Security Insurance of Cloud Computing Services through Cross Roads of Human-Immune and Intrusion-Detection Systems

Abstract

- Cloud computing has emerged as a new computer model that aims to provide reliable, customized and dynamic information technology environments oriented towards a better quality of service and availability of infrastructure without much financial burden.

- However, this advanced paradigm has immediately highlighted a serious security problem whose resolution is a real challenge. This challenge is explained by the importance of using services offered by cloud computing in distributed applications and by the interest to fully take advantage of their strengths

- . In this paper, we propose a novel intrusion detection system dedicated to the security of cloud computing resources and services. This system takes advantage from: (*i) the intrusion* detection system paradigm to implement an efficient security system; and (*ii) the integration of human immune techniques, i.e. macrophage, B cells, T cells, and natural killer* cells. The performed experiments show the high performance of our proposed system in terms of detection of novel attacks as well as of good detection rates and low false ones.

Existing system

- memory and computing capabilities of computers and servers around the world linked by a network, the Internet. Users are no longer the owners of their computer servers.

- However, they can access in a scalable manner to a lot of online services without having to manage the underlying infrastructure that is often complex.

Disadvantages

- Cloud computing has emerged as a new computer model that aims to provide reliable, customized and dynamic information technology environments oriented towards a better quality of service and availability of infrastructure without much financial burden.

- However, thisadvanced paradigm has immediately highlighted a serious security problem whose resolution is a real challenge.

Proposed system

➤ In this paper, we investigate another way of tackling the above mentioned troubles within cloud computing security. Thus, we introduce a novel intrusion detection system based on a human immune system for cloud computing services.

➤ It permits simulating the behaviour of a vulnerable cloud service and detecting the captured attacks. The strength of our solution is the data analysis module that we have integrated. In fact, to facilitate the analysis of data, an automatic analysis

Advantages

- A novel intrusion detection system dedicated to the security of cloud computing resources and services. This system takes advantage from: (i) the intrusion detection system paradigm to implement an efficient security system; and (ii) the integration of human immune techniques, cells.

- The performed experiments show the high performance of our proposed system in terms of detection of novel attacks as well as of good detection rates and low false ones.

Hardware Requirements

- Processor   :Intel Pentium IV 1GHz

- RAM   :256MB (Min)

- Hard Drive   :5GB free space

- Monitor   :1024 * 768, High Color inch

- Mouse   :Scroll Mouse(Logitech)

- Keyboard   :104 keys

Software requirements

- OS   :   Windows XP/7/8

- Front End   :   Visual Studio 2010/ netbeans 7.1

- Back End   :   SQL Server 2005/ heidisql 3.2

- Browser   :   Any Web Browser

conclusion

- In this work, we put forward a cloud-computing-based intrusion detection system dedicated to attract some cloud service attacks and discover their characteristics. To avoid the problems encountered when analyzing a great amount of data, we introduce an approach to automatically analyze the data collected from the user's received requests.

- The analysis technique is based on human immune system, and an immune memory. The goal of these techniques is to characterize all types of attacks captured by our cloud-based IDS and detect novel attacks.

- To evaluate the effectiveness of our approach, we have done several tests in order to show the performance and the strengths of our IDS. The experimentation has been also conducted to classify and group the novel attacks of cloud computing services. In the near future, we will use the opportunities offered by deep learning to acquire good knowledge of attack strategies.

References

[1] H. Singh Lamba and G. Singh, (2011). "Cloud Computing- Future Framework for emanagement of NGO's", IJoAT,ISSN 0976-4860, Vol 2, No 3, Department Of Computer Science, Eternal University, Baru Sahib, HP, India.

[2] K. Weins, (2014). "Cloud Computing Trends: 2014 State of the Cloud Survey". Rightscale, 2, 209

[3] N. Thirumoorthy, M. Aramudhan and M. S. Saravanan, (2015). Signature Based Intrusion Detection In Cloud Based Multi-Tenant System Using MTM Algorithm, ARPN Journal of Engineering and Applied Sciences VOL. 10, NO. 14.

[4] S. Sangeetha, R. Ramya, M. K. Dharani, & P. Sathya, (2015). "Signature based semantic intrusion detection system on cloud". In Information Systems Design and Intelligent Applications (pp. 657-666). Springer India.

[5] A. Sari, (2015). "A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications", Journal of Information Security, 6, 142-154