Dissection and Proposal of Multitudinal Security Threats and Menace in Cloud Computing

Seema Rawat
Assistant Professor Amity University Noida
srawat1@amity.edu

Bhawna Dhruv
M.Tech (CS&E)
Amity University Noida
bdhruv08gmail.com

Praveen Kumar
Assistant Professor Amity University Noida
pkumar3@amity.edu

Payal Mittal
M.Tech (CS&E)
Amity University Noida
payalmittal6792@gmail.com

***Abstract*- Cloud computing has emerged as a amazing field in IT world today. It fords all the impediment of computing technology and allows the working and storage of data over internet itself. It has allowed the IT workers to expand their business over internet giving a hike to capabilities and potential in the business field. But the question of security remains unanswered as till now all the IT firms have not accepted cloud completely. Business firms still fear to deploy their enterprise solely on cloud due to the security issues. In this paper, we study about issues in the cloud service delivery models and the various security issue faced in cloud computing. Based on this detailed study, we further provide recommendation that could be followed to conquer the security concerns in the cloud.**

Keywords: Cloud Computing; Data Security Threats and Risks; Cloud Delivery Models.

I. INTRODUCTION

Cloud Computing has emerged as a new field in the IT sector that serves the purpose of need of increasing storage. Whenever any enterprise expands its business, the need of infrastructure, resources arises which directly demands higher cost. To overcome this issue, cloud emerges as a rescuer providing fascinating features with the least cost. The customer is highly motivated with the emergence of cloud as it allows every possible working on the internet related to your business with least cost [1]. There exists different cloud platform like Amazon, Rackspace etc. that fulfils the demand of user. Any enterprise can just ping and demand for required resources and hence complete their working over internet keeping their data intact with third party. But the question here arises is whether the data stored with the third party is safe or not [13]. Due to this unanswered query, till now cloud has not been accepted widely.

A. Intricacy of Security in Cloud Domain

Although cloud is meant for better consumption and utilization of resources so here figure 1 describes the intricacy of security policies in cloud environment. The lowest layer of figure shows heterogeneous cloud deployment models of cloud computing i.e. Private, Public, Community and Hybrid Cloud. There is a layer of cloud delivery models above the layer of deployment models. Delivery Models includes Software as a service (SAAS), Platform as a Service (PAAS), and Infrastructure as a service (IAAS).

978-1-4799-6023-1/15 $31.00 © 2015 IEEE
DOI 10.1109/CICT.2015.130

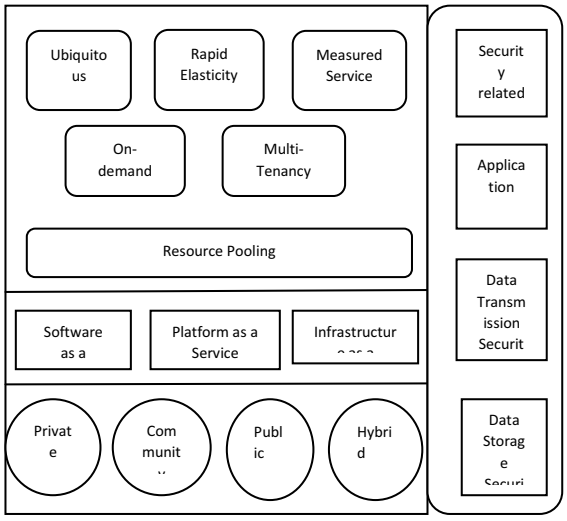

Fig.1. Complexity of Security in Cloud Domain

These delivery models show some characteristics like On-demand Self Service, Multi-Tenancy, Measured Service, Rapid Elasticity and Ubiquitous Network. In addition to this complex computing entities, there are certain security challenges like security related to third party resources, application, data transmission and storage security. The motivation of this paper is to study what are the possible threats and issues in the cloud computing architecture. Further recommendations are provided to minimize the level of existing threats by deploying different mechanisms.

B. Security Concerns and Detailed Characteristics

The basic problem that occurs is that if security concerns are handled and mechanism are deployed to secure the data, there would be much more expenditure [2]. The whole sole purpose of cloud is to keep the expenditure less but if security mechanisms are deployed, they demand huge capital to be invested. This remains an open issue to both customer as well as cloud service provider. Due to this reason only, there is a question mark on the credibility of cloud computing.

Fig.2. Cloud Computing Security Concerns

The fig 2 shown above explains the cloud computing security concerns in our IT infrastructure environment. Given below are the features of cloud computing:

- Metered Usage: The most important benefit of cloud is its metered usage. Any customer only needs to pay for what he uses. The amount of usage of resources is proportional to the cost [3]. This helps customers in a way that they do not need to work bout huge capital to be invested. The cloud service provides all the resources, infrastructure and the customer pays as per need.
- Accessibility: The cloud can be accessible from anywhere, any location. All a customer needs is the internet connection. The client need not worry about infrastructure, wherever he goes, all he needs is an internet connection to access the cloud services.
- Cost: As all the resources (physical or virtual), infrastructure are provided by the cloud services provide only, so definitely the cost involved is very less [12]. According to pay per usage plan, the cost is minimized to a greater level.

II.IMPACT OF CLOUD SERVICE & DEPLOYMENT MODELS

A. Impact of Cloud Delivery Models

- Infrastructure-as-a-Service: The task of the clients in Cloud Computing is merely not only restricted t maintenance of cloud but also managing the whole application [4]. This maintenance is performed with the help of APIs .For example- Rackspace Cloud.

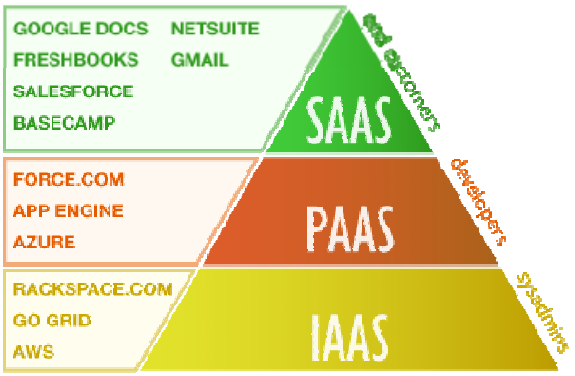

Fig.3. Cloud Delivery Models

The figure 3 above shows the delivery models of cloud computing with examples which are further explained.

- Platform-as-a-Service: With the help of this, any client can gain access to a particular platform and hence implement their applications on the cloud. The platform demanded by a client may have development tools, deployment tools etc. For example - Microsoft Azure.
- Software-as-Service: As the name suggests, any client if wants to gain access over a particular service, needs to demand for it [14].

There exists a SAAS stack of security between cloud vendors and customers to ensure security of enterprise data as shown in fig. 4. Initially, tenant 1 validates input through SAAS Applications while user authentication is achieved simultaneously. These SAAS applications manage application services through data aggregation and user authorization. Now infrastructure services like network, storage, fault etc. are achieved via data security and SLAs secure transport. Now patch is managed and operating system is hardened by virtualization layer and finally data center layer in which servers, disks and network applications are embedded. Every software will have a different service and varying implementation. For example- Online Word Processing.

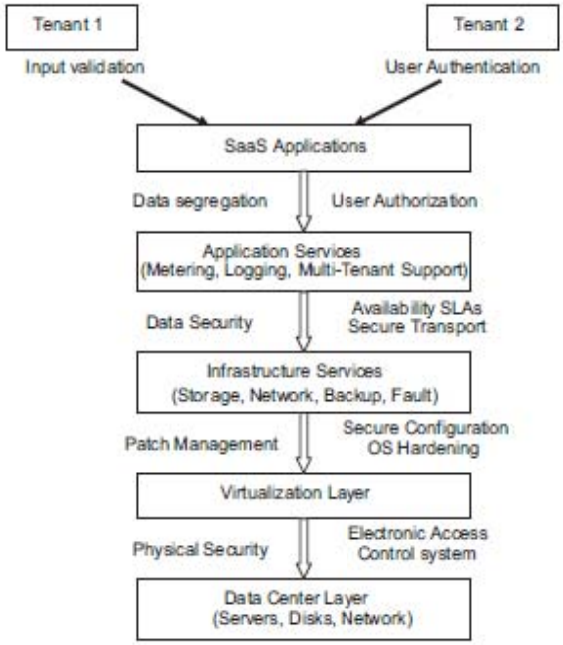

Fig.4. SAAS Security Stack [17]

B. Impact of Cloud Deployment Models

We have four deployment models namely public, private, community and hybrid, their access and consumption, infrastructure location, ownership and management are describing briefly in a table 1 shown below.

Table I. Cloud Deployment Models Impact

Cloud Deployment Models	Infra. Mgmt.	Infra. Ownership	Infra loc.	Access & Consumption
Public/community cloud	Third Party Provider	Third Party Provider	Off Premise	Entrusted
Private cloud	Organization/third party provider	Organization/third party provider	On/Off Premise	Trusted
Hybrid Cloud	Both	Both	Both	Both

III. SERVICE DELIVERY MODEL ISSUES

A. IaaS Issues

- Hypervisor Security: A hypervisor is compute utilization software that allows various operating system to run on a physical machine concurrently. It is further divided into two components. It can be considered as a major role player that allows any access to physical resources. If there is a breach in the security of the hypervisor, the whole infrastructure of virtual machine becomes insecure [5]. Because can it be possible to cloud and data center hypervisor be same? 62% of the vendors think that yes they can be the same and only 5-6% of users think they cannot be same as shown in fig. 5 because if they match, security of data center breaches due to cloud hypervisor.

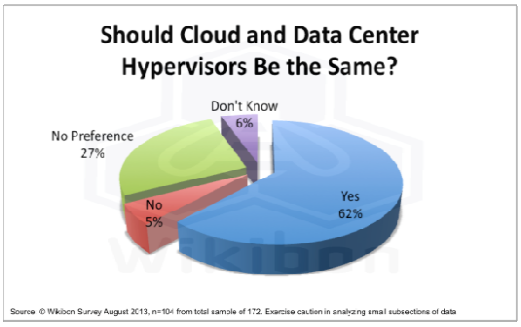

Fig.5. Data Center and Cloud Hypervisor Analysis [7]

- VM Security: The security of a VM becomes a task for the cloud clients as they are the ones exploiting it. The cloud providers can make security policies at their own ends [15]. The clients must implement different security model at their own end to secure their virtual machine.

B. PaaS Issues

- API Security: Whenever any client demands for various API for the processing of deployment tools, there arises a need for different storage space for each API in the memory [6]. Due to this, every API can have their own security controls.
- Service Oriented Architecture Issues: For any application to be secure, whether it is traditional or cloud model, there is a need of authentication as well as authorization of every user. Both the cloud providers and the user must work together to solve this issue.

C. SaaS Issue

- Web Application Security: For different application which the user demands, there is a need for proper security measures as the exploitation is being done on the web [7]. There should be proper firewalls on every system so as to avoid any vulnerable attacker. All the application that have to be carried out on the cloud should be properly validated in advance itself.

IV. SECURITY THREATS

As the technology is massive, because of its advancement, threats are more prone to cloud models. In cloud computing, basic entity is data and accumulated data growth lead to threats of being stolen or misuse by unauthorized user and when threats increases, there arises risk of storage failure as shown the fig. 6 below. So there must be some security principles implied on cloud to achieve stability and prevention from threats and risks.

Fig. 6. Cloud Security Threats [6]

A. Information Security

In Cloud computing, information security plays an important role. Just like many other applications and technologies, cloud also face different types of security threats. These threats may be physical security, loss of data, legal issues etc. The model developed to overcome the issues of information security is CIA-Confidentiality, Integrity, and Availability [8]. Therefore it becomes the responsibility of a cloud provider to serve the customer with data security.

B. Data Security

As in Cloud Computing, the customer uses the infrastructure of the cloud provider, so that the data of the customer is also stored in the cloud provider's physical devices only. Both the actual data and its backup is stored in a physical device only. In case of any loss of data, it can be recovered from its backup [9]. A proper and genuine restoration of all the data is must. Cloud must not only preserve the data but also prevent it.

C. Data Integration

For implementing cloud, proper infrastructure is required, which includes no. of physical device. Therefore for any attacker, a proper investigation is required about the residual of each and every data so as to steal it [10]. There arises a need of imposing restrictions on the network as a whole to keep it safe. Any organization must choose best of the cloud providers to keep their data intact and safe as well.

D. Multi-tenancy

Cloud serves as platform as a whole package where multiple users demands similar resources and share same applications to run their virtual machines as shown in fig 7. Due to sharing of resources whether hardware or software, there are chances that the information gets leaked due to some reasons [11]. The sharing of resources increases further chances of attack.

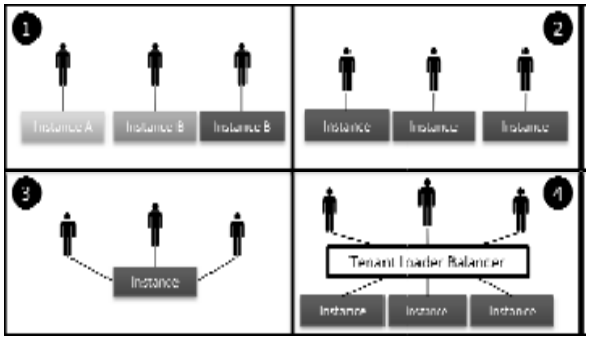

Fig.7. Multi- tenancy Approaches [17]

E. Service Disruption

Various attacks like phishing or fraud still tend to take place in Cloud. The attacker only requires the credentials of an authorized user s as to manipulate the actual data [16]. This type of attack is most critical because it can give rise to further DOS or DDOS attacks. Hence there is a need to secure the critical data.

V. RECOMMENDATIONS

A. Confidentiality

Confidentiality basically means that the data sent from party A to party B must remain between A and B only. Any third party must not have the right to access the data. To achieve this confidentiality, encryption techniques must be followed. The techniques may either be symmetric key encryption or asymmetric key encryption. In this way, just like other credentials, the key must also be sustained securely to have genuine access of the authorized user over various applications.

B. Integrated Security between Clouds

Whenever any customer demands resources from different cloud platforms due to various reasons, there arises the need of much more security between the cloud and the customer. To work as a single entity for a particular customer, there is a need for security that works in an integrated manner so that operability becomes simple for any user keeping the applications secure.

CONCLUSION

Cloud Computing is fascinating field that has emerged as a powerful model providing virtual business to various enterprises. In this paper we studied about what is the basic architecture of cloud

computing and what are the delivery models deployed in it. Further discussion is on issues and security threats that are existent on the cloud. Few recommendations are given regarding deployment of different techniques which proves the cloud services to be secure and safe.

Different mechanisms studied encourage us to study more techniques to be deployed so as to keep the cloud platforms safe for both cloud provider and the clients.

REFERENCES

[1] Mohamed Almorry, John Grundy, Amani S Ibrahim, "Collaboration-Based Cloud Computing Security Management Framework", IEEE 4th International Conference on Cloud Computing, 2011.

[2] Farzad Sabahi, "Cloud Computing Security Threats and Responses", IEEE, 2011.

[3] Kwang Mong Sim,"Agent Based Cloud Computing" IEEE Transactions on Service Computing, Vol 5, No.4 Oct-Dec, 2012.

[4] Akhil Behl,"Emerging Security Challenges in Cloud Computing, IEEE, 2011.

[5] Farhan Bashir Shaikh, Sajjad Haider," Security Threats in Cloud Computing", 6th International Conference on Internet Technology and Secured Transactions, 11-14 Dec, 2011.

[6] Wentao Liu, " Research on Cloud Computing Security Problem and Strategy", IEEE, 2012.

[7] Xu Xiaoping, Yan Junhu, " Research on Cloud Computing Security Platform", 4th International Conference on Computational and Information Sciences, 2012.

[8] Anas Bouayad, Amar Bilat Nour el Honda Mejhed,Mohd el Ghazi," Cloud Computing Security Challenges," IEEE,2012.

[9] Akhil Behl, Kanika Behl," An Analysis of Cloud Computing Security Issues", IEEE, 2012.

[10] Ni Zhang, Di Liu, Yum Yong Zhang,"A Research on Cloud Computing Security", International Conference on Information Technology and Application, 2013.

[11] Aws Naser Jaber, Mohd Fadli Bin Zollipli,"Use of Cryptography in Cloud Computing", IEEE International Conference on Control System, Computer and Engineering, 2013.

[12] Hanim Eken," Security Threats and Solutions in Cloud Computing", World Congress on Internet Security, 2013.

[13] G Kulkarni and J Gambhir,T Patil,A Donare," A Security Aspects in Cloud Computing",IEEE,2012.

[14] Cloud Security Alliance Congress, 2010, Orlando, F L, Nov, 2010.

[15] A Amies, H Sluiman, Q Tong, G Liu,"Infrastructure as a Service Cloud Concepts", IEEE,2012.

[16] A Mana, A Munoz J Gonzalez," Dynamic Security Monitoring for Virtualized Environment in Cloud Computing", 1st International Workshop on Security Services on Cloud (IWSSC), 2011.

[17] Microsoft, "Multi-Tenant Data Architecture" available at http://msdn.microsoft.com/en-us/library/aa479086.aspx. 2006.