A review on Cloud Computing Security requirements and threats

Bin Yu

Submission date: 2013-5-10

ABSTRACT

The economic case for cloud computing is compelling. However the security challenges it poses are equally striking. Though many researchers have done a lot on various types of security threats, there are a few researches that address the classification of the security requirements and threats. The goal of this paper is to provide a review on publications specific in cloud computing security. We discuss which types of threats have been under-researched and which are most investigated. From previous publications we classify the threats or requirement into nine sub-areas. We found that some sub-areas are the most investigated, while a few research have been done on others. In conclusion we analyze this phenomenon and give our own suggestions on future studies.

I. Introduction

The Cloud Computing (CC) model is consisted of two participants, one is cloud service provider (CSP) and another is cloud service consumer (CSC). The CSPs deliver the service through the Internet. And the CSCs access the service from the web browsers or end-user software. A three level model is built to describe the services that cloud provided: Infrastructure as a service (IAAS), Platform as a service (PAAS) and Software as a service (SAAS). For all the three, security has been ranked as the greatest challenge. The goal of this paper is to provide an overview of the security requirements and threats. To achieve this goal we will investigate which security threats has been identified, how can they be addressed and what solutions are proposed. We use a frame to present our discoveries in the literature. From many security frameworks, we choose the one of Firesmith [1] which provides taxonomy of security sub-factors that can be used as a basis for organizing and identifying different security threats. In section II we will describe our review methods, and how we establish the boundary of this review. In section III we will talk about the threats models, classification of different literatures. In section IV we will give a conclusion.

II. Review Method

This study aims to answer the following research questions: (1) What security threats have been addressed in published literatures? (2) What solutions are offered to them? (3)What are the new security requirements and threats that have not pay much attention to.

We use these research questions for determining the content of our paper, for locating and selecting primary studies, for critically evaluating the studies and for analyzing the results. Our review just classifies and presents the publications according to the sub security areas they are addressed.

We use Monash library explores as a search engine because it contains the most important publication from journals and conference proceedings. We search with the search condition ‘cloud security and threats’ and ‘cloud security audit’ to find papers that have these words in title, abstract and keywords. We also set the searching filters as (a) Limitation of paper source (journal articles and conference papers) (b) Limitation of subject area (computer science, engineering and business).

We consider as relevant all publications that comply with the criteria.(1) Cloud computing security must be the major topic or one of the major topics of the publications,(2) Where multiple publications are reporting the same study only the most recent is selected. We do not include the papers that with these features (1) Security models for very specific context (e.g. healthcare, national security, etc). (2) Publications covering service level agreements (SLA) and multi-tenancy issues but not elaborating on the security clauses and threats. (3) Publications focusing on security threats but not explicitly focusing on cloud computing (e.g. traditional network security, grids computing, etc).

III. Classifying and using a model for security threats

We use the security analyze model in [1] to analyze and classify the selected publications. Figure 1 gives the nine sub-classes of the whole security models. This model gives researchers convenience to classify their security issues.

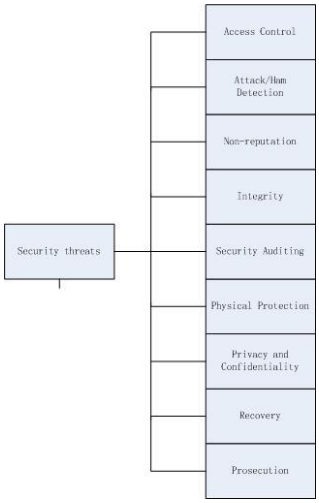

Figure 1 security analyze model in [1].

A. Access Control

Access control is one of the most important aspects in CC security and has been addressed a lot by many articles. With this mechanism, the CSP only provides resources to the authorized entities. The access control security addresses the requirement to recognize the participants that want to have an interaction with the CSPs. The traditional way of handle access control cannot work well in CC. Almulla and Yeun [2] describe a new protocol that works in CC environment called Identity and Access Management(IAM). Other approaches in this sub-class use a combination of asymmetric and symmetric cryptography, and capability based access control. In [3], the access to platform services is regulated based on the permissions encoded in cryptographic capability tokens, and [4] addresses security threats and requirements of personal cloud computing through major cloud services.

Some articles focus on the method of access to the cloud. Jensen and Schwenk [5] address the access to the service of cloud (email, online-stream etc) through web applications, which open deem as the weakest part of CC. At the end Jensen and Schwenk give technical solutions to overcome these obstacles like encrypting data or using more security protocols for transmission (https, ssl etc).

Multi-tenant has been addressed by some publications. Though multi-tenant brings many benefits, it also causes many potential security threats like role management confliction, cross-level role access control. One solution for these issues is the SAAS Role Based Access Control (S-RBAC) model [6]. The solutions help to distinguish between ‘home cloud’ and ‘foreign cloud’. The ‘home cloud’ is a CSP which is unable to meet the demand with its current resources and, therefore, forward federation requests to ‘foreign cloud’ with the purpose to exploit their virtualization infrastructures.

B. Attack /Harm Detection

This refers to the detection, recording, and notification requirements when an attack is attempted and/or succeeds [1]. Currently, the solutions are classified as four groups. The first groups include cloud firewalls as the filtering mechanism for attack prevention. Their essential feature is to take full advantage of cloud environment. The firewall can changes its policy dynamically and shares the threats information dynamically. Unfortunately the cloud security standards in the cloud firewalls are still in chaotic state, different vendors use different standards. The second group refers to security measuring framework suitable to SAAS [7]. The third group takes advantages of the cloud community, different CSPs share the information about attacks. It will use system watch service to analyze and detected malware attacks [8]. The unwilling to share the malware attacks information maybe an obstacle for the adoption of this approach. The fourth group covers the multi-technology based approaches, e.g. for example, the cloud security based intelligent Network-based Intrusion Prevention system (NIPS) [9] that includes four key technologies – active defense technology, linkage technology with firewall, synthesis detecting method, and hardware acceleration system, to block visits under the real-time determination. However the multi-technology based approaches like NIPS system is not so easy to apply in reality, as many different technologies work together, The error output of one module will definitely affects other modules.

C. Security Auditing

This is about enabling the security personnel to audit the status and use of security mechanisms by analyzing security-related events [1]. Audit of security events is usually based on the configuration management and vulnerability assessment. The approach in [10] assesses the vulnerability of each VM in an infrastructure. Using a logging system to do the audit has been proposed by many radicals. Other papers address building a Security Model for IAAS to guide security assessment and enhancement in IAAS layer. On the PAAS layer, it is suggested to

build an infrastructure that combines semantic security risk management tools with dynamic web service policy framework to support the mitigation of security threats.

D. Privacy and Confidentiality

This is about preventing unauthorized participants from obtaining the sensitive information [1]. For privacy requirements to be well defined, it is vital that meaningful, clear and valuable privacy metrics are identified. Currently, one solution to enhance the privacy is to uses cloud-based malware scanners and data fragmentation technology to hide the data, or separate the CSUs' data from the software layer.

E. Integrity

Integrity means focus on how the different parts of the cloud system works together as a whole to enhance the security [1]. We found that most of the selected papers address the security threats in this area. As CC is so complex, many issues in cloud computing cannot be solved until consider these issues in a whole cloud system. Different security level modules have been proposed by many papers to enhance the security.

F. Finding of the review

We found that most of the publications address the issues in access control, privacy, attack detection, security auditing and Integrity. However none papers discuss Physical Protection, Recovery and Prosecution. The reason maybe that (a) security of the Physical machine does not included in our review. (b)Security threats about Physical protection, Recovery have been involved in other sub-classes. (c) Researchers may find that few or limited improvement can be done on Physical layer.

We also found that few papers address the threats in data privacy and confidentially. One possible reason is that people find the data privacy is an old issue and the traditional solutions of privacy can be applied in CC. Another reason may be the data privacy is closely related to the access control. The privacy of data can be guaranteed by enforcing a strong access control by preventing the unauthorized users to obtain the confidential data.

Many articles have addressed the security requirements and threats in CC, however many of the threats they described only reflects the traditional network problems. The security requirements that multi-tenant and data sharing bring are rarely addressed. We regard these two features are quite significant for further study.

IV.Conclusions

Within this study we aim to provide a classification of the recent papers on Cloud Computing into Firesmith security model [1].

As an answer to research question 1, we found that six out of nine sub-areas [1] are discussed in recent papers. Among these issues, Access control, auditablity and integrity are the most investigated.

As an answer to research question 2, we found that most solutions for the threats focus on multi security sub-classes. These solutions solve the security threats to some extent, and every solution has its own limitations. And some solutions may out of time as CC is a fast developing technology.

As an answer to research question 3, we found that new threats in multi-tenant and data sharing are rarely addressed by the current research. These security requirements are critical to the deployment of the CC. And this is a good research topic for further study.

In this paper, we give classification of published lectures. We also analyze the research trend in CC. And in the end we give some ideas and suggestions for future research.

References

[1] D. Firesmith, "Specifying reusable security requirements," *Journal of Object Technology,* vol. 3, pp. 61-75, 2004.

[2] S. A. Almulla and C. Y. Yeun, "Cloud computing security management," in *Engineering Systems Management and Its Applications (ICESMA), 2010 Second International Conference on*, 2010, pp. 1-7.

[3] Y. Karabulut and I. Nassi, "Secure enterprise services consumption for SaaS technology platforms," in *Data Engineering, 2009. ICDE'09. IEEE 25th International Conference on*, 2009, pp. 1749-1756.

[4] S.-H. Na, J.-Y. Park, and E.-N. Huh, "Personal Cloud Computing Security Framework," in *Services Computing Conference (APSCC), 2010 IEEE Asia-Pacific*, 2010, pp. 671-675.

[5] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On technical security issues in cloud computing," in *Cloud Computing, 2009. CLOUD'09. IEEE International Conference on*, 2009, pp. 109-116.

[6] D. Li, C. Liu, Q. Wei, Z. Liu, and B. Liu, "RBAC-based access control for SaaS systems," in

Information Engineering and Computer Science (ICIECS), 2010 2nd International Conference on, 2010, pp. 1-4.

[7] Q. Liu, C. Weng, M. Li, and Y. Luo, "An In-VM measuring framework for increasing virtual machine security in clouds," *Security & Privacy, IEEE,* vol. 8, pp. 56-62, 2010.

[8] N. Hawthorn, "Finding security in the cloud," *Computer Fraud & Security,* vol. 2009, pp. 19-20, 2009.

[9] J. Tiejun and W. Xiaogang, "The construction and realization of the intelligent NIPS based on the cloud security," in *Information Science and Engineering (ICISE), 2009 1st International Conference on*, 2009, pp. 1885-1888.

[10] S. Bleikertz, M. Schunter, C. W. Probst, D. Pendarakis, and K. Eriksson, "Security audits of multi-tier virtual infrastructures in public infrastructure clouds," in *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, 2010, pp. 93-102.