Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 3; January-March, 2015 pp. 196-200

http://www.krishisanskriti.org/acsit.html

Addressing Cloud Computing Security Concerns

Vasundhara Bhatia[1], NehaPrabhakar[2] and SumatiManchanda[3]

[1,2,3]Amity School of Engg. and Technology Amity University, Noida, Uttar Pradesh
E-mail: [1]vasundhara.bhatia9@gmail.com, [2]nehaprabhakar91@gmail.com, [3]matimanchanda@gmail.com

Abstract—*Cloud computing is an upcoming model which provides various services over the network. One can share resources, request for various services or store their data at another site very conveniently. It is excessively used these days by a number of users. Cloud has a number of advantages which makes it a widely used model these days. Cloud computing offers the facility of paying for only the amount of resources that are required by a particular user at some time, thus, it provides cost saving. But cloud computing has issues, which still makes many organizations to follow the old traditional approach. We discover that security issue is one of the major issues in cloud. Security has to be kept in mind in any field and also in cloud computing. In this paper we discuss some of the security issues which affect the cloud computing system. We analyse the basics of cloud computing, characteristics, advantages, models and most importantly the security issues that it faces.*

1. INTRODUCTION

Cloud computing refers to using and utilizing services provided by a third party. These services may be applications, development environment, storage etc. Instead of storing applications or documents on one's own personal computer, one can pay for cloud services where the data may be stored or the required services may be provided through the cloud vendor's servers. The person has to pay for only what they use and the resources can be minimized and expanded according to the user's needs. An application developer uses cloud services to gain more processing power, development environment or storage facility. An end user mostly uses applications which are provided by a developer or storage space. The major benefit is that the services are accessible from wherever you are which removes any limitations that one can only access their documents or applications only through their personal computers or laptops. All one needs is an internet connection and any device which connects to the cloud server to provide the required services [1].

2. CHARACTERISTICS OF CLOUD COMPUTING

- Cloud computing offers an important facility in which the cloud resources are demanded as and when they are required. It gives user the authority to use the cloud resources only when the user needs to use it.
- Cloud computing offers scalability services. It allows users of cloud to request for some services as and when they are required. These capabilities can be scaled out, i.e. expanded or scaled in, i.e. some services can be released quickly. This allows users to use only those services that are essential to them or use the services which are additionally required.
- The resources that are hosted by a cloud vendor can be accessed from a wide range of locations and these resources can be accessed through a variety of devices such as laptops, computers, mobile phones etc. This allows the cloud resources to be accessed from anywhere at any time. So the services are always available to the user.
- The cloud vendor provides shared resources to various users which serves multiple users at the same time. It uses the multi-tenant model which has consumers with different virtual and physical addresses. Sharing allows the utilization of resources that are provided by the vendor.
- Cloud computing systems have a facility that tries to measure and keep a track of storage or processing and many more. The usage of the resource can be monitored and controlled which provides transparency for both the vendor and the user. This controlling allows the user and vendor to be aware of the services that are used and that are required [2].

3. ADVANTAGES OF CLOUD COMPUTING

- Providing the amount of storage required: When one stores data or information in the cloud then one can get a capacity of almost unlimited storage. It is the responsibility of the cloud vendor to provide the amount of storage necessary for the user. In the traditional system, the users had to worry about increasing the storage capacity according to the requirements, but cloud facilitates the users to have as much as space needed for storage. The users are charged for only what they use.
- Easy recovery and backup is provided: Since, all the data is stored in the cloud so backing up the data that is stored at the cloud vendor's site is much easier than storing and backing up on a physical device or your own device. Cloud vendors ensure that backup is provided so a user does not have to worry about constantly backing up their data.

- Automatic integration of software: This allows the users not to worry on how their cloud services should be customized and integrated as per their requirements. One can simply pick and carefully select only those services and software applications that you think are suitable for you. The user just has the responsibility to provide their requirements to the cloud vendor and the cloud vendor may automatically integrate the software according to the desired requirements.
- Access to information is simple: The information can be accessed from anywhere. This is because once a user starts to use a cloud service then the user only needs an internet connection, which are easily available these days. The cloud computing services can be provided on smart phones, laptops, tablets etc. Whenever a user wishes to access some information from the cloud, the user only needs an internet connection and a device to use it.
- Fast and easy deployment: Cloud computing provides you the advantage and benefits of quickly deploying an application. When cloud system is chosen then the system which has to be deployed can be done in very few minutes. But the time depends on the technology that is needed for a particular user. The time of deployment varies from one user to another. The user can easily deploy the application that he/she wishes to deploy within a very short duration. [3]
- Saving money: Cloud computing is very cost effective method to use. It is also easy to maintain and upgrade which helps to reduce the cost. When users are using the earlier methods, more cost is required in them when compared to cloud computing methods. This is because, additional licensing fees is required for various software. Various cloud vendors may provide different rates so a user has the option to choose the vendor with the cheaper rates and thus expenses are reduced.
- Globalization of workforce: Since all the data is stored on cloud, people having a simple internet connection can access the required resources. This helps in globalization and employment of workforce globally, since employees working in a different part of the world can have a quick access to the required resources. [4]

4. SERVICE MODELS

There are three types of cloud services that are provided by a cloud model [2,5,9]:

4.1 Software as a Service (SaaS)

This is the top most layers of the services which is provided by the cloud. It provides the capability to the user to use the vendor's applications running on a cloud infrastructure provided by the vendor. It provides the users with applications and services which can be used directly by a user which can easily be accessed from several client devices which provides on-demand services.

4.1 Platform as a Service (PaaS)

It is the middle layer of the cloud services. A user can deploy his applications on the cloud without installing any platform on which the application is to be deployed. PaaS provides platform layer resources, which includes the support of the operating system and the frameworks which are used for development of various services. These services control the installed applications and available hosting environment configuration.It provides user with the option to deploy on the cloud, various technologies and applications which are developed by a user or various other applications that may be supported by the vendor.

4.2 Infrastructure as a Service (IaaS)

This layer is the bottom layer of the three layers and it provides infrastructure services. These services may include resources such as memory, CPU and storage. The service that is provided to the user involves storage, processing, networks and various other computing resources.

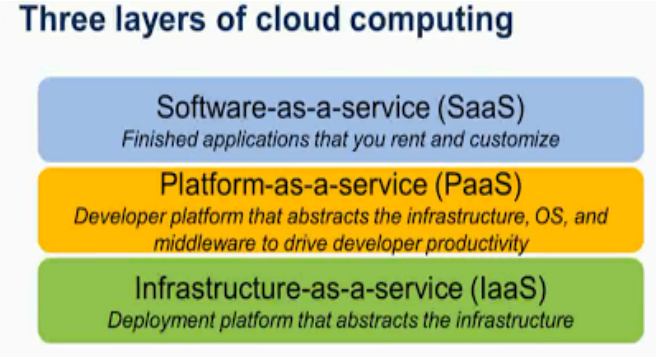

Fig. 1: Three Layers of Cloud Computing

All of these three services are related to each other but understanding their relationships and dependencies is critical to understanding the risks of cloud computing security [12]. IaaS is the bottom layer which forms the basic formation of all the services. The PaaS builds upon IaaS and SaaS builds upon PaaS. All these services are provided directly to the user/client.

5. DEPLOYMENT MODELS

The major factor to provide a secure cloud computing is the type of cloud to be implemented. The types of cloud deployment models offered are[7,6,6,7]:

5.1 Private cloud

This type of cloud is only used for a particular organization or a group of people. It may be managed by the organization which is using it, which has the access to this cloud or third party. It is can be also named as internal cloud. The organization or the people are responsible for setting up the

cloud according to their own needs and maintaining them. Thus any organization can take better control of the services and all the work done within their cloud. Since only the organization has the access to this private cloud, so it is more secure.

5.2 Community cloud

This type of cloud infrastructure is used by particular groups of organizations or communities. It is a semi-private cloud which is available to only those groups which have access to it. The community cloud acts as a private cloud for a particular community. Only the users that have access to this community cloud can access the services and resources provided by it.

5.3 Public cloud

This type of cloud infrastructure is used to provide services to a lot of public or large group people. Public cloud is the cloud services which is provided by third parties and hosted and managed by the service providers or the vendors. All the cloud vendors have the responsibility to manage the installation, maintaining and providing services to the user. There is a huge potential for cost saving. Users are charged according the services and the resources they use. Major drawback of this type of model is the lack of security. This is because the resources and services are provided by a cloud vendor who also provides services to various unknown users. The public cloud vendors often use the multi-tenancy model in which the various users share the same resources. Since the resources are shared and the separation is vulnerable, the data and application of one organization may have a threat to be exposed to another unknown user.

5.4 Hybrid cloud

Hybrid cloud is composed of a number of clouds. These clouds could be private, public or community clouds. They remain independent from each other but they remain together by a technology that enables the user to access the data and the application. The responsibilities of managing the cloud are divided amongst the organizations using the cloud and the public cloud vendors.

6. SECURITY CHALLENGES IN CLOUD

There was a survey which was conducted by International Data Corporation (IDC) IT group in order to rate the cloud services and know more about its issues in 2008 [2]. This survey was conducted in 224 IT executives. The IT executives were asked to rate which cloud computing issue is of the maximum concern. The following Fig. shows the percentage of the individual issues that are found in cloud.

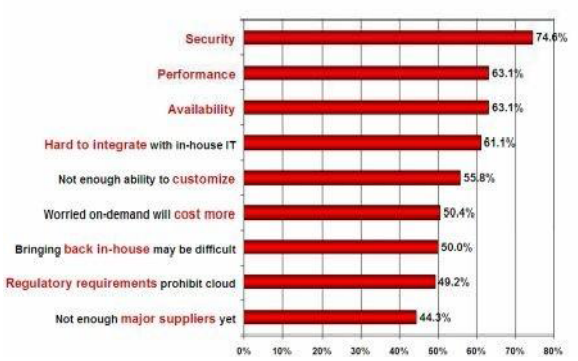

Fig. 2: Survey of Issues in Cloud

This survey conveys that the percentage of cloud security issues is found to be 74.6%, which is the highest percentage amongst all the issues that are considered in the survey.

It can be concluded that that security is the major concern and it comes with a lot of threats in cloud computing [13,19]. That is the reason that cloud computing security issues are given a huge attention so that they may be prevented. It is extremely important to face these issues to make cloud computing a better and safer environment which can be expanded and used by various people.

7. EVALUATION OF SECURITY

Evaluating how secure is a particular cloud system is a crucial task [14]. For evaluating the security of a cloud there are certain objectives that could be taken into consideration. The objectives that are considered an important part for a cloud to be secure are [8]:

- Confidentiality: Confidentiality means that only authorized people, parties or systems have the ability to access any protected data. Every user or organization that opts for the services of a cloud vendor always wants that the information and the organizational data must remain secure. This should be done only by providing access to the users that the organization allows. Even the cloud vendor must not have access to a cloud user's private data. Since cloud services are provided to multiple users sharing the same resources, devices and applications, the risk that the data is compromised is increased to a high level.
- Integrity: Integrity means that the information or the resources that belong to a particular user can be modified only by the people who are authorized and in an authorized way.It means that the data must be protected from deletion, modification or addition to the existing data by an unauthorized person. Data and services of an organization must not be stolen or misused. Any change in the data should only be done by the person who has an authorized access provided by the cloud user itself. It is

essential to respect one's privacy and this should also be accepted in terms of cloud.

- Availability: Availability means that a system is accessible and it can be used when it is in demand by the authorized person. The cloud vendor must always keep a backup of the resources and data to ensure that the cloud user is always provided with the required services even under difficult circumstances. Availability is not only limited to data and software but also hardware being available to authorized users when it is needed. The cloud owner must ensure that the services are available to the user as and when they are required.

8. WHY SECURITY IS A MAJOR CONCERN

- Lack of employee confidence and poor recruitment practices: There are some cloud vendors who may not perform background checks of their employeesor service providers. It is possible that the person might misuse the private data of an organization. The cloud vendors often do not check personally on the people they hire who may harm the vendor or the users later. Some special users such as cloud administrators usually have unlimited access to the data present in the cloud which may not be acceptable to a cloud user.
- Lack of checking background of customers: Most cloud vendors do not make the effort to check the background of the customer they are providing. This gives a threat that almost anyone can open an account that has a valid credit card and an email. Some fake accounts can let attackers perform any malicious activity without being identified and tracked. One user may gain access to the resources and data of the data which compromises the security of another cloud user.
- Lack of education regarding security: People have been a weak point in the knowledge about information security. This case is true in any type of organization or company. In the cloud there is more impact because there are more number of people that have to use the cloud. These people are cloud vendors, third party vendors, suppliers, customers of organizations [2].

9. SECURITY ISSUES

The various security issues that are encountered when using cloud computing are as follows.

9.1 Data Security

Data security is a major concern everywhere, but it is a major problem when the users have to rely on the vendors for providing proper and essential security. In traditional application deployment, the data resides within the boundary of the organization itself and it has physical and logical security access policies. These type of data breaches and issues in the data security often occur in cases of public cloud because the cloud users have less control over the data and resources that are present at the vendor's site. Storing the data at another site always has the risks that it can be accessed by some other party [17]. It can be accessed by the vendor itself or by another cloud user which the cloud vendor serves.It is an extremely important responsibility of the vendor to apply strong encryption techniques so that the data is secure and only selective people can control and access the data [10]. The cloud vendor should ensure that only the people who are authorized by the cloud user can change, add, modify or delete any information of the cloud user. The cloud vendor must not have any control whatsoever to change any information that belongs to the user. Backup and recovery of data is another issue. There may be certain circumstances where the data at the vendor's site may be lost or compromised. In such a case, the vendors often have a backup somewhere else to ensure that the data is always available to the cloud user. But, keeping a backup at different locations or sites may not ensure that the data is in safe hands.

9.2 Multi-tenancy

In public cloud services the user shares the resources and components with other users at the vendor's site [7]. These users may be unknown to them. In a multitenant environment, many customers share the same application, which uses similar operating system, on the same hardware, with the same functionalities of data storage. The differentiation amongst the data of a particular user is made on the application layer. Multi tenancy allows for cost savings for the vendor and thus may also provide cost saving for the cloud user. This is possible because various resources are shared among various users so the cloud vendor does not need to install additional infrastructure for different users. Since the vendor saves money so it is possible that the vendor offers these services to the users for less cost. Using resources from a multitenant environment poses risk to the resources and data of one user from another. An attacker could simply be another cloud user and may discover the vulnerabilities that the cloud environment is having. The separation between the different users may be have been overcome and the data and resources of another user can be accessed by an attacker who poses as a user to the vendor [11]. The risk of an attacker posing as a user often increases because the vendors do not have background checks on the users there are going to provide services. Vendors simply think of their benefit and ignore the cause that and if a user is not as he poses to be then he might cause loss to the vendor.

9.3 Application Security

Applications are delivered and used via the Internet through a Web browser. SaaS provides the software which is deployed over the internet and is also deployed to run behind a firewall in local area network or personal computer [10]. People who attackers the applications they use the web to gain access of user's information and perform malicious activities such as

steal sensitive data of a user etc. [5]. The threats that might be present in a cloud based environment are generally more than the traditional system. It is also possible that tenants using the same SaaS infrastructure, gains access to the data of another tenant through the vulnerability in the web layer.

9.4 Trusted Third-party

A trusted third party provides secure interaction between two parties who trust a third party. These trusted third parties provide various security services which are based on standards. They are useful across various geographical areas, domains and specialization sectors. These third parties provide an assurance of trust between two parties by special techniques and mechanisms [16]. So it becomes necessary to choose the correct third party which provides appropriate mechanism for the secure interaction between the two parties. A high level of trust and reliability has to be established because if the third party does not provide the correct means then it may lead to the information and data of a party to be insecure. The two parties rely on the third party to perform various functions such as cryptographic separation of data which encrypts the data and ensures that the data is not visible to any outsider and server and client authentication in which both the interaction parties require to certify their server and network devices.

9.5 Service Level Agreement

Service level agreements are the contracts which are signed by a cloud vendor provided by the cloud user. It specifies the services that are to be provided by the cloud vendor to the user.The service level agreements, also defines the terms and conditions and period of service to be provided. If the service provided by the vendor is to be discontinued by the user then the conditions for termination are decided at the initial level itself. In case the termination of the agreement between the cloud user and vendor is to be performed then removal of the user data from the vendor's site after termination is to be done [1]. This should be ensured that the data is removed after termination of services otherwise the cloud vendor may misuse the user's data.The authentication and authorization is specified to identify who can access the services. This is a crucial part because it defines who can access the data and services of the user. These conditions should be correctly represented to ensure that the vendor or any third party may not find something faulty in it and gains access to the user data. The vendor has to clearly specify the services that will be provided to the user. It also includes the measures that the vendor will take to ensure security. Information about any backup that is to be done in any scenarios is also to be given. If a cloud vendor is unsatisfactory in any of the conditions that are provided in these agreements then legal action may be taken using these service level agreements. These ensure that what user expects and what the vendor provides is clearly specified in these agreements so that no expectation gaps occur between the user and vendor. It represents clarity in the understanding of the services to both the vendor and the user.

10. CONCLUSION

Thus, we can observe that even though cloud computing offers enumerable advantages but at the same time one faces with a variety of issues. It becomes the responsibility of every cloud user to be aware of both the advantages and disadvantages of the cloud services in order to use the cloud services efficiently and securely.

REFERENCES

[1] National Institute Of Standard and technology. csrc.nist.gov/groups/ SNS/cloud-computing/cloud-def-v15.doc, 2009

[2] Rajesh et al , International Journal of Advanced Research in Computer Science and Software Engineering 2 (9), September-2012, pp. 115-120

[3] http://mobiledevices.about.com/od/additionalresources/a/Cloud-Computing-Is-It-Really-All-That-Beneficial.htm

[4] http://www.verio.com/resource-center/articles/cloud-computing-benefits/

[5] Hashizume et al.: An analysis of security issues for cloud computing. Journal of Internet Services and Applications 2013 4:5.

[6] Florin OGIGAU-NEAMTIU, CLOUD COMPUTING SECURITY ISSUES,Journal of Defense Resource Management,Vol. 3,Issue 2(5)/2012

[7] ABHA THAKRAL SACHDEV* et al ISSN: 2319 - 1163 Volume: 2 Issue: 2 126 – 130

[8] D. Zissis, D. Lekkas / Future Generation Computer Systems 28 (2012) 583–592

[9] Wayne A. Jansen, NIST, Proceedings of the 44th Hawaii International Conference on System Sciences – 2011 Cloud Hooks: Security and Privacy Issues in Cloud Computing

[10] S. Subashini, V. Kavitha / Journal of Network and Computer Applications 34 (2011) 1–11

[11] National Institute of Standards and Technology Special Publication 800-144 80 pages (December 2011)

[12] http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[13] GregBoss, Padma Malladi, Dennis Quan, Linda Legregni and Harold hall 2007. Cloud Computing.Available from www.ibm.com/developerworks/websphere/zones/hipods/.

[14] Anthony T.Velte, Toby J.Velte and Robert Elsenpeter 2010. Cloud Computing- A Practical Approach. Publishing of Tata McGRAWHil.

[15] Mohamed Al Morsy, John Grundy and Ingo Müller, An Analysis of The Cloud Computing Security Problem, In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.

[16] Kevin Hamlen et al.: Security Issues for Cloud Computing, International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010

[17] 2009. Cloud Computing: An Overview, Pages 2 (June 2009), 2 pages. DOI=10.1145/1538947.1554608 http://doi.acm.org/10.1145/1538947.1554608

[18] Basta, A., &Halton, W. (2007). *Computer Security and Penetration Testing* (1st ed.). Delmar Cengage Learning.

[19] NitashaHasteer ,AbhayBansal , B. K. Murthy, Pragmatic assessment of research intensive areas in cloud: a systematic review, ACM SIGSOFT Software Engineering Notes, v.38 n.3, May 2013