, provides various advantages and benefits for the organizations and individuals. Among them resource provisioning is a big advantage that supports cloud providers cloud resources with their users. Providing a secure way for resource provisioning is a critical issue, so that any neglect of it causes a lot of concerns for both providers and users. Service Level Agreement (SLA) defines the level of access to the resources providing in cloud environment. The main aim of this study is providing a model to integrate the common security policies and mechanisms with SLA. It proposed a security infrastructure for on-demand service provisioning.

Keywords: *Cloud Computing, Resource Provisioning, Service Level Agreement (SLA), Security, Secure Model*

1. INTRODUCTION

Cloud computing is emerging as a common approach and a model for provisioning services on demand that include both computation, storage and advanced network infrastructure. It allows minimizing infrastructure cost management for both customers and providers [1].

Cloud computing is defined as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storages, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [2]. Furthermore, cloud computing enables dynamic provisioning of resources based on the requirements of the user [3],[4].

Infrastructure as a Service (IaaS) is considered as the lowest layer and provides virtualized computer infrastructure components as a service. Above this, Platform as a Service (PaaS) delivers computing environments tailored to specific needs as a service. The upper-most layer, Software as a Service (SaaS), provides complex software functionality. Their inherent independence of a specific platform and operating system makes them perfectly suitable to connect service consumers and service providers over the Internet and provide a technical foundation for cloud.

The huge interest in cloud technology and the inherent security concerns that come with it have steered a number of researches on security and privacy. Although some studies have argued that most security concerns in the cloud are similar to those previously found in traditional systems, security concerns in cloud services are more than traditional information systems, poses increased security challenges for the Cloud Service Consumers (CSC). For instance, the 2011 hacking of the Sony’s network, whereby millions of users’ personal and credit cards information were compromised was attributed to a hacker renting the service of Amazon’ EC2. [5]

Accordingly, Cloud computing and its predecessor technologies such as resource provisioning demand more studies especially from security point of view. In this study, at first the challenges and requirements of secure resource provisioning in cloud computing will be discussed. Then a new framework is proposed to integrate common security mechanisms with SLA in order to improve secure resource provisioning in cloud environment.

The rest of paper is as follows: at first we try to review some of the related works. Then Security risks of resource provisioning will be the next section. After that, security requirements for resource provisioning will be elaborated. At the end, our proposed model and conclusion are the last two sections of this study.

2. RELATED WORKS

Due to the young nature of cloud computing, the number of papers with focus on secure resource provisioning is not too many.

In their work, Ngo et al [1] discussed the ongoing research on developing security framework for Cloud computing environments and infrastructure services provisioned on-demand which aims to deliver a security infrastructure to support consistent trust establishment, identity management, access control, as well as security context management. Based on the analysis of possible Cloud scenarios, their model identifies requirements and functionalities of the security infrastructure for Clouds. In addition, their paper proposes a security reference model that is used as a basic for defining the architecture and practical mechanisms. The presented research is conducted as a part of few EU projects such as GEYSERS and GEANT3 which provide a prototype implementation and test-bed.

Author of [6] offered a security architecture that enables service owners to provision a dynamic and service-oriented secure virtual private network on top of multiple cloud IaaS providers. It does this by leveraging the scalability, robustness and flexibility of peer to peer overlay techniques to eliminate the manual configuration, key management and peer churn problems encountered in setting up the secure communication channels dynamically, between different components of a typical service that is deployed on multiple clouds.

According to [7], the rise of virtualization and cloud computing is one of the most significant features of computing in the last 10 years. Data security and the lack of trust that users have in relying on cloud services to provide the foundation of their IT infrastructure is a big challenge. This is a highly complex issue, which covers multiple inter-related factors such as platform integrity, robust service guarantees, data and network security, and many others that have yet to be overcome in a meaningful way. This paper presents a concept for an innovative integrated platform to reinforce the integrity and security of cloud services and they applied this in the context of Critical Infrastructures to identify the core requirements, components, and features of this infrastructure.

3. SECURITY RISKS APPLY TO RESOURCE PROVISIONING

The dependability and the predictability in reference to the availability of the cloud services is not definite [8]. The risks listed below might include other cloud service models in addition to IaaS with only high probability of occurrence according to the author's research and experience. The security breach of any large service provider will have a much bigger impact than if it was occurred on a medium to large organizations [9] in terms of economic and reputation to a large number of customers and the provider as well. The ability to open web-based Amazon EC2 management console and start several hundreds of virtual servers based on Linux/Unix or Windows with few clicks, cost of pennies per hour and within a short period of time is amazing. This speed in setting up system like this will encourage the underground hackers to utilize cloud for a malicious usage and add more risks to the internet community.

A. IaaS has been used to host crimeware. For example, in 2009, Zeus toolkit utilized Amazon's EC2 IaaS to command, control and launch botnet attacks. This type of attack makes hard for companies to list the source in the blacklist [10], since the source of the attack is coming from a legitimate CSP such as Amazon. IaaS was subject to DoS attacks. A demonstration by Slaviero [11] was performed against Amazon EC2 by a cloud subscriber. The cloud subscriber created 20 accounts and started a preliminary 20 accounts and then started new VM instances for each, then using those accounts to create further 20 accounts and VM instances in an iterative manner, exponentially growing and consuming resources beyond set limits.

B. Virtualization software contains well-known bugs, which provide a "break loose" or known by European Network and Information Security Agency (ENISA) as "isolation failure" where the mechanisms used to separate storage, memory and routing fails among different tenants of the shared infrastructure. Multi-tenancy and the use of shared resources can also increase the risk. In fact, United States Government Accountability Office stated that twenty three out of the 24 US agencies identified multi-tenancy as a possible risk because one client could deliberately or inadvertently gain access to another customer's data, causing the release of sensitive information. This bug might provide a code access to some parts of the provider's infrastructure, or other consumer's resources [4].

C. Another issue is when several VMs are running and sharing memory space on the same server happens when an attacker steals data, by using an eavesdropping program to analyze the way those programs share memory space [12].

D. Another risk in IaaS is the secure preservation and removal of records, including those sentenced for destruction must be performed by an approved procedure since this is a legal requirement otherwise data may not truly be wiped. Identifying the location of the destroyed data and determining the number of copies may not be conceivable, because data might be preserved at diverse locations as a redundant data to improve cost-effectiveness and reliability, which means the user doesn't know where the data are stored.

So concisely, the aforementioned potential risks can be summarized as continue:

a) Authentication and identity management of users.
b) DOS and DDOS attacks to/from cloud environment.
c) Service availability for end user.
d) Virtualization potential risks.
e) Trustworthiness and reliability challenges.
f) Shared memory issues.
g) Data confidentiality.
h) Misuse the vulnerabilities of the system by .end user.

4. SECURITY REQUIREMENTS FOR RESOURCE PROVISIONING

Security requirements for Cloud computing Environments have been investigated by the first generation of Cloud computing research and then further analyzed based on recently proposed Cloud reference architecture models [13, 14]. Based on the scenario in the previous section, the requirements could be summarized as follows:

- ➢ Identity management and access control mechanisms in the multi-tenancy and multi-provider Cloud environments. There is some preliminary work on this area which defines principal use-cases on identity and access control management, multi-tenancy authorization system for Cloud services [15]. However, most of them do not take into account the relevance of these issues to the service lifecycle model or lack of multi-provider scenarios.

- ➢ Management of the trustworthiness and reliability of the Inter-cloud. Most of existing work in this area do not investigate practical solutions in detail and propose feasible mechanisms [1].Some related work on trust management [16] needs to be investigated and propose to suite with the Cloud characteristics.

- ➢ Mechanisms to isolate operations and mutual effects among tenancies in the sharing physical resources by virtualization and hypervisors[14].

- ➢ Supporting security compliance and regulations.

- ➢ Issues on protect Cloud providers' resources infrastructure. It requires not only the traditional perimeter security mechanisms but also need to aware of the characteristics of Cloud computing reference models [13].

So briefly, these requirements should be addressed in any model for secure resource provisioning:

1) Integrity of SLA and security policies for secure resource provisioning.
2) Efficient authentication mechanism.
3) Well organized Access control list (ACL)
4) Keeping the track of end user by keeping his/her IP and session ID and other necessary information
5) Deploying a well-organized mechanism to keep resource always available (avoidance from DOS and DDOS attack)
6) Notifying end user while failed login to the end user happened.

With distinguished characteristics of on-demand provisioned services and Cloud computing, providing a consistent and robust security infrastructure is not trivial task and has many challenges to solve. Next section proposes a security infrastructure reference model for On-demand service provisioning to meet these requirements.

5. PROPOSED SOLUTION: SECURITY INFRASTRUCTURE FOR ON-DEMAND SERVICE PROVISIONING

The general security framework for on-demand provisioned infrastructure services should address two general aspects [1]: (1) secure operations resource management at cloud provider side, and (2) provisioning security services as part of the Cloud that is known as provisioned on-demand virtual infrastructure. The first is related to system protections in a cloud provider and collaboration between providers that some solutions on identity and access control management have solved; while dynamic provisioning of managed security services is and open issue requiring additional research for cloud computing.

Based on what has been discussed, any model for secure resource provisioning should fulfill the following requirements:

1. Applying well-organized security policy
2. Effective Monitoring and logging mechanism to monitor and record the activity of end user
3. Monitoring the level of usage of resources and any sign of DOS or DDOS attack
4. More secure virtualization based software.
5. Access control and grant permission management
6. Checking the bugs and vulnerability of developed software by cloud provider before it st PaaS model
7. Secure development and configuration of cloud based software

Accordingly a model that can fulfill majority of these requirements is offered in Figure 1 to secure resource provisioning in cloud computing. As it can be observed, this model has several components that each of which is added based on the demands that was argued. Discussion about each component's responsibility's is explained in continue:

1. Service Level agreement: In this model, the core component is the Service Level Agreement (SLA) Management which handles initial agreements between actors. These actors can be multiple providers form the supply-chain from computing services to customers. It also includes not only the customer (tenant) who subscribes computing services from providers but also end-users who consume a particular cloud service. The SLA Management is the substrate to build up the trust relationships among involved actors in a virtual infrastructure eco system.

2. Authentication and identity management: The identity of the user is the first thing that needs to be clarified. Depends on the environment, either static Public Key Infrastructure (PKI) or password based authentication could be done.

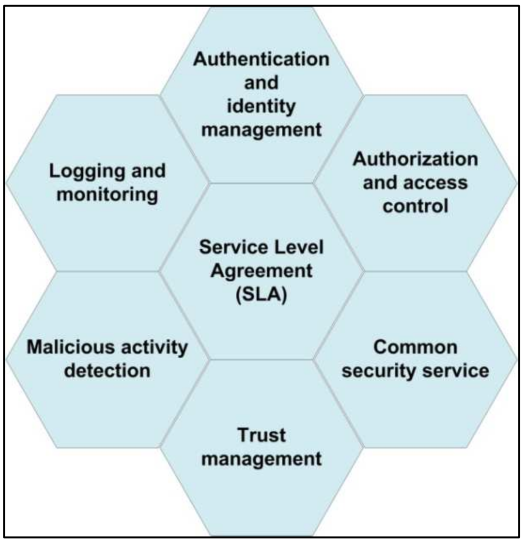
Authentication and identity management
Logging and monitoring
Authorization and access control
Service Level Agreement (SLA)
Malicious activity detection
Common security service
Trust management

Figure 1: Description Is Placed Right Below The Figure

3. Authorization and access control: This is an important module which determines the level of access of cloud user to the resources that cloud vendor offers. It is clear that the legitimacy and legality of user activities would be determined based on the SLA and this module.

4. Common Secure services: basically the integration of security services between cloud user and provider is the duty of this module. So confidentiality of data in communication and storage and integrity of data are done by this component. As an example, In order to secure the communication between two parties, prior solutions such as virtual private network (VPN) or dynamic-VPN [6] might be used.

5. Trust management: in the real world, trust is a matter of time. In other word, how much two person or parties can trust each other relies on

their history of interactions. This component keeps a history of user so in the future cloud provider will know how much sensitive should be about that customer.

6. Malicious activity detection: As it was mentioned, since the intention of user is not clear at first when he/she wants to use the service of cloud, some attacks such as DOS or DDOS and so on might start by misusing the dedicated resources. So it is essential to detect any kind of malicious activity by this module. For example, during the time the normal and healthy activity of user will be exposed to cloud provider more or less. So any abnormality in the future can be recognized. Many researchers devote their study to address this issues and variety of solutions available for use.

7. Logging and monitoring: this module is responsible to record and keep a track of user activities which would be used in the future by other sections.

6. CONCLUSION AND FUTURE WORK

Cloud computing is a new paradigm of 21st century. It has introduced many benefits for both organizations and individual users. Provision of the resources is one these advantages in which cloud providers share their resources with their users. Clearly this resource provisioning must be done in the secure way otherwise it causes lots of concerns for providers and users. Generally the level of access to the resources in cloud is defined based on the service level agreement (SLA). In this paper we tried to integrate the common security mechanisms and policies with SLA.

It is clear for reader that this model is a preliminary and tentative model and probably it demands more considerations and modification. In addition, evaluation and verification of this model can to be performed based on the implementation which is going to be the future work of this study.

REFRENCES:

[1] N. Canh, P. Membrey, Y. Demchenko, and C. De Laat, "Security Framework for Virtualised Infrastructure Services Provisioned On-demand," in Cloud Computing Technology and Science (CloudCom) IEEE Third International Conference, 2011, pp. 698-704.

[2] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST special publication, vol. 800, 2011, p. 145.

[3] A. Bakshi and B. Yogesh, "Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine," in Communication Software and Networks, ICCSN 2nd International Conference on, 2010, pp. 260-264.

[4] L. Karadsheh, "Applying security policies and service level agreement to IaaS service model to enhance security and transition," Computers & Security, vol. 31, 2012, pp. 315-326.

[5] M. Ouedraogo and H. Mouratidis, "Selecting a Cloud Service Provider in the age of cybercrime," Computers & Security, vol. 38, 2013, pp. 3-13.

[6] A. Sajjad, A. Zisman, M. Rajarajan, S. K. Nair, and T. Dimitrakos, "Secure communication using dynamic VPN provisioning in an Inter-Cloud environment," in 18th IEEE International Conference on Networks, 2012, pp. 428-433.

[7] M. Mackay, T. Baker, and A. Al-Yasiri, "Security-oriented cloud computing platform for critical infrastructures," Computer Law & Security Review, vol. 28, 2012, pp. 679-686.

[8] R. Sandhu, R. Boppana, R. Krishnan, J. Reich, T. Wolff, and J. Zachry, "Towards a discipline of mission-aware cloud computing," in Proceedings of the 2010 ACM workshop on Cloud computing security workshop, 2010, pp. 13-18.

[9] W. Kim, S. D. Kim, E. Lee, and S. Lee, "Adoption issues for cloud computing," in Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia, 2009, pp. 2-5.

[10] D. Danchev, "Zeus crimeware using amazon's EC2 as command and control server," Available: http://tinyurl.com/ltgtbsm.

[11] M. Slaviero, "BlackHat presentation Demo Vids: amazon," Available: http://www.sensepost.com/blog/3797.html

[12] D. Talbot, "Security in the Ether," Technology Review, vol. 113, 2010, pp. 36-42.

[13] NIST, "NIST Cloud Computing Standards Roadmap," ed: NIST, 2011.

[14] H. Takabi, J. B. D. Joshi, and A. Gail-Joon, "Security and Privacy Challenges in Cloud Computing Environments," Security & Privacy, IEEE, vol. 8, 2010, pp. 24-31.

[15] J. M. Alcaraz Calero, N. Edwards, J. Kirschnick, L. Wilcock, and M. Wray, "Toward a Multi-Tenancy Authorization System for Cloud Services," Security & Privacy, IEEE, vol. 8, 2010, pp. 48-55.

[16] M. Blaze, S. Kannan, I. Lee, O. Sokolsky, J. M. Smith, A. D. Keromytis, and W. Lee, "Dynamic trust management," Computer, vol. 42, 2009, pp. 44-52.