Tending to Security Issues in Cloud Computing

Sumati Manchanda
Amity School of Engineering and technology
Amity University, Noida Uttar Pradesh
matimanchanda@gmail.com
Manpreet Singh Bajwa
Amity School of Engineering and technology
Amity University,Noida Uttar Pradesh
manisinghbajwa@gmail.com

---ABSTRACT---

Cloud computing is an upcoming model which provides various services over the network. One can share resources, store their data at another site very conveniently. Cloud computing is a more adaptable i.e flexible, cost effective also demonstrated conveyance stage for giving business or consumer benefits over the Internet. Cloud computing supports distributed service, multi-user and multi-domain administrative infrastructure and therefore it is more inclined to security dangers and vulnerabilities. Security is one of the major concern to the cloud service providers who are actually the ones who host the various services. Much of the time, the supplier must ensure that their foundation is secure and customers' information and applications are protected, by executing security strategies and instruments. In this paper we discuss some of the security issues which affect the cloud computing system. We analyze the basics of cloud computing and the security issues that it faces.

Keywords: cloud computing; data security; cloud security; integrity; multi tanency ; confidentiality; elasticity.

I. INTRODUCTION

Cloud computing nouns and its prototype in quite a while prior there have been [1], however it is as a business figuring model idea by Google CEO Eric Schmidt at the General Get together of the internet searcher in 2006, [2] first proposed2007, Google and IBM to open cloud computing course numerous renowned colleges in the United States, plan to vivaciously advance distributed computing, distributed computing will soon be known. Statistics demonstrate that consideration regarding cloud computing in the first and foremost a large portion of 2008, significantly more than the matrix processing i.e grid computing and other appropriated processing model [3]. Some conventional registering to unified power supply mode movement compared cloud registering from a solitary generator force directing force plant, it implies that processing limit can likewise be utilized as a ware flow, water, power, access to advantageous low costs [4].

Basically, cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing technologies can be implemented in a wide variety of architectures, under different service and deployment models, and can coexist with other technologies and software design approaches. The emergence of cloud computing, gives a promise to have positive effects on the systems and networks of various organizations. Cloud computing provides the next generation of internet based, highly scalable distributed computing systems in which computational resources are offered 'as a service'. Cloud computing services benefit from economies of scale achieved through versatile use of resources, specialization, and other efficiencies.

This article discusses the issues of cloud computing on data storage and security.

II. CHARACTERISTICS OF CLOUD FOR SECURITY

A. 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 [5]. 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 [6]. 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.

B. Multi-tenancy

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.

Multi-tenancy is a peculiarity one of a kind to resource sharing in clouds, particularly out in the public clouds. Basically, it permits cloud suppliers to oversee resources use all the more effectively by apportioning a virtualized, imparted foundation among different clients. Multitenancy in cloud computing is realized typically by multiplexing the execution of VMs for potentially different users on the same physical server [7].

C. 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[8]. 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.

D. 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 [9]. 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.

E. Elasticity

In cloud computing, clients need to utilize resources to the extent that is required while having the capacity to expand or diminishing resources utilization focused around genuine requests. To address such needs, cloud services must be elastic, i.e., the obliged resources of capacity and processing power can be expanded or diminished focused around clients' requirements. Elasticity suggests having the capacity to scale up or down resources assigned out to services focused around the current interest. Scaling here and there of an tenant's resources gives the chance to different tenant to utilize tenant's previously assigned resources.

Besides, security necessities characterized by clients ought to be moved with the services and launch a procedure to uphold security prerequisites on the new environment, as characterized by cloud clients, and redesigns the current cloud security model.

III. EVALUATION OF SECURITY

Evaluating how secure is a particular cloud system is a crucial task [10]. 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 [11]:

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.

IV. 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 [12].

V. STRANDS OF SECURITY ISSUES

As indicated by [13] vulnerability "is a weakness in the security system" that could be abused to cause harm. Cloud computing is pretty much as defenseless as whatever other engineering that uses the general population web for network. The vulnerability incorporates eavesdropping, hacking, cracking, malicious attacks denial-of-service attacks and outages.

Cloud Security Alliance [14] and Gartner [15] have distinguished different security dangers to cloud computing,[6] arranges security dangers in cloud focused around the service conveyance models of a cloud framework. Nonetheless, security obliges an all encompassing methodology. Service delivery model is one of many aspects that need to be considered for cloud security. Security at diverse levels is essential to guarantee fitting usage of cloud computing, for example, host server security, information stockpiling security, web/system security, and application security.

Cloud security can be dissected along three strands, i.e., character security, data security, base security[16].

Identity security: End-to-end identity management, thirdparty verification services, and unified identity will get to be key components of cloud security.Identity security safeguards the honesty and privacy of information and applications while making get to promptly accessible to proper clients. Help for these character administration capacities for both clients and foundation parts will be a real necessity for distributed computing, and personality will must be overseen in ways that assemble trust.

Information security: In the conventional datacenter, controls on physical access, access to equipment and software and identity controls all consolidate to secure the information. In the cloud, that defensive boundary that secures framework is diffused. To adjust, security will need to end up informationcentric. The information needs its own particular security that goes with it and ensures it.

Information security is nearly identified with outsider information control. Normal concerns incorporate the path in which information or say data is stored and accessed, consistence and review prerequisites. All delicate or controlled information needs to be appropriately isolated on the cloud storage foundation, including archieved information.

Encrypting and managing encryption keys of data in transit to the cloud or data at rest in the service provider's datacenter is critical to protecting data privacy and complying with legal and regulatory mandates.

Infrastructure security: The foundational infratsructure for a cloud must be characteristically secure whether it is a private or open cloud or whether the administration is Saas, Paas or Iaas. The cloud computing base, including servers, switches, switches, capacity gadgets, power supplies, and other segments that help operations and exchange of information also data, ought to be physically secure.

VI. CONCLUSION

In the advancing of cloud computing servicess, the issue of security is a standout amongst the most huge issues to be determined. Today's system development, security items, and encryption convention have been ensured the wellbeing of information transmission essentially; Data stockpiling security can be understood through specialized means in the outline phase of cloud administrations, for example, excess, equality, client confirmation and access control; security includes numerous angles, the first is to enhance the important laws and regulations as quickly as time permits, and the second is good with information between distributed computing administration suppliers to guarantee that clients can consistently dish information, and administration suppliers ought to create a quick and successful disaster recovery mechanisms to ensure the accessibility of the information.

REFERENCES

[I] "Cloud computing," http://en.wikipedia.org/wiki/ Cloud_computing,2011.

[2] SEMO 2006 San Jose.http://www.searchengine strategies.com/sew/summer06/index.html.

[3] Google Trends.http://www.google.com/trends?q= Cloud+Computing.20 11.1.

[4] Liu Peng, "Coud Computing," in Proceedings of Electronic Industry Press, 20 I OJ.

[5] 2009. Cloud Computing: An Overview, Pages 2 (June 2009), 2 pages. DOI=10.1145/1538947.155 4608 http://doi.acm.org/10.1145/1538947.155460 8

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

[7] T. Ristenpart, E. Tromer, H. Shacham, S. Savage, Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds,Proceedings of ACM Conf. on Computer and Communications Security(CCS 2009), November 2009, pp. 199-212.

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

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

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

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

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

[13] C. P. Pfleeger, S. L. Pfleeger, Security in Computing. Fourth Edition.Prentice Hall

[14] G. Zhao, et al., Deployment models: Towards eliminating security concerns from cloud computing. in Proceedings of Int. Conf. on High Performance Computing and Simulation (HPCS), June 28 - July 2, 2010, Caen, France, pp. 189 – 195

[15] J. Brodkin, Gartner: Seven cloud-computing security risks. In: Infoworld 2008 http://www. infoworld.com /d/security-central/gartnerseven cloudcomputing-security-risks-53?page=0, 1.

[16] S. Dokras, et al., The role of security in trustworthy cloud computing. White paper, RSA, The Security Division of EMC.