International Journal of Cloud Computing and Services Science (IJ-CLOSER)
Vol.1, No.3, August 2012, pp. 85~89
ISSN: 2089-3337

A Study on Security Threats in Cloud

Hena Shabeeb*, N. Jeyanthi*, N.Ch.S.N. Iyengar**
* School of Inforamtion Technology and Engineering, VIT University, Vellore, TN, India
** School of Computing Science and Engineering, VIT University, Vellore, TN, India

Article Info

Article history:

Received June 20th, 2012
Revised July 15th, 2012
Accepted July 26th, 2012

Keyword:

Cloud Computing
Security issues
Countermeasures

ABSTRACT

Cloud computing is now invading almost all IT industry and has become a rich area of research. It enables the users to share the resources which are done through resource virtualization and they have to pay only for what they use. The new paradigm freed the organizations from the burden of installing and maintaining the expensive and critical software, platform and infrastructure. The only thing they need to see is the Internet enabled systems. As the number of dependents on the cloud services shoots up, the security issue has become an overwhelming problem for cloud service providers. In order to make use of the cloud benefits to full extent, these issues need to be addressed first. This paper presents the major security issues in cloud computing. Some of the countermeasures that can be implemented are also suggested.

Corresponding Author:

Hena Shabeeb,
School of Inforamtion Technology and Engineering,
VIT University, Vellore – 632 014,
Tamilnadu, India
Email: henashabeebvit@gmail.com

1. INTRODUCTION

Cloud computing is the hottest topic of discussion in the IT & research world today. Industrial world is expecting profound miracles to happen with the intervention of cloud services in all spheres of business. It is a new computing model in which resources are pooled to provide software, platform and infrastructure to as many users as possible by sharing the available resources. Figure 1 depicts various deployment models, service models as well as essential characteristics of cloud which are described below:

1.1 Deployment Models:

The cloud can be deployed for private, public, community or uses. Private cloud will be used by an organization and/or its customers, who owns it where as public cloud is made available for public use. Community model is for a community of users having same mission/goal. Hybrid model of cloud shares the properties of any of the above models.

1.2 Delivery Models:

The cloud delivers its services in the form of software, platform and infrastructure. Costly applications like ERP, CRM etc. will be offloaded onto the cloud by provider. They run at providers' cost. Platform includes the languages, libraries etc. The database, operating system, network bandwidth etc. comes under infrastructure.

1.3 Hallmarks of cloud:

The cloud services needn't be paid in advance. It provides services on demand. These services are available on any Internet enabled device having browser software installed in it through the broad network access feature of cloud. The providers pool the resource from various sources and make these services

available. Rapid Elasticity enables the cloud to scale up/down based on the demand. As the cloud is a metered/measured service, the consumers need to be bothered only during the time when bill comes.

Cloud computing is actually a hybrid of various traditional computing techniques like virtualization, distributed computing, load balancing, grid computing, etc. It combines the feature of all these and is evolving as a new model on which everyone can rely for everything. As depicted in the figure 1, cloud has 4 deployment models and 3 delivery models. The most attractive feature of the cloud service is users needn't be bothered at all about the resource management. Provider can do scale up and down the resource from the pool on demand basis. It is a metered service in sense users needn't have to invest huge amount for the resources. They will be charged for what they use. Google Apps, Amazon, Microsoft Azure, etc are some of the popular cloud service providers today. So, security issues have to be dealt with urgently so as to make the global acceptance of cloud computing paradigm.

Like every coin has two sides, though cloud is attracting the world towards it with all these wide flavors of benefits, it has various challenges to overcome also. As the pulse of interest in cloud is increasing among the globe, attackers also found cloud as a best ground for their activities. These attacks will affect the users as well as providers. For users, the impact will be in the form of economic loss. The providers may lose their reputation if they are unable to provide the requested services.The following of this paper is organized as follows: Section 2 discusses various security issues in cloud and section 3 suggests some countermeasures for some of these issues. Section 4 concludes the study.

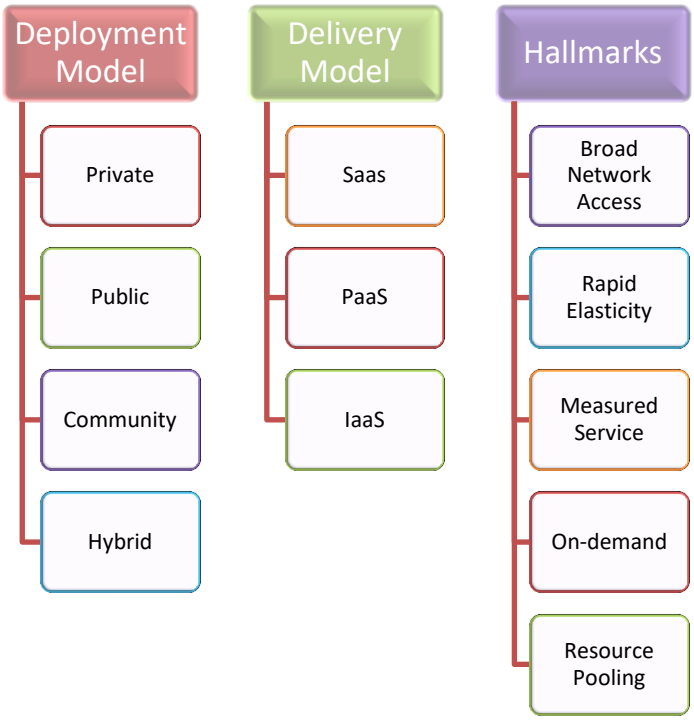

Figure 1. Cloud in Nutshell

2. SECURITY ISSUES IN CLOUD COMPUTING

Trustworthiness of the cloud service provider is the key concern. The organizations are deliberately offloading their sensitive as well as insensitive data to cloud for getting the services. But they are unaware of the location where it is going to be processed or stored. It is possible that the provider shares this information with others or the provider itself uses this for some malicious deeds. The seven famous security issues in cloud computing pointed out by the analyst firm Gartner [7] are:

- Privileged user access
- Regulatory compliance
- Data location
- Data segregation

- Recovery
- Investigative report
- Long term viability

Ziyuan Wang [10] has discussed the key security and privacy issues like access control, authentication and identification, availability, policy integration, audit and so on. The risk of illegal access is higher in cloud as there is no strong access control mechanism. Even confidential data may be accessed illegally when the access control mechanism is not adequate. In a multi-tenant environment like the one which cloud provides, several users will be served by a single entity. Different users will be using different protocols which make it more difficult to provide an interoperable authentication and identification mechanism. Virtualization poses threat to availability of data. For example, if a user has stored some data in storage provided by Amazon EC2 and if the server is down means the data won't be available until the server is up. Different cloud providers follow different security policies. So, integration of these policies is difficult and in a shared environment the probability of security breaches due to this heterogeneity is high. It is required to audit the activities of cloud as users trust the cloud service provider. But, due to the large amount of data stored in cloud it is impossible to audit all data.

John C. Roberts II and Wasim Al-Hamdani [3] has discussed about "wrapper attack" in which the attacker wraps some malicious code in XML signature and injects this signature into the XML codes which is essential in cloud computing for resource sharing. Another issue they have dealt with is flooding attack or DoS (Denial of Service) attack. The cloud works on pay for use basis. If numerous requests are sent to a server on cloud by the DoS attacker, the owner of that particular cloud will be large with huge amounts for processing the requests. Moreover, other users will be denied of the service which they request as the server on cloud is expending all its requests for serving the malicious DoS request. The situation will be more drastic if the attacker compromises some more host for sending the flood requests, which is called Distribute Denial of Service (DDoS). 'Reputation Fate sharing' is another serious issue discussed here. Side Channel attack in which the sharing of hardware resources lead to data leakage from one system to another is also a probing threat. In addition to all these, the user will lose the control over the data once cloud environment is deployed. None can tell where it is going to be processed, how and where it is stored, who can and can't access it and so on.

Dawei Sun et al. [1] has classified the security issues into six categories. The need for monitoring the cloud server, data confidentiality, malicious insiders activities, service hijacking, issues due to multi tenancy and so on are dealt with. Privacy issues like enabling users to have control over data, preventing data loss while replicating etc are also discussed. Various security issues [8] in the different delivery models of cloud threaten the endusers. In Software as a Service (SaaS) model they have quoted various issues like Data confidentiality, Web application security, Data breaches, Virtualization vulnerability, Availability, Backup, Identity management and sign-on process. In Paas, the provider has to make sure that there is no data leakage between applications. In IaaS model, the provider and consumer has to provide different levels of security. D. Zissis, D. Lekkas [2] has addressed various security issues like trust, confidentiality and privacy, integrity and availability. In a cloud environment trustworthiness is a relevant term as data is outsourced out of owner's security boundaries. The data and resources can be compromised as there is high sharing of resources which may affect the confidentiality and privacy of data. Cloud provider need to ensure data as well as software integrity. Cloud services need to be reliable and available always.

Spoofing the IP address of virtual machines [6] is another serious security challenge. The malicious users get the IP address of the virtual machines and implant malicious machines to attack the users of these VMs. This enables hacking and the attackers access can confidential data of users and use it for harmful deeds. As cloud is providing on-demand service and supports multi-tenancy, it is more prone to DDoS attack also. As the attacker goes on flooding the target, the target will invest more and more resources for processing the flood request. After an extent, the provider will go out of resources and can't service even the legitimate users. Unless Data Leakage Prevention (DLP) agents are embedded in cloud, due to multi-tenancy and moving away of data from users control to cloud environment, the problem of data leakage will also be there.

Cloud computing has become a tempting target for cyber crime [4]. The prominent providers like Amazon and Google has mechanisms to defend against this type of attack. But, not all providers do have. A cloud environment consists of numerous heterogeneous entities and the security of such an environment is dependant of the security guaranteed by the weakest entity. Various privacy issues like retention (how long the cloud service provider retains the data), destruction of data (e.g.: cloud service provider retaining copy of sensitive data without fully deleting it) etc [5] is also there. Different countries are coming with different rules, regulations and policies [9]. This causes problems while cross border data transition takes place.

3. SOME COUNTERMEASURES FOR THE SECURITY ISSUES IN CLOUD

As a countermeasure against the trustworthiness of provider, encryption can be suggested. Users have to encrypt the sensitive data before offloading it to cloud for storage purpose. It's high time to develop a uniform standard for security policies and protocol that can be used by all cloud service providers. Denial of Service (DoS) and Distributed Denial of Service (DDoS) can be controlled to a great extend by asking the requestors to solve some puzzle (say, mathematical operations) and distinguish the legitimate users and attackers based on their puzzle solving ability. Honey pots with Intrusion detection system can be another good solution in this regard. Several dummy CSPs can be kept and the attackers'/ legitimate users' request can be first forwarded to these dummies having some intrusion detection mechanism. Thus, only legitimate traffic reaches the cloud and cloud can save a lot of its critical resources and time without being got wasted for attack traffic processing.

4. CONCLUSION AND FUTURE WORK

Cloud computing is evolving as one of the best basement of all industries in the globe. Because of this, it has been attracted by everyone including the attackers. The security and privacy has become the most overwhelming issue that pose major obstacle in the cloud computing scenario. So, these issues have to be addressed as soon as possible to make maximum benefits out of the emerging trend. This paper discussed various security issues in cloud computing and suggested some defense measures for some o f these issues. The paper is expected to be a good guidance for those who works or does research in cloud computing.

From the study, we understood that DDoS attack is the most dangerous ones as the cloud has the property of scaling up when huge amount of request comes. But when the cloud scales up for servicing DDoS attack traffic, it will be a tremendous loss to providers as well as customers. So, as a future work we are planning to do more research on DDoS attack and come up with most effective and profitable solution.

REFERENCES

[1] Dawei Sun, Guiran Chang, Lina Sun and Xingwei Wang, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments", 2011 Published by Elsevier Ltd. Selection and/or peer-review under responsibility of [CEIS 2011], Science Direct, pp. 2852 – 2856.
[2] Dimitrios Zissis, Dimitrios Lekkas, "Addressing cloud computing security issues", Future Generation Computer Systems 28 (2012),Science Direct 2012, pp. 583–592.
[3] John C. Roberts II, Wasim Al-Hamdani, "Who Can You Trust in the Cloud? A Review of Security Issues within Cloud Computing", Information Security Curriculum Development Conference 2011, ACM 2011, pp. 15-19.
[4] John Harauz, Lori M. Kaufman, Bruce Potter, "Data Security in the World of Cloud Computing", IEEE 2009, pp. 61-64.
[5] Kresimir Popovic, Zeljko Hocenski, "Cloud computing security issues and challenges", MIPRO 2010, pp.344-349.
[6] Farzad Sabahi, "Cloud Computing Security Threats and Responses", IEEE 2011, pp.245-249.
[7] http://www.networkworld.com/news/2008/070208-cloud.html
[8] S. Subashini n, V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, Science Direct , 2011,pp.1-11.
[9] Zaigham Mahmood, "Data Location and Security Issues in Cloud Computing", 2011 International Conference on Emerging Intelligent Data and Web Technologies, IEEE 2011, pp.49-54.
[10] Ziyuan Wang, "Security and privacy issues within the Cloud Computing", 2011 International Conference on Computational and Information Sciences, IEEE 2011, pp.175-178.

BIOGRAPHY OF AUTHORS

Hena Shabeeb is pursuing her M.Tech. with Software Technology as specialization in VIT University, Vellore, Tamilnadu, India. She received her B.tech in Computer Science and Engineering from Cochin Univerisity of Science & Technology in 2011. Her are of interest is on Network Security, Web Application Development.

Prof. N Jeyanthi is a faculty cum Research Scholar in VIT University. She received her M.Tech in Information Technology with Networking as Specialization from VIT University, India in 2006 and B.E. in Computer Science and Engineering from Madurai Kamaraj University, Madurai, India in 1999. Her current research interest is on Network Security in Real-Time applications. She is a life member of Indian Society of Technical Education.

Dr.N.Ch.Sriman Narayana Iyengar received M.Sc (Applied Mathematics) & PhD (Applied Mathematics) from Regional Engineering College Warangal (Presently known as NIT Warangal), Kakatiya University, Andhra Pradesh, India, & M.E. (Computer Science and Engineering) from Anna University, Chennai, India. Currently he is Director of Periyar EVR Central library and also Senior Professor at the School of Computing Science and Engineering at VIT University, Vellore, Tamilnadu, India which is the world's one of the best premier Technical Educational Institution. He had 26 years of teaching and research experience. His research interests include Agent based Secured Applications, Data Privacy, Information security, Mobile Commerce, Cryptography, Intelligent Computing, and Fluid Dynamics (Porous Media),

He got best research contribution award in 2009, best active research award in 2008 and Best teacher award in 2004 by VIT University. Dr.Iyengar chaired many International Conferences, delivered Key note/ Invited/Guest/Technical lectures being International Programme committee member and had a credit of nearly 167 publications in reputed International Journals & IEEE Conferences. He has authored/co-authored several textbooks/learning materials for the student community. He is an Editor in Chief for International Journal of Software Engineering and Applications(IJSEA) of AIRCC and Editorial Board member for many International Journals like IJConvC (Inderscience -China), IJCA (USA),IJAST(SERSC-Korea) etc.,