Implement Access Control Architecture to Enhance Security and Availability of Cloud Computing Systems

Xixu Fu, Kaijun Wu and XiZhang Gong

Institute of Information Technology, Shanghai Ocean University, Shanghai, China
xxfu@shou.edu.cn

Abstract

Cloud computing can improve utilization of powerful computer systems. However, security problems become an important challenge in the cloud systems. Implementation of antivirus software can cost a lot of resource. This paper advanced an access-control based architecture of operation systems which ensure the high availability of the whole system. System resource cost on security can be dropped by the implementation of this architecture.

Keywords: *Cloud System, Security, Virus, Access Control*

1. Introduction

Security is a serious problem for any computer systems. Malwares exhaust system resource, steal important information and tamper important configurations. What's more, virus can spread through the internet in amazing speed. Antivirus software systems tried to prevent systems from threatens of attacking and infection by recognizing the pattern of virus. However, a lot of resource had been used on preventing malicious software and fixing system vulnerabilities. As new virus emerges, more and more resource will be used on malware protection.

Nowadays, computers and servers become more and more powerful. Cloud computing architectures can make full use of powerful machines by creating virtual machines on them and rearrange the computing power for different applications [1]. In cloud systems, infrastructure, platform and software are regarded as services. All resource can be distributed for different applications. IaaS corresponds to hardware of traditional computer system. PaaS corresponds to the operation system layer of traditional computer system. SaaS corresponds to the software and applications of traditional computer system.

In cloud computing systems, malwares can be even more fatal [2]. Virus can spread easily in virtual machines than in real machines. Furthermore, manager of virtual machines can be the super user over many servers. The whole system will be in danger if administrator access gained by hackers [3]. On the other hand, antivirus software can cost more computing resource than that in traditional systems.

This paper analyzed security in traditional systems and cloud systems. Based on the finding that executing and writing priority caused most invulnerability and performance degrading of computing system, access control based cloud security architecture was advanced in the paper. The architecture was introduced on the aspects of IaaS and PaaS respectively. Antivirus software reducing, Availability enhancing and reliable data management are discussed based on the model.

2. Related Work

2.1 Virus and Anti-Virus Software

Traditional antivirus systems prevent computers from malware by recognition patterns of virus. Although effective antivirus software developed every year, many new viruses spread in computers every year. Table1 shows the virus in computers every year stated by an antivirus corporation.

Table 1. New virus emerges every year. Millions of computers were infected [5]

Year	New Types of Virus	Infected Computers
2006	10375	18832094
2007	100017	34414776
2008	47743	27998478
2009	101586	14933761
2010	91994	11533661
2011	66686	3743721

Figure 1 shows the virus categories and percentage discovered in recent years.

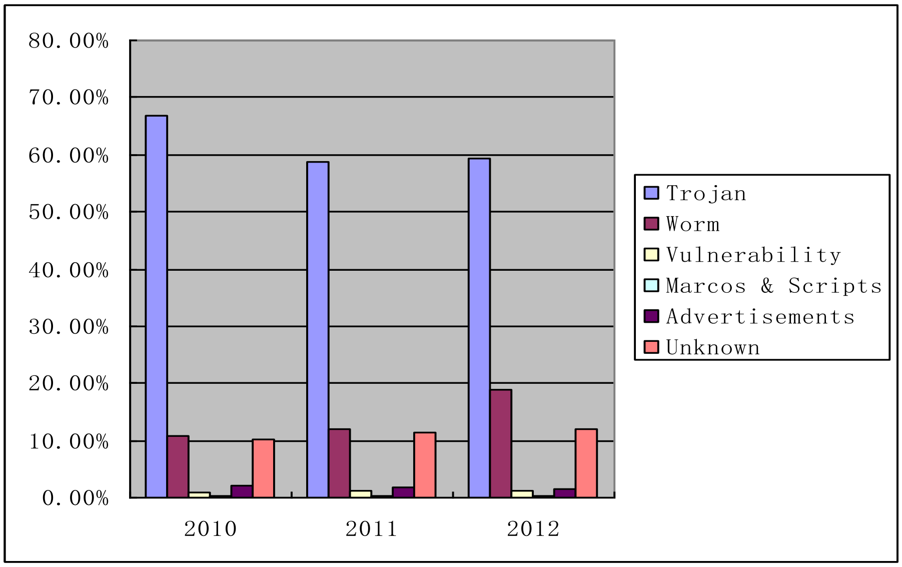

Figure 1. Percentage of Computers Infected by Categorized Virus

As shown in Table 1 and Figure 1, although similar security problems occurred every year, new malware and attack methods emerged quickly. About 10% of new security problems can not be indentified every year.

On the other hand, virus feature database of antivirus become bigger and bigger. The full installation package of Norton antivirus was about 23 megabytes in size at 2002. The virus database of Norton antivirus became more than 100 megabytes by the year 2012.

Machine learning based method such as frequent pattern recognition [6] had been implemented for security. However, malware and hacking have not stop till now with these methods while the cost of antivirus software was rising steadily.

2.2 Security in Clouds

The core of cloud computing is everything as service. To share computing capability, servers can be divided into virtual machines to run light weighted applications or gathered as a powerful virtual machine to deal with hard problems in IaaS layer. To provide customized platform services, many operation systems can be run on one server in parallel at one server in PaaS layer. To share software as services, platforms can be assigned for various applications on unknown servers.

Cloud architecture break the physical isolation of servers, virus can be more infectious in such architectures. By traditional method, every virtual machine in the cloud should install antivirus software and update operating systems frequently. It is a big cost for light weighted virtual machines. Some works also advanced architecture to enhance the security of cloud computing systems [5], the availability and security can not be ensured with this system.

3. Security and Availability

3.1 Target of Hackers

Although various malicious software and hacking methods have been developed, target of hackers remains the three as shown below.

- Stop or hamper normal applications.
- Get unwarranted information.
- Distort or destroy information in the system.

The first and the third target can seriously hamper the performance of a computer system.

3.2 Write, Execute and Access Control

Control writing and executing priorities can prevent system from being hampered or distorted. Most operation systems control these priorities merely by an authority system. Once the authority system does not work, nothing can be warranted.

A good example for high availability is the computer lab system. Computers in the lab are protected by a recovery card or even boot from the network. Once they are infected, reboot can fully recover the computer.

Effective control of writing and executing authorization can solve most security problems and keep system high available.

4. Secure Architecture

Effective access control should be implemented mainly on hardware infrastructure and operation systems. Categorizing of applications can be helpful to implement a secure environment. Figure 2 shows a secure architecture of IaaS and PaaS for cloud computing systems.

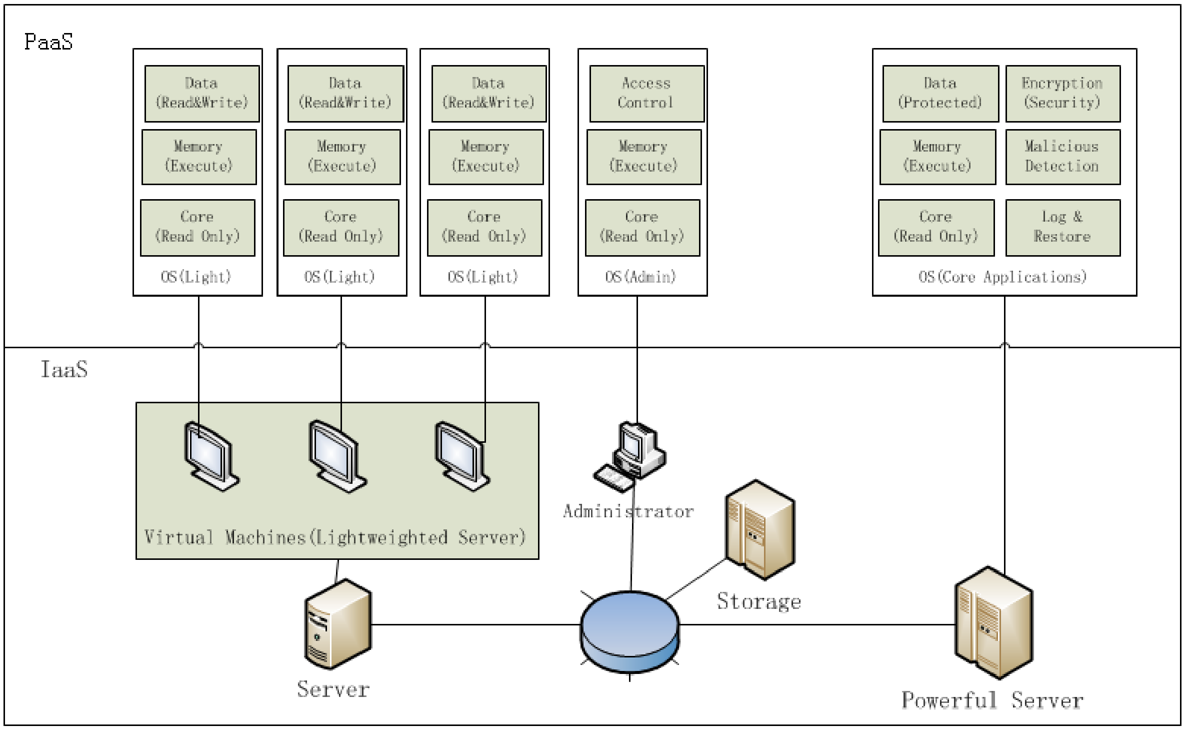

Figure 2. A secure architecture of infrastructure and operating system structure is described in this figure. Categorizing and access control are essence.

Severs and applications are categorized in this architecture. Light weighted services can be implemented on virtual machines divided from servers. Core applications should be run on powerful servers or clusters. The administrator node should be kept in secure environment and implement simple operation system with access control. All platforms in virtual machines should have a read-only core and isolated execution and data section.

4.1 Security and High Availability of Infrastructure as Service

Nowadays, severs are powerful enough to run many instances normal applications such as web service. However, some computations need large amount of resource. Some core applications need high security and computation capability too. Due to the high cost of arrange resource from different servers, powerful and secure servers should be used exclusively for these applications. Administrator node should have read-only storage system and being set in private network or access the cloud without network.

4.2 Secure Platform as Service

Light weighted servers such as web servers need to be stable. Limited executions need to be run at these virtual machines. No special security software should be installed on such operations. Executions should run in the memory. Executions can not take place on data section.

Operation systems for core applications should implement more security components to stop malicious operations such as password stealing.

All operations should have features below.

- Read-only system core.
- Isolation of writing and executing section.
- As simple as needed.

4.3 High Availability and Recoverable Data Management

Although availability of operation system can be preserved by the methods mentioned before, data can be deleted by malicious operations through vulnerabilities of programs. Logs become important for recovery and malicious operation detection at this situation.

Logs should be stored in an append-only system which can not be accessed from the internet. Operations on data of important systems should be recorded as logs which can support recovery.

5. Conclusion

This paper advanced a secure architecture for cloud computing systems. By controlling the writing and executing operations, system can be stable. Advanced availability and security can be further warranted by using simple operating systems. At last, high availability can be provided by full logging. As a conclusion, the architecture can provide high availability and security for cloud computing.

References

[1] H. Gonz´alez-V´elez and M. Kontagora, “Performance evaluation of MapReduce using full virtualisation on a departmental cloud”, Int. J. Appl. Math. Comput. Sci., 21, pp. 275-284 **(2011)**.

[2] Ren Kui, Wang Cong, Wang Qian, “Security Challenges for the Public Cloud”, IEEE INTERNET COMPUTING, 16, pp. 69-73 **(2012)**.

[3] Garber Lee, “Serious Security Flaws Identified in Cloud Systems”, COMPUTER, 44, pp. 21-23 **(2011)**.

[4] Liu QA, “An In-VM Measuring Framework for Increasing Virtual Machine Security in Clouds”, IEEE SECURITY & PRIVACY, 8, pp. 56-62 **(2010)**.

[5] JiangMing, “Virus Early Warning Center”, http://virusinfo.jiangmin.com

[6] Reza Sadoddin and Ali A. Ghorbani, “An incremental frequent structure mining framework for real-time alert correlation”, Computers & Security, 28, pp. 153-173 **(2009)**.

Authors

Xixu Fu

Xixu Fu was born on 1981. He received his bachelor and master degree at 2002 and 2007 respectively. Now he is a PhD candidate in Fudan university as well as a lecturer in Shanghai Ocean University. His research interests include artificial intelligence, system integration and cloud computing.

Kaijun Wu

Kaijun Wu was born on 1969. He is a professor in Shanghai Ocean University. His research interests include software engineering, system integration and cloud computing.

Xizhang Gong

Xizhang Gong was born on 1969. He is an associate professor in Shanghai Ocean University. His research interests include software engineering and system integration.