ISSN 2348 – 9928
IJAICT Volume 2, Issue 12, December 2015 Doi:01.0401/ijaict.2014.04.05 Published on 05 (12) 2015

SECURITY MEASURES IN CLOUD COMPUTING AN EXTENSIVE ASSESSMENT

Mr. M. Newlin Rajkumar ***Dr. V. Venkatesakumar***
Assistant Professor,
Department of Computer Science and Engineering,
Anna university Regional Centre,
Coimbatore, Tamilnadu, India

Mr. T. Mahadevan ***Mr. C. Chatrapathi***
PG Scholar,
Department of Computer Science and Engineering,
Anna university Regional Centre,
Coimbatore, Tamilnadu, India

Abstract— Cloud computing is a technology that is emerging and developing at a greater scale from the day it comes into existence. It is widely adopted by various organizations and by governments. Cloud computing has also received major attention among researchers. Large number of researcher re going on in the fields of cloud. Security in cloud computing is one of the major issues in the perspective of both research and organization. In this paper, we presented the in depth survey on security of cloud. Our work contains a detailed study about threats, vulnerabilities, attack and intrusions on a cloud.

Keywords— Cloud Computing, Intrusion, Attacks, Threats, Vulnerabilities.

I. INTRODUCTION

Cloud computing brings the long term vision of computing as service in reality. Cloud provide computation related services and resources to user. According to [1] cloud computing is one of the technology among top 10 technology that is useful and brings success and profit to organizations.

The high impact of the cloud computing is due to its pay as you use [2] characteristics. It frees the user from the burden of investing a huge amount of money in deploying infrastructure for storage and processing. Cloud also provide secure, flexible services to its user. Cloud also has several advantages like availability and the ability to handle demand variations of the user, Cost reduction and high computation power and so on.

The recent development in high speed network and ubiquitous internet processing helps in realizing cloud in reality. It allows user to use a cloud service without knowing much about how and where computation is carried out. Even though cloud computing has huge impact on organizations. Still organizations are little concern about using cloud due to its security issue.

According to the International Data Corporation (IDC) [3] security is the major issue of cloud computing before going to study deeply about cloud security. It is important to understand major stakeholders [4] of cloud computing. They are:

Cloud service provider: It is the organization or company that has data center and server that provides services to its clients.

Client/owner: It may be individual or organization that is getting service from the CSP. The client may use the cloud to store their data or run their application, etc..

User: It is individuals who registered with clients who can able to access his data stored in the cloud.

Also cloud security attack can be classified into two major categories.

Internal attack: Cloud Service Provider may himself compromise and leak clients confidential data.

External attack: An unauthorized person may try to access the clients confidential data.

Traditional security mechanisms can't be applied to cloud environments since user are not having direct control over their data, It is difficult to impose security in the cloud. Verification and authorization process are carried out by the CSP. It arises question about privacy of data. Also, some providers may outsource their security functions to third part it also creates new security risks.

Availability is also a big concern in cloud computing. Even some of the famous service providers also faces this problem of availability. Even the few hours lack of availability can able to cause a big loss in terms of finance and asserts for both cloud service providers and clients.

Several papers have provided in depth survey about security issues of cloud. In our work we try to provide a detailed survey about various security risks in the different security model along with we provide survey about threats and vulnerability in cloud environments with possible countermeasures for handling threats and vulnerability. We also extend our work to various types of intrusion and intrusion detection techniques.

ISSN 2348 – 9928
Doi:01.0401/ijaict.2014.04.05 Published on 05 (12) 2015

II. SECURITY ISSUE IN SPI MODEL

There are three basic delivery model in cloud computing. They are known as SaaS, PaaS, IaaS (SPI) based on the type of service that model provides. Characteristics of each service differs from one another and have its own and unique security challenges. Sometimes the integration of these services many leads to a new kind of security challenges. Since user perceive cloud service as the SPI model it is important to understand the security challenges in this aspect.

TABLE 1 : Security Issue In Spi Model

	Application Security	Multi-tenancy	Data security	Development Life cycle	Infra-structure security	Hypervisor security	Shared memory	VM rollback	Virtual network
SaaS	✓	✓	✓						
PaaS		✓	✓	✓	✓				
IaaS		✓	✓	✓	✓	✓	✓	✓	✓

In order to understand the security issues in SPI model it is mandatory to get a clear understanding on the way each model interact with one another and dependencies among them. Among these three model IaaS is the basic and lower layer above which PaaS are built. Similarly PaaS provides a platform to build and run software service provided by SaaS. Hence, any attack on IaaS can directly impact both PaaS and IaaS. Similarly PaaS has a direct impact on SaaS. Each model has some unique challenges to face, but also they share some common challenges that they needed to face. Sometimes different providers may interact with each other to serve client needs. In such case each provider should take care of the security of their services.

2.1 Software as a service

Compare to other service model SaaS offers less security control to the user. This model provides software service like E-mail, business app like ERP and CPM and conferencing applications to users based on their demand.

- ***Application Security***

Security challenges for application provided by SaaS model is very similar to challenges faced by web application, but the traditional solution for web application are insufficient to handle attacks on SaaS. Since cloud provides application service via internet. Hence attacker may make use of internet and exploit its vulnerabilities to attack SaaS.

- ***Multi-Tenancy***

SaaS has three types of maturity model each having its own challenges. In first one, each customer is provided with individual, unique or customize instance of software. The second model is similar to first in the sense that each user is individual instance, but all instances will have the similar applica code. Third model all users use a single instance of the application [5], it have several advantages like effective resource sharing but also has limitations like scalability. Since information of all users shares single database to store their data. There is high possibility of data leakage. Several techniques are proposed to handle this problem.

- ***Data Security***

The biggest challenge in cloud environment is data security. Unlike traditional computation, in cloud user data is managed by the SaaS service provider in most of the time, hence the user has to be depends on the cloud service provider in a SaaS model. Also service provider may outsource security related services to a third party. It also increases risk of data security in a cloud environment. To maintain robustness, data backup becomes mandatory, but also creates new challenges.

- ***Platform as a Service***

The PaaS allows the user to deploy their application in cloud without having to buy and maintain underlying platform requirement. PaaS not only need to secure the PaaS platform, but also it need to ensure the security of the software provided by SaaS that is deployed over PaaS.

- ***Development Lifecycle***

Since applications are deployed on a PaaS platform it creates an extra burden on developers. They should have proper knowledge about data legal agreement, i.e., where to store data. It is important that copy of data should not be stored in inappropriate places. Also software development lifecycle should be flexible in order to synchronize with the speed with which application will update in the cloud.

- ***Infrastructure Security***

In PaaS most of the security of the application is controlled by developers. But the security of underlying platform on which their software going to deploy is not in their control, also they are uncertain about security of development tool provided by

ISSN 2348 – 9928
Doi:01.0401/ijaict.2014.04.05 Published on 05 (12) 2015

PaaS provider. There is only very few literature the security issue of the PaaS.

2.2 Infrastructure as a Service

IaaS provides storage, network and other resource as a service to the clients. Comparing to other two models user has greater security control over their application security. Even the control of whole software resides with users, security of underlying storage and other resources are still with provider only.

- ***Hypervisor Security***

Hypervisors are used to control virtual machines. It is also called a virtual machine monitor. If an attacker compromise a hypervisor then he/she can able to access all underlying VMs. The Hypervisor is actually a software that controls VM. Hypervisor should be simple so that it has the minimum possibility of risk. For load balancing VMs may migrate between servers. This migration is carried over the internet. This also exposes a weak link since expose content to network.

- ***Shared Resource***

With the help of hypervisor single server can handle large number VMs. These VMs in same server shares memory and other resources. Hence a malicious VM can obtain information about other VMs without knowledge of the hypervisor. Also, according to [6] with help of covert channels all the security rules by bypassed by the VMs.

- ***Virtual Machine Roll Back***

In order to handle error all the VMs are having the capabilities of rollback to the previous state. It creates the new risk like re-enable disabled accounts and re-storing previous passwords. Also for supporting rollback, we create the state of VM as a snapshot. It also creates new vulnerability.

- ***Virtual Network***

For efficient resource allocation network components are shared among multiple users. Hence attackers can able to attack VMs of others who sharing resources with him. With increased VM interconnection risk of vulnerability increases. In general, most hypervisor communicate with VM using the VM network. Hence attacks like spoofing and sniffing.

III. THREATS AND VULNERABILITIES

Cloud computing is developed from some of the existing technologies like virtualization, distributed computing and web services. Threats and vulnerabilities associated with these technologies also directly affect cloud computing. Separation of data, resource, computing platforms and other computational element from direct control of the user also creates new threats and vulnerabilities. In general vulnerability arises due to following reason.

According to [7] improper recruitment of employee is the main cause for inside attack. Cloud service providers have to be very careful in hiring process. Since high privileged employee like administrator has lots of security rights. If he becomes disloyal to his company it lead to a big loss to the service provider.

Improper customer screening also one of the major vulnerabilities. Currently, most of the cloud service providers won't care about the background of their customer. Any person can easily register, pay and open account with them. Hence an attacker can easily become part of the cloud and do some malicious activity.

According to [8] lack of proper knowledge is also a vulnerability. Security of cloud environment is very sensitive because of the wide variety of attacks, threats and vulnerabilities of cloud, but most of the users are not aware of security issues of cloud. It is the main cause for the most of the attacks in the cloud.

In this section we try to relate threats and vulnerabilities with possible counter measures.

3.1 Account Hijacking

An attacker can try to get access to the legitimate user account to access his cloud resource.

Vulnerability: Cloud uses API provides services to its user. Hence, any vulnerability in interface compromises its security. Improper authentication and improper data validation and weak credentials are the basic vulnerability to this attack.

Threat: Social engineering is basic techniques used by an attacker to get access to user account.

Solution: Identity management techniques and dynamic credentials are the solution for this atack. Cloud Security Alliance Provides [9] set of guidelines and recommendation that needed to be performed in order to preserve the privacy of the user. Dynamic credential [10] is another technique to preserve user credentials. In this scheme credentials will chance with user location or after the threshold time or data packet.

ISSN 2348 – 9928
Doi:01.0401/ijaict.2014.04.05 Published on 05 (12) 2015

3.2 Data Scavenging

In cloud mostly data's are shared among multiple user, hence it is sometimes not possible to remove completely.

Vulnerability: In some case separation among user's data are not properly done and also there may be incomplete data deletion.

Threat: Due to the development of many effective data recovery. Software attacker can easily recover deleted data.

Solution: It is necessary to have sufficient data destruction techniques in SLA.

3.3 Data Leakage

An attacker can obtain user's confidential information from VMs that are under the control of the same hypervisor in a single server.

Vulnerability: Third party that performs data backup may leak data; uncontrolled data allocation and data migration in a VM is main vulnerability data leakage.

Threat: During data transmission, storage and processing there is the possibility that an attacker may get data.

Solution: Fragmentation [11] is one of the solution for data leakage. In this method confidential data is fragmented into many fragments with no useful data in single fragment and stored at different locations. Also, we can protect the data with digital signature [12] with the help of RSA algorithm. Homomorphic encryption is also used to handle this attack. In traditional encryption technologies, data is encrypted before it being transmitted and at the receiver end transmitted data has to be decrypted, but homomorphic encryption allows user to perform action on encrypted data itself. But currently this technique is in very early stage and it can perform only addition and multiplication function on the data.

3.4 Denial Of Service

Since the cloud is on demand service, availability is very important criteria for its quality of service (QOS), any issue regarding availability directly affect service provider.

Vulnerability: Over provisioning may occur due to an improper resource allocation policy which may lead to resource over blocking.

Threat: If an attacker can able to request and get a large volume of resources. Then the attacker can block services for authenticated users.

Solution: Cloud service provider should have a strict policy that allows only limited resource allocation to only legitimate user based on his demand.

3.5 Malicious VM Creation

If there is no proper screening of customer then the attacker can register and become legitimate user. Thus he gets separate VM in which he can append malicious code and perform the attack.

Vulnerability: If the placement of VM in repository properly controlled, then malicious VM can access the data of other VMs.

Threat: An attacker can create trojan and deploy it on the server easily if he is able to register and become legitimate user.

Solution: Some solution like a mirage [13] can be used to solve this issue. It uses a filter to scan all the user data for malware. But this scheme also has some severe disadvantage like it may not able to identify all the malware are this scheme need to scan data this raise a privacy issue.

3.6 Data Manipulation

There is a possibility of attacker to perform attacks like SQL injection and cross-site scripting.

Vulnerability: If the interface that provide service to the user is insecure then attacker may exploit its weakness.

Threat: If the user may manipulate the data sent to the application server in order to perform malicious activity Eg: SQL injection.

Solution: Web application is the primary victim of this attack some solution like web application scanner [14] and web application firewall can be used to protect cloud from that threat.

IV. INTRUSIONS IN CLOUD ENVIRONMENT

According to [15] survey intrusion detection is a very important issue than data security. Detecting intrusion is a very important aspect in the cloud. Since as early as instruction are detected amount of damaged varied by the attacker will be minimized. Hence it is very important to understand intrusion and intrusion detection techniques in the cloud. This section provides reviews about intrusion in the cloud.

ISSN 2348 – 9928
Doi:01.0401/ijaict.2014.04.05 Published on 05 (12) 2015

4.1 Intrution Types

- ***Insider Attack***

One of the major security concerns for cloud service provider is preventing insider attack. Since these attacks are performed by their own employee. They know security policies of the company well, also they have special privilege. These kind of intrusion are harder to detect and prevent. If these attacks are performed, then it affects the organization severely.

- ***Flooding Attack***

This attack targets availability of service provided by the service. In this attack, attacker launches a large number of requests to cloud from a large set of compromised zombie system. By attacking a cloud service providing a particular server, it is possible to block the service for a certain period of time. Since availability relates with QoS and also with SLA. It makes a very hard impact on the provider.

- ***User To Root Attack***

In this attack, the attacker tries to get access to a legitimate user account. Attacker achieves this using phishing attack key logger or social engineering. Once, if he gets access to a particular VM of a legitimate user. The attacker tries to exploit vulnerability in the cloud to get access to the root or server.

- ***Attack On Virtual Machine***

Since single cloud server runs multiple VMs which are controlled by the hypervisor. If an attacker is able to compromise hypervisor then he is able to compromise all VM in the server. Some of the attacks are use zero day vulnerability to attack VM.

4.2 Detection Techniques

- ***Signature Based Detection***

This method is based on the pattern of usage of the legitimate user. In this scheme security rules are derived based on user patterns. These are used to detect intrusion with high level of accuracy and with minimal effort. It is very easy and rules can easily upgraded. But if different in pattern between user and intruder are less than it is difficult to identify intrusion with this technique also identify only known attacks.

- ***Artificial Neural Network Based***

In some case we don't have efficient amount of data to classify patterns of legitimate user and intruder. In such case we can use ANN to distinguish between pattern with incomplete data. The accuracy of this scheme depends on the data set used for ANN. In general back propagation multilayer perception, multilayer feed forward neural network is used.

- ***Fuzzy Logic Based***

If the data set is incomplete and are we don't know the exact pattern of intrusion, then it is useful to apply fuzzy logic to identify intrusion. Also, using fuzzy logic with ANN [16] reduces the time required to train neutral network also detect the unknown attack easily and quick. Several techniques proposed general rule set and apply fuzzy logic in intrusion detection in the cloud.

- ***Association Rule Based***

Sometimes intrusions are not exactly based on the known pattern, but they may be in the form of variations of known patterns. In such case apriori algorithm are used which are able to find these variables in attack pattern.

Initially proposed solutions [17,18] consumes large amount of data since they are data mining technique which scans the entire database for creating signatures. Later [19] proposed an apriori algorithm having a length decreasing ability which faster than older algorithm and can used in real time.

- ***Genetic Algorithm***

A genetic algorithm is used in the cloud intrusion system to increase the accuracy of detection in the cloud. Intrusion detection accuracy depends on the optimal selection of appropriate parameter. GA are used for this purpose of selection.

Several features like source port and IP, destination port and IP duration, attack name protocol are proposed [20]. This approach is simple and effective but has a best fit problem. Xiao et al [21] proposed GA based approach, but it won't cover complete feature of intrusion detection.

Dhanalakshmi and Ramesh Babu [22] propose a technique of combining both fuzzy and GA. This eliminates best fit problem and increases the efficiency of the intrusion detection system.combination of these approaches also reduce training time

- ***Hybrid Techniques***

By combining different techniques of IDS we can generate a new technique with the combined advantages of that technique. These kind of IDS is called Hybrid techniques.

A soft computing techniques are highly used by IDS to improve it, but soft computing techniques have both advantages and disadvantages. For eg: ANN takes large learning time, also it is less flexible. GA is good for selecting parameters also it has good efficiency, but in a specific manner based on selected parameters. Fuzzy logic can be used

ISSN 2348 – 9928
Doi:01.0401/ijaict.2014.04.05 Published on 05 (12) 2015

to improve flexibility if it combines with determining technique. Similarly fuzzy can improve efficiency when used with the GA.

V. CONCLUSION

Cloud computing is deployed widely by many major organizations also. It is expected to grow higher in future. Due to its wide adoption any security breach in cloud security will affect service provider and its clients badly. Hence it is important for the client to understand security issues in cloud so as to identify their vulnerabilities and protect themselves from the attacks. In this paper we did a deep survey on various threats, vulnerability and attacks also we briefly discussed about intrusion detection.

References

[1] Gartner Inc Gartner identifies the Top 10 strategic technologies for 2011. Online. Available: http:// www.gartner.com /it/page.jsp? id =1454221. Accessed: 15-Jul-2011

[2] Md. Tanzim Khorshed, A.B.M. Shawkat Ali, Saleh A. Wasimi, "A Survey on gaps, threat remediation and some thoughts for proactive attack detection in cloud computing", Future Generation Computer Systems 28 (2012)833-851.

[3] Gens F, NewIDCITCloudServiceSurvey: TopBenefitsandChallenges, IDC Exchange, /http://blogs.idc.com/ie/?p=730S; 2009.

[4] Sandeep K. Sood,"A Combined approach to ensure data security in cloud computing", Journal of Network and Computer Application 35 (2012) 1831-1838.

[5] Chong F, Carraro G, Wolter R (2006) Multi-tenant data architecture. Online. Available: http://msdn.microsoft.com/en-us/library/aa479086.aspx. Accessed: 05-Jun-2011.

[6] Ranjith P, Chandran P, Kaleeswaran S (2012) On covert channels between virtual machines. Journal in Computer Virology Springer, 8:85–97.

[7] Cloud Security Alliance (2010) Top Threats to Cloud Computing V1.0. Available: https://cloudsecurityalliance.org/research/top-threats.

[8] Popovic K, Hocenski Z (2010) Cloud Computing Security issues and challenges. In: Proceedings of the 33rd International convention MIPRO. IEEE Computer Society, Washington, DC, USA, pp 344–349.

[9] Cloud Security Alliance (2012) SecaaS implementation guidance, category 1: identity and Access management. Available: https://downloads.cloudsecurityalliance.org/ initiatives/schools/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf.

[10] Xiao S, Gong W (2010) Mobility Can help: protect user identity with dynamic credential. In: Eleventh International conference on Mobile data Management (MDM). IEEE Computer Society, Washington, DC, USA, pp 378–380.

[11] Wylie J, Bakkaloglu M, Pandurangan V, Bigrigg M, Oguz S, Tew K, Williams C, Ganger G, Khosla P (2001) Selecting the right data distribution scheme for a survivable Storage system. CMU-CS-01-120, Pittsburgh, PA.

[12] Somani U, Lakhani, K, Mundra M (2010) Implementing digital signature with RSA encryption algorithm to enhance the data Security of

[13] Cloud in Cloud Computing. In: 1st International conference on parallel, distributed and grid Computing (PDGC). IEEE Computer Society Washington, DC, USA, pp 211–216.

[14] Wei J, Zhang X, Ammons G, Bala V, Ning P (2009) Managing Security of virtual machine images in a Cloud environment. In: Proceedings of the 2009 ACM workshop on Cloud Computing Security. ACM New York, NY, USA, pp 91–96.

[15] Fong E, Okun V (2007) Web application scanners: definitions and functions. In: Proceedings of the 40th annual Hawaii International conference on system sciences. IEEE Computer Society, Washington, DC, USA.

[16] Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Hiren Patel, Avi Patel, MuttuKrishnan Rajarajan, "A Survey of intrusion detection techniques in cloud", Journal of Network and Computer Application 36 (2013)42-57.

[17] Han H, Lu XL, Ren LY.Using data mining to discover signatures in network-based intrusion detection. In: Proceedings of the first international conference on machine learning and cybernetics, Beijing (1) (2002).

[18] Zhengbing H, Zhitang L, Jumgi W, Novel A. Intrusion detection system (NIDS) based on signature search of datamining, WKDD First International Workshop on Knowledge discovery and Data Ming; 2008: pp. 10–6.

[19] Lei L, Yang D-Z, Shen F-C. A Novel rule based Intrusion Detection system using Data Ming. 3rd IEEE International Conference on Computer Science and Information Technology 2010;6:169–72.

[20] Gong RH, Zulkernine M, Abolmaesumi P. A software implementation of a genetic algorithm based approach to network intrusion detection. In: Proceedings of the sixth international conference on software engineering, artificial intelligence, networking and parallel/distributed computing and first ACIS international workshop on self-assembling wireless networks (SNPD/SAWN'05); 2005.

[21] Xiao T, Qu G, Hariri S, Yousif M. An efficient network intrusion detection method based on information theory and genetic algorithm. In: Proceedings of the 24th IEEE international performance computing and communications con- ference (IPCCC '05), Phoenix, AZ, USA; 2005.

[22] Dhanalakshmi Y, Ramesh Babu I. Intrusion detection using data mining along fuzzy logic and genetic algorithms. International Journal of Computer Science & Security 2008;8 (2): 27–32.