International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 2 No. 2 Jun. 2014, pp. 308-312
© 2014 Innovative Space of Scientific Research Journals
http://www.ijisr.issr-journals.org/

Analysis of Cloud Computing Vulnerabilities

***Masudur Rahman*[1] *and Wah Man Cheung*[1-3]**

[1]Faculty of Business and Services,
Colchester Institute, United Kingdom

[2]Faculty of Business and Services,
Colchester Institute, United Kingdom,

[3]School of Computer Science and Electronic Engineering,
University of Essex, United Kingdom

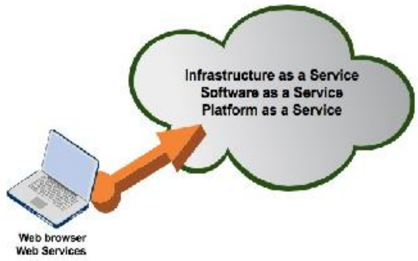
ABSTRACT: Cloud computing is one of the most emerging networking technology, which has been considered as significantly effective among different types of users. Using cloud computing can be cost effective and organisation can focus more on their unique business idea instead of IT infrastructure or developing software, if they use IaaS or SaaS according to the business needs. However, there are issues with security of critical business data that is stored on cloud service provider's server. There are many concerns in regards to cloud computing security, which have many vulnerabilities and threats. In our previous paper, we have investigated security issues for cloud computing environment, where we have revealed the lack of awareness of cloud service providers to ensure the security. In this paper we have discussed about more threats and vulnerabilities of cloud computing, which cover some of the technical aspects of this burning issue. We would like to propose a cost effective and efficient security model for cloud computing environment after identifying the security risks involved in this sector of modern computing.

KEYWORDS: Cloud computing security, vulnerability of SaaS and PaaS, DoS and DDoS attack, authentication attack, cloud malware injection, metadata-spoofing attack.

Introduction: Gertner[1] study described cloud computing as one of the top 10 latest communication technologies, which is expected to have better prospects in coming years. They have described both personal cloud and cloud computing as top 10 strategic technology trends. Main concept of cloud computing is to reduce the processing burden from client end by improving the ability of "cloud". Cloud computing would encourage to use client's terminal as simple input output device and provide required services on-demand. There are many reasons why consumers have considered cloud computing very useful and fit for purpose. One of the key feature offered by cloud computing is flexibility of resources. Instead of paying significant amount of money in advance, customer can have processing power or storage capacity for exactly what they need; which can be increased at any time in future. Small business found this feature very useful along with the idea of paying only for their usage, which helps them to concentrate and invest more on their core business functions rather than IT infrastructure. Organisation can enjoy the flexibility of "not saving" upfront to buy expensive computing equipment. Cloud is offering range of different types of services, which includes storage, readymade and customisable software, IT platform for software development and use, processing power, applications, database or even virtual private computer according to needs. The consumers have hugely accepted SaaS, IaaS and PaaS in past years. Key advantages of using cloud are on-demand service, reduced upfront cost and maintenance cost, less maintenance responsibility, reduced risk, easier disaster recovery business continuity, efficient backup system etc.

Corresponding Author: Masudur Rahman (Masudur.rahman@colchester.ac.uk)

Shailza[2] has explained that structure of cloud computing that includes service model and deployment model. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) are the example of cloud computing service model. Virtualisation is the key technology used by cloud service providers to offer these services. Cloud infrastructure and platforms are heavily depends on virtualisation, where different virtual machines may use same sets of hardware resources. According to Shailza[2], there can be three different cloud computing deployment models. Deployment model includes "public cloud" where number of customers' share same computing resources provided by cloud service provider, user will pay only for their use. This model is mainly on-demand service model. "Private cloud" is another type of cloud deployment model, where resources are used by a private organisation. Whether it is SaaS, PaaS or IaaS, cloud service will be used by using web browser or web service, where each of these media has different set vulnerabilities. Furthermore, each of these model of cloud computing are vulnerable to different security threats as well.

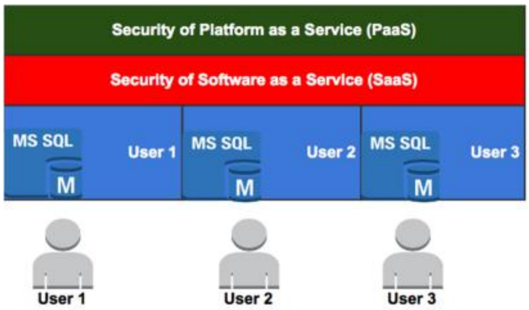


We have investigated about cloud computing security risks in our previous paper[3], where we have revealed number of critical threats for cloud computing environment, mainly the lack of awareness within cloud service providers to ensure the security of data. In this paper, we will be investigating about recent threats to cloud environment that focus on different technical aspects of security risks. The threats we will be discussing in this paper, will cover all of these different models of cloud structure.

Different types of cloud services are closely coupled or interlinked in many cases. For example PaaS and SaaS may be hosted on IaaS. Therefore, any security breach to IaaS will make the PaaS and SaaS vulnerable or other way around. Furthermore, SaaS can be hosted on other provider's PaaS, which also can be hosted on different provider's IaaS by renting the structure. In case of any security incident within any of these services, it will become very complicated to decide the responsibility as well as respond efficiently to resolve the issue [4].

Customers, who use SaaS, have minimum control in regards to security over this type of cloud service; therefore service providers are more responsible to ensure the security. However, as we have discussed in previous paper[3], significant number of cloud service providers are interested in providing different useful services rather than investing more to ensure the security. One of the key vulnerability for SaaS is the security of application, which allows user to use this service. Open Web Application Security Project (OWASP) has described top 10 threats for web applications, which is applicable for SaaS. Significant number of cloud service providers releases an application to use cloud services without effective penetration testing of the application, which makes whole SaaS vulnerable.

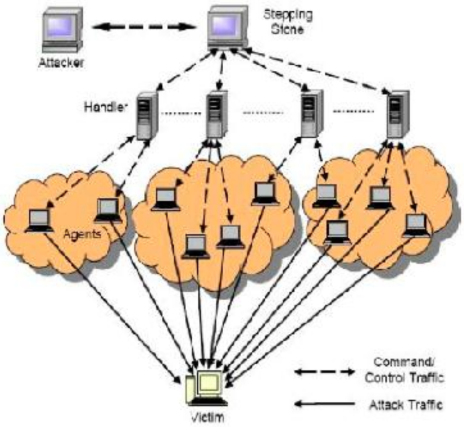
Multi-tenancy approach of hosting SaaS can also raise security concerns of data leakage. In this cloud architecture, service provider has different instances for individual customer but used the same application code. More likely, different customer's data will be stored on same database server; therefore risks of data leakage between these tenants are high[4]. Gartner[1] has found that virtually all the cloud service providers are offering secure socket layer to ensure the security and integrity of the data while transferring between different nodes. However, the security challenges remain while it comes to data storage within shared cloud service environment as many providers do not have encryption technology embedded to store user data into their server.


Security of Platform as a Service (PaaS)
Security of Software as a Service (SaaS)
MS SQL
M
User 1
MS SQL
M
User 2
MS SQL
M
User 3
User 1
User 2
User 3

Platform as a Service (PaaS) provides the facility to develop or host a software without investing excessive amount of money to have hardware and software. Security of PaaS depends on data transfer security as well as the application security. PaaS also needs to have effective security system while data been stored of cloud provider's server. To ensure the security of data transfer, it is crucial to secure the network. Suitable encryption method should be used for data transfer. However, the challenges to ensure the security remain with customer's application instances and security of PaaS itself.

Infrastructure as a Service (IaaS) heavily depends on virtualisation technology, which offers consumers to use scalable computing power or storage capacity. Cloud service providers offer certain resource, which in their resource pool, by using server virtualisation technology. IaaS offer more control to the end users. However, it is also important that the IaaS itself is secured. VM Hopping and VM Escape are two common threats to virtualisation techniques[3]. Strong authentication technique can offer better security to IaaS along with data encryption technology within data storage.

In next section, we will discuss about some critical threats to cloud service environment, which is applicable for any of these cloud architecture explained above.



Denial of Service (DoS) / Distributed Denial of Service (DDoS) / Flooding Attack is one of the biggest security risks for cloud computing as like any other internet based service, where the availability of the data or service can go down because of high volume of traffic to the server. Normally attacker sends large amount of data packets, which can be simple TCP/ UDP or any other type of data. Target of any of these attacks is to negatively affect the availability of service for legitimate users by overloading server's capacity and bandwidth. "Buffer overflow attack" works on similar principle like DoS attack, where large amount of data, which exits the buffer size of a system, will be given to the service provider's system to process. This attack may cause Denial of Service (DoS). Furthermore, distributed denial of service (DDoS) attack is more dangerous for cloud computing, because of its distinctive nature of source of the attack. DDoS use hundreds of different computers, which are known as "bot", to attack on server. The nature of this type of attack make it complicated to protect the server against DDoS attack while the attacker uses different types of data packets. DDoS bandwidth attack can take place by using TCP SYN flood, ICMP or UDP flood; which will overload the allocated bandwidth of service provider so that legitimate customers will not be able to access their services. Smurf attack, Ping of Death attack, TearDrop or Land attack are some common ways to attacking cloud computing environment, all of these will cause denial of service to genuine user if successful. DoS or DDoS attack can take place against any SaaS, PaaS, IaaS, private cloud or public cloud environment.

Authentication Attacks: Regardless of architecture of cloud environment, all cloud service providers will use types of authentication system to give access to the service, which may include “something a person knows” , “something a person has” and “something a person are”. However, most of the SaaS, PaaS and IaaS environment use the authentication method, where a person will know “something” such as username and password. Vulnerabilities in authentication process is one of the common target for attacker specially the one which does not have effective encryption system. There are very small numbers of service providers who offer cloud service based on “two factors authentication method” with encryption technology enabled.

Cloud Malware Injection Attack is one of the critical attacks on cloud computing environment, which is complicated to detect. Attackers use this method to inject malicious code or applications to one of the user instances, which is running on any SaaS, PaaS or IaaS architecture. When this specific instance starts running on cloud server, the only check take place is whether that instance is authorised to run certain services or not. In general, cloud server does not check the integrity of individual instances before running. If successful, attacker gets the opportunity to eavesdrop on other services and data on that server. This type of injection of malware in particular instances, therefore the cloud server, can create serious security concerns such as server deadlock, denial of service or loss of data within any type of cloud computing architecture. This can raise massive security issue within multi-tenant Software as a Service (SaaS) architecture[7].

Metadata Spoofing Attack: Metadata of cloud service will provide the information for the user about different services including location of different network components, format of data or security requirements. Attackers try to modify the information in server’s metadata so that user can be redirected to different place, which is similar to the concept of DNS poisoning[9]. Following steps can be used for metadata spoofing attack:

Web Services Description Language (WSDL) is XML based widely used language that has been used by many service providers to describe the functionalities offered by particular web service. With this type of attack, attacker will change information within WSDL, which will take place as man-in-middle attack. It is possible to change endpoint URL, change message schema, add or modify WSDL security policy, eavesdropping, change cryptographic algorithm or running batch commands to execute certain operations. As the Cloud system itself has kind of WSDL repository functionality, new users most assumably will gather information for a service’s WSDL file more dynamically. Thus, the potential spread of the malicious WSDL file and thus the probability for a successful attack rises by far[10].

Session Hijacking and Session Riding: Attacker can hijack a valid session key from authenticated user to access certain cloud service, which is capable of performing variety of malicious activities. Session hijacking can take place through browsers or application system’s vulnerability. When attacker sends commands to cloud based web application on behalf of legitimate users. Session riding can cause user data deletion, sending spam or performing online transection etc[12].

Strong authentication system can help cloud service providers to provide efficient security against these types of attack. Strong hashing and digital signature can protect the organisation data against metadata spoofing and cloud malware spoofing. However, it is important to adopt different strategies and technologies to protect cloud services from DoS or DDoS attack, what we will be discussing in next paper. Application system’s vulnerability is one of the biggest concerns for service providers, where authentication plays significant role with “single sign on (SSO)” architecture.

We have discussed about different critical security concerns of using cloud computing. One of the key security issues in cloud environment is “authentication system”. In our next paper, we will be investigating potential method of authentication by using cost-effective hardware cryptographic system, which will allow end users to encrypt their data while using cloud based services.

REFERENCES

[1] Gartner Identifies the Top 10 Strategic Technology Trends for 2013.
Available at http://www.gartner.com/newsroom/id/2209615, accessed at 20th March 2014

[2] Cloud Computing Security Issue: Survey, Shailza Kamal, Rajpreet Kaur

[3] M. Rahman, P. Chaung, Cloud Computing, Security Issues and Potential Solution by Using ICMetrics or Biometrics Based Encryption

[4] An analysis of security issues for cloud computing, K. Hashizume, D. G. Rosado, E. Fernandez-Medina and E B Fernandez

[5] OWASP top 10 project, available at https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project, accessed at 25th March 2014

[6] Securing Cloud Servers against Flooding Based DDoS Attacks, Niraj Suresh Katkamwa1, Atharva Girish Puranik and Purva Deshpande

[7] Security Attacks and Solutions in Clouds, Kazi Zunnurhain and Susan V. Vrbsky

[8] Data Storage Security in Cloud using Metadata, R. Anitha, P.Pradeepan, P.Yogesh and Saswati Mukherjee

[9] M. Jensen, N. Gruschka, and R. Herkenhöner, “A survey of attacks on web services,” Computer Science- Research, vol. 24, no. 4, 2009.

[10] On Technical Security Issues in Cloud Computing, Meiko Jensen, Jo ̈rg Schwenk, Nils Gruschka, Luigi Lo Iacono

[11] L. Clement, A. Hately, C. von Riegen, and T. Rogers, “UDDI Version 3.0.2,” OASIS UDDI Spec Technical Committee Draft, 2004.

[12] Preliminary Analysis of Cloud Computing Vulnerabilities, Dr. Sunil Batra and Anju Chhibber