Defensive Security Mechanisms for Cloud Computing Security Risks- A Review

Geethu Krishna[1], Jyothis T. S[2]

[1]PG Student, Department of Computer Science and Engineering,
Jyothi Engineering College, Cheruthuruthy, Kerala, India

[2]Assistant Professor, Department of Computer Science and Engineering,
Jyothi Engineering College, Cheruthuruthy, Kerala, India

Abstract: ***This paper compares various mitigation techniques which are used to reduce the security risks that the cloud computing environment underlying with and as well as the concepts through which these tasks are accomplished. Also analyses whether such defensive security mechanisms can provide an automated defence for both the known and unknown malware security risks in the cloud.***

Keywords: Mitigation techniques, cloud computing, defensive security mechanisms, malware security risks.

1. Introduction

Information Technology is rapidly evolving with the term cloud computing which is well-known in the fast growing IT arena.Even though, there exist various definitions for cloud computing, one of the commonly recognized definition is provided by the National Institute of Standards and Technology (NIST) [1]: Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Despite all of the attention on the added advantage of cloud computing, it is not clear if Cloud will be able to withstand the attack from malware without a significant change to current infrastructure. This paper briefly describes various defensive mechanisms which implement on the cloud in order to mitigate the underlying security risks, which consider as the main threat in cloud computing paradigm. There are various such measures which differs each other based on the concepts with which they are developed. Each has their own advantages and disadvantages. The effective mechanism is used by the most of the cloud based organizations

In this context, it is important to analyse the prevailing security defence mechanisms in the cloud computing arena, so that it is easy to point out the best and the most effective measures for the cloud to overwhelm the malwares. In this paper, some of the works on the security risks mitigation in cloud computing environments are compared. The comparison reveals the fact of the appropriate mechanisms which paves the way for secure cloud.

2. Related Works

The paper compares some of the existing works in the area of cloud computing. These works are mainly implemented to safeguard the cloud from the security threats by means of various defensive mechanisms which encompasses different concepts such as ontologies, intelligent multi agent systems and computational intelligence etc. The mentioned concepts are incorporated to attain automated defence for the malware security risks that may be either known or otherwise unknown. Thus can be able to maintain and improve the interoperability which is necessary to attain international standards which in turn improve the belief of the cloud subscribers on the providers.

A new mechanism was proposed for identifying the intrusions from the distributed architecture and intelligent agents in [2]. This is based on the analysis comprised of two levels which allows eliminating the strong malware attacks and as well as the weak attacks of the intrusions. The solution offered by this work was autonomous and the decision ensures high level of security architecture. The architecture described encompassed by several agents each have different roles and distributed at different network points. These agents make the capabilities responsive to cognitive abilities. It consists of two levels; the first level is based on rules and safety procedures. This approach allows to shape the rules that describe the unintended uses which is relying on past intrusions or known weaknesses. The main advantage of this approach is based on the elimination of the known attacks. The system was established based on the multi-agent aspect.

In spite of the threats in the cyber world, the preservation of the same is one of the inevitable works. This has accomplished by ontological approach in the cloud computing paradigm [3]. A new approach was introduced based on the concept of ontology and through can made some changes in the cloud computing such as data-asset decoupling, composition of multiple resources and external resource usage. These three are the characteristics of cloud computing. The major criterion discussed in this work was to fortify the cloud from the cyber security information risks. The cyber security can be improved and the standard of the cyber operational performance can be achieved by implementing the security measure prescribed in this work.

In the IT fields, computational security is one of the upsetting factors and it can be overcome by implementing a system known as AutoCore [4]. Based on ontology, multi-agent system and intelligent interface, the goal can be achieved. The system consists of an interface, known as Core

Editor and a formal ontology known as CoreSec. The method was mainly developed to maintain the computational security in the corporate world and also to encapsulate the computational resources from the hackers. This proposal was successfully implemented, tested and certified in the real world.

The approach uses two main ideas namely, autonomic computing and ontology. The concept of autonomic computing works on the basis of human autonomic nervous system, which works efficiently and smoothly even without the intervention of any human. This will leave the administrator freely; as self-management is the important boon of the concept autonomic computing which in turn increases the quality of the system by fulfilling services such as self-configuring, self-optimizing, self-healing and self-protecting. Ontologies allow the developers to reuse the knowledge artefacts. The system developed identifies and correct the Denial of Service attacks and such type of attack can be easily identified and difficult to prevent.

Cloud computing paradigm introduces one another system where a defensive security mechanism was introduced [5]. The system established based on the concepts such as computational intelligence, network ontologies and intelligent multi- agent systems. It creates autonomic defence mechanism so that the system can automatically reaches to its defence posture which in turn processes the new data within the cloud. Altogether, the system can tackle the known and unknown security threats through the aforementioned autonomic mechanism.

3. Comparison

The works related to the cloud computing defence mechanisms have discussed in the earlier section. When compared each of them, I can able to understand that each was developed based on some concepts or the combination of those concepts. Each of them has their own advantages and limitations.

The work proposed by DrissRaoui et al. [2] used distributed architecture and intelligent agents for the elimination of stronger as well as the weaker threats. It concentrated on the protection of both strong and weak security attacks. But it can perform this action only on the known attacks. It doesn't gives any information about the elimination of the unknown security malwares. Even though, to some extent it manages the cloud from the security threats, thus can maintain the trust of the cloud users on to the service providers.

But the ontological approach was used by Takeshi Takahashi et al. [3] for the accomplishment of reliable cyber services. Through this work, they aimed a secure cloud which is free from the cyber security information risks. Thus the system attains cyber operational performance.

In recent years, there are some efforts have been spent to maintain computational security in the IT sector. This was accomplished by the work of Ryan Ribeiro de Azevedo et al. [4]. It uses two main concepts such as, autonomic computing and ontology. As incorporating these, the system has certain added services. But this will only detect and prevent one kind of security risk only, namely Denial of Service (DoS) attack. The system specially built in for the above mentioned attack only, cannot detect any other malwares. This is considered to be the curse of the proposed system.

Another work by Steven Mazur et al. [5] developed a system which encompasses three main concepts namely computational intelligence, network ontologies and intelligent multi-agent systems. Since an autonomic defence system was implemented, it can adjust to any changes automatically in the cloud.

Thus the concepts which are discussed in the works related to the cloud security defensive mechanisms have some characteristics and are tabulated in Table 1.

Table 1: Characteristics of the concepts

Type of Classifier	*Generality*	*Distributed*	*Prior Knowledge*
Computational Intelligence	Normal	Possible	Assumption
Ontology	Medium	Possible	Yes
Intelligent Multi-Agents	High	Necessary	Not

The characteristics such as generality, distribution and prior knowledge of the concepts are summarized and tabulated.

4. Conclusion

The comparative study on the defensive security mechanisms of the cloud computing are carried out and also analyses the various concepts behind those works. Each of them has their own merits and demerits. Thus can able to conclude that, by incorporating all the concepts such as computational intelligence, ontologies and intelligent multi-agent systems in an effective manner, then we maintain a secure cloud.

5. Future Enhancement

As future works, most of the cloud based organizations has to understand the ways to maximize the benefits of cloud as well as to reduce the security risks that the cloud computing paradigm faces.Now a day, various contributions are came into being to protect the cloud from the security malware issues. Among them, one of the effective measures was the development of TWAREN [6], which is a distributed platform on the cloud network act as a defender against malicious attacks. It can able to block the incoming threats too, and it mainly back traces the DDos attacks which flows through its entry points.

References

[1] Peter Mell, The NIST Definition of Cloud. Reports on Computer Systems Technology, September 2000
[2] D. Raoui S. Benhadou, H. Medromi, New distributed platform for intrusion detection based on multi-agents system. J of Engg. & Tech. Research vol.2-10), pp.200-206, October 2000.
[3] T. Takahashi, Y. Kadobayashi and H. Fujiwara, "Ontological approach toward cybersecurity in cloud computing," 3rd Int. Conf. on Security of Information

and Networks (SIN 2010), Taganrog, Rostov region, Russia, Sep. 2010.

[4] R. Rebeiro de Azevedo et al, An autonomic ontology based multi-agent system for intrusion detection in computing environments inside computing environments, An International Journal for Infonomics(IJI), vol 3,issue 1, march 2010

[5] Steven Mazur, Erik Blasch, Yu Chen, Victor Skormin, "Mitigating Cloud Computing Security Risks using a Self-Monitoring Defensive Scheme", 2011 IEEE.

[6] Ming-Chang Liang, Meng-Jang Lin, et al, The flow back tracing and DDos defensive mechanism of the TWAREN defender cloud. National center for High Performance Computing, Proceedings of the Asia-Pacific Advanced Network 2013, v.36, p.32-40

Author Profile

Geethu Krishna, received B.Tech degree in Information Technology from Anna University, Tamil Nadu, India in 2011 and she is currently pursuing M.Tech in Jyothi Engineering College, Cheruthuruthy, Thrissur, Kerala, India.

Jyothis T. S, received B. Tech degree in Computer Science from LBS College of Engineering., Kasargod, Kerala and secured MBA from Tamil Nadu College of Engineering., Coimbatore. She has attained M. Tech in Computer Science from PSG college of Technology, Coimbatore and worked as lecturer in College of Applied Sciences, Malappuram, Kerala and University College of Engg., Thodupuzha, Kerala. Currently she is working as Asst. Professor in the Department of Computer Science & Engineering in Jyothi Engineering College, Cheruthuruthy, Kerala, India.