Proceedings of 2013 International Conference on
Technology Innovation and Industrial Management
29-31 May 2013, Phuket, Thailand

A NOVEL INFRASTRUCTURE FOR DATA SANITIZATION IN CLOUD COMPUTING (RESEARCH PAPER)

Cheng-Yuan Ku, National Chung Cheng University, Taiwan, ROC
E-mail: cooper.c.y.ku@gmail.com

Yu-Siang Chiu ,National Chung Cheng University, Taiwan, ROC
E-mail: fishfly1115@gmail.com

ABSTRACT

Purpose- *In this extended abstract, we propose a novel infrastructure in cloud computing environment which assures the data sanitization after the customers decide to delete them.*
Design- *A mechanism with monitoring agents is suggested to watch the data usage over entire life cycle and assure the data sanitization in the end.*
Findings- *Security analysis and performance analysis will be done after the complete infrastructure is decided. We expect this mechanism should fulfill the security and performance requirements for cloud computing users.*
Originality/Value- *The emerging cloud computing technology needs the assurance of various security requirements, otherwise most of customers/organizations do not dare to adopt it. Our research proposes an infrastructure to solve one of the security problems, i.e. data sanitization. As well known, only after the security requirements of cloud computing could be managed and guaranteed, the prospects of the cloud services are brightening.*

Keywords: cloud computing, cloud services, information security, data sanitization, trusted third party (TTP), agent

INTRODUCTION

In recent years, as cloud computing becomes more and more popular, it has gradually drawn many enterprises' attention. Ironically, one of the major factors which lead the development of cloud computing is the previous economic recession. Due to the keen business competition and tight budget, enterprises need to find any possible ways to reduce cost. According to the National Institute of Standards and Technology (NIST), cloud computing providers offer services with three fundamental models (Mell and Grance, 2011):

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Based on the individual need, enterprises can choose anyone, both or all of the above-mentioned methods to construct computing services for stakeholder. From the perspective of technology, cloud computing seems to be able to give a chance to divest infrastructure management of information systems and to enhance core competencies. However the potential security issues may hinder the cloud services from fast developing.

Even with the protecting mechanism in cloud, the attacker still can take various attack models to invade. Cloudburst virtual machine (VM) escape is an exploit method that enables

a guest-level virtual machine to attack its host (Kortchinsky, 2009). A method that prevents the VM escape has been proposed by security researchers (Ristenpart et al., 2009). In addition to the above-mentioned attack, one of the other major security considerations is data sanitization. Actually a deleted file only means the erased directory, not the file itself. This issue becomes even more complicate in cloud environment and still has no concrete solutions until now.

The trusted third party (TTP) and agent are two of the popular methods to solve many security issues. The TTP can act as a monitor and audit the performance of service providers for customers. An agent is generally developed to monitor network activity, collect information, act for a user or other program … and so on. For example, it can identify malicious network behavior that does not comply with the policy and send the alert to the managing center (Manzoor and Nefti, 2009). According to the published security guidance in cloud computing by Cloud Security Alliance (CSA) (CSA, 2011), there are two types of monitoring mode:

- Database Activity Monitoring (DAM)：Database Activity Monitor captures and records all Structured Query Language (SQL) activity in database in real time or near real time. The database monitoring server will generate alerts on policy violations.
- File Activity Monitoring (FAM)：FAM records how the customers access file and generate alerts on policy violations.

Until now, there are some solutions of new generation DAM which are based on kernel-level implementations and other intrusive approaches (Lombardi and Di Pietro, 2011; Shao et al., 2010). This means that adding a layer of security requires changes in architecture and relies on the virtualization technology. McAfee, the world's largest dedicated security technology company, has made an effective solution which can be easily embedded into the guest VM. This is the so-called McAfee Database Activity Monitoring (McAfee, 2012). In short, within the proposed infrastructure, the TTP, agent modules and improved sanitization procedure are adopted to assure the security of sensitive data.

PROPOSED MECHANISM

In order to achieve the data sanitization, the entire data life cycle must be monitored. In this way, the manager can record and control the detailed process of data usage and storage. Based on the above-mentioned McAfee Database Activity Monitoring, we further design a monitoring mechanism to handle the data sanitization problem as shown in Figure 1. In cloud environments, the customers, in general, deploy the needed applications, platforms or infrastructures on VMs. Therefore, we suggest that a monitoring agent should be embedded into every VM which hosts the application or database.

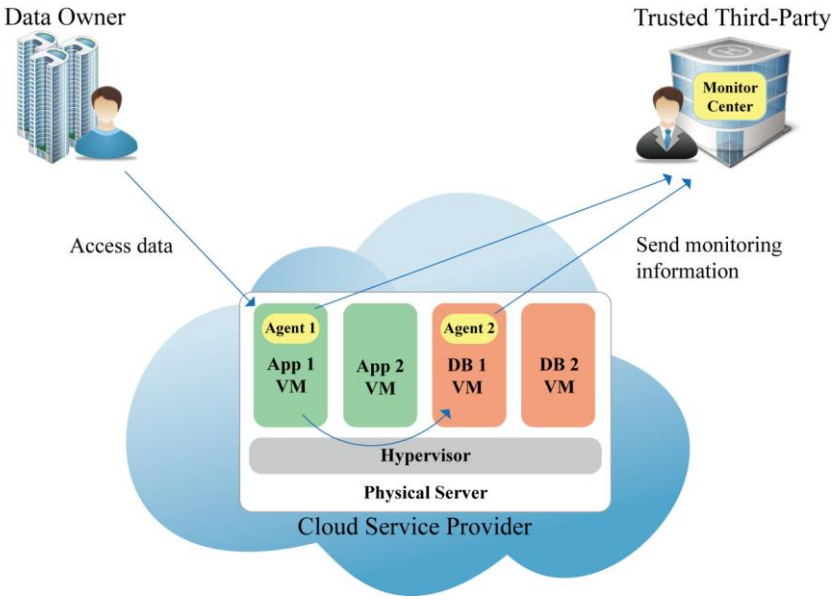

Fig. 1 Monitoring architecture

- Access function：while the data owner accesses data via applications on VM, agent 1 shall collect the log information and sent to the TTP.
- Process function：agent 1 shall also monitor communication between the applications and database.
- Store function：agent 2 shall monitor the database and have all activity reports sent to TTP.

FUTURE WORKS

Currently the design of monitoring mechanism in cloud environment is already finished but the detailed data sanitization procedure is still under construction. Furthermore, the security analysis and performance analysis should be conducted thereafter. The security analysis is going to include the man-in-the-middle attack, verifiability, brute-force attack, and spoofing and so on. We plan to implement the prototype of proposed mechanism by using Hadoop platform. As for the performance analysis, the speed of overwriting and the efficiency of monitoring center will be assessed. Finally, we will compare with McAfee Database Activity Monitoring about performance.

REFERENCES

1. CSA (2011), “Security guidance for critical areas of focus in cloud computing v3.0”, Cloud Security Alliance.
2. Kortchinsky, K. (2009), “CLOUDBURST: A VMware guest to host escape story”, Black Hat USA, Las. Vegas, USA, June 2009.
3. Lombardi, F., and Di Pietro, R. (2011), “Secure virtualization for cloud computing”, Journal of Network and Computer Applications, Vol. 34 No. 4, pp. 1113-1122.
4. Manzoor, U., and Nefti, S. (2009), “An agent based system for activity monitoring on network–ABSAMN”, Expert Systems with Applications, Vol. 36 No. 8, pp. 10987-10994.

5. McAfee (2012), “Database security in virtualization and cloud computing environments”, McAfee.
6. Mell, P., and Grance, T. (2011), “The NIST definition of cloud computing”, NIST Special Publication 800-145.
7. Ristenpart, T., Tromer, E., Shacham, H., and Savage, S. (2009), “Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds”, in the 16th ACM Conference on Computer and Communications Security Proceeding of the International Conference in Chicago, IL, USA.
8. Shao, J., Wei, H., Wang, Q., and Mei, H. (2010), “A runtime model based monitoring approach for cloud”, presented at the 2010 IEEE 3rd International Conference on Cloud Computing.