IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-3, Issue-2 E-ISSN: 2347-2693

Security Issues in Cloud Computing

Indu Sharma[1], Mandeep kaur[2]

[1*,2] Dept. of Computer Science Engg., *Rayat and Bahra Institute of Engg., Sahuaran, PTU Punjab , India*

www.ijcaonline.org

Received: Jan /09/2015 Revised: Feb/08/2015 Accepted: Feb/14/2014 Published: Feb/28/2014

Abstract—**Cloud computing trend is increasing rapidly so to make cloud computing more popular the very first step for the organization is to identify exact area where the cloud related threats lie. At an unusual pace, cloud computing has transformed business and government. And this created new security challenges. The development of the cloud service model provide business – supporting technology in a more efficient way than ever before .the shift from server to service based technology brought a drastic change in computing technology. However these developments have created new security vulnerabilities, including security issues whose full impressions are still rising. This paper presents an overview and study of cloud computing, with several security threats, security issues, currently used cloud technologies and security solutions.**

Keywords— *Data Security, Cloud, Computing, Privacy*

I. INTRODUCTION

Cloud computing is set of resources that are being allocated on demand. Cloud computing proposes new ways to provide services. Cloud Computing is today's most inspiring technology in computer industry and in research. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources(e.g., network, servers, storage, applications, and services) that can rapidly provisioned and released with minimal management effort or service provider interaction.[1]Cloud computing services are quickly becoming formal and integral members of IT portfolio. Cloud computing is a collection of resources and serviced provided by cloud service provider through internet. Cloud services are distributed from data canters sited all over the world. Cloud computing makes possible for its users to use the virtual resources via internet as per requirements. Cloud computing grabbed the spotlight in few years. Organizations are adopting cloud-based platforms which provides infrastructure and application services as a pay-per-use basic. Client organization are more concern with lack of security and it is the, most important reasons organizations are hesitating for adopting cloud services.[2] To make cloud computing adopted by users and industry, the security concerns has to be rectified. When we Compared with the traditional IT model, the cloud computing has many potential advantages. Basicaly it helps the users to use services from other without actually buying it for huge costs. But from the consumers' perspective, cloud computing security concerns remain a major barrier for the adoption of cloud computing. According to a survey from IDCI in 2009, 74% IT managers and CIOs believed that the primary challenge that hinders them from using cloud computing services is cloud computing security issues [3].

II. CLOUD COMPUTING ENVIRONMENT

Before the data security issues are discussed we will see the functions of cloud. Cloud computing has particularly many characteristics:

- On-demand capabilities
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

Basically there is a cloud service provider that provides services and manages the services. The provider facilitates the services over the internet and end user use them for their needs and pay for the service provider accordingly. Because of high performance computational services at cheaper rate cloud is growing continuously and many famous companies such as Microsoft (Azure), Amazon, Google, etc, are providing cloud services on the internet.

Depending on the access scope, cloud can be classified as :

Private cloud : Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization's internal enterprise datacenter. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud.[4]

Public Cloud: Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. It is typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization.[5] Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.

Hybrid Cloud: Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network [6]. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Cloud provides more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems. Hybrid cloud can describe configuration combining a local device, such as a Plug computer with cloud services.

III. DATA SECURITY ISSUES

Cloud computing faces as much security threats as that are existing in the networks, intranets .these threats come in various forms. Cloud computing alliance did research in 2013 on cloud computing security threats and identified these threats.

- Traffic Hijacking
- Insecure Interface and APIs.
- Denial of Service.
- Malicious Insiders
- Abuse of Cloud Services.
- Insufficient Due Diligence.
- Shared Technology Vulnerabilities
- Data Breaches

While cost and ease of use are the two main strong benefits of the cloud computing, there are some major alarming issues that need to be referenced when allowing moving critical application and sensitive data to public and shared cloud environment. The main aspect describing the achievement of any new computing technology is the height of security it provides whether the data located in the cloud is protected at that level that it can avoid any sort of security issue. So we must say that Security and privacy are the key challenges in the cloud computing. Here are some security issues, we have presented in this paper.

Data confidentiality issue: Confidentiality is a set of rules or an agreement that bounds access or location restriction on certain types of information so in cloud data reside publically so Confidentiality refers to, customer's data and computation task are to be kept confidential from both cloud provider and other customers who is using the service. We must make sure that user‟s private or confidential information should not be accessed by anyone in the cloud computing system, including application, platform, CPU and physical memory.

Data availability issue – when keeping data at remote location which is owned by others, data owner may face the problem of system failure of the service provider. And if cloud stops working, data will not be available as the data depends on single service provider. Threats to data availability are flooding attacks causes deny of service and Direct /Indirect (DOS) attack. Cloud computing is to provide on-demand service of different levels. If a certain service is no longer available or the quality of service cannot meet the Service Level Agreement (SLA), customers may lose faith in the cloud system.

Data integrity issue –as the word itself explains the "completeness" and "wholeness" of the data which is the basic and central needs of the information technology, As we know that integrity of data is important in the database equally integrity of data storage is important and necessary requirement in the cloud, it is the key factor that shaken the performance of the cloud. The data integrity proofs the validity, consistency and regularity of the data. It is the perfect method of writing of the data in a secure way the persistent data storage which can be reclaim or retrieved in the same layout as it was stored later. Therefore cloud storage is becoming popular for the outsourcing of day-to-day management of data .So integrity monitoring of the data in the cloud is also very important to escape all possibilities of data corruption and data crash. The cloud provider should provide surety to the user that integrity of their data is maintained in the cloud

IV. CONCLUSIONS

Cloud computing is the cost, time and performance effective technology. Of course the usage of cloud computing will surely will increase more in next few years. In this paper we have discussed and surveyed basic of cloud computing and security issues in the cloud computing. Some security issues are the key concern in the cloud computing. Especially privacy and integrity of data are the key concern security issues. In the cloud as data is stored publically and we really don‟t know where the data is being stored, we don‟t know the exact location of the data, due to this data stored in the cloud has a higher risk of being accessed by un- theorized person during storage as well as transmission.

REFERENCES

[1]The Forrester Wave™: Public Cloud Platform Service Providers' Security, Q4 2014 by Andras Cser and Ed Ferrara, November 17, 2014

[2] R. Latif, H. Abbas, S. Assar, and Q. Ali, "Cloud computing risk assessment: a systematic literature review," in Future Information Technology, Springer, Berlin, Germany, , pp. 285–295,2014.

[3] A. Avi˘zienis, J. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing,"IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11–33, 2004.

[4] Subashini S, Kavitha V (2011) A survey on Security issues in service deliverymodels of Cloud Computing. J Netw Comput Appl 34(1):1–11, 2011

[5] Keiko Hashizume1*, David G Rosado2, Eduardo Fernández-Medina2 and Eduardo B Fernandez1 "An analysis of security issues for cloud computing" Hashizume et al. Journal of Internet Services and Applications, 4:5 , 2013

[6] Mohammed A.AlZain, Eric Pardede, Ben Soh, James A.Thom2012."Cloud ComputingSecurity:From Single to Multi-Clouds" 2012 5thHawaii International Conference on System Sciences. 2012

[7] Yunchuan Sun, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu Data Security and Privacy in Cloud Computing Data Security and Privacy in Cloud Computing.

[8] D. H. Rakesh, R. R. Bhavsar, and A. S. Thorve, "Data security over cloud," International Journal of Computer Applications, no.5, pp. 11–14, 2012.

AUTHORS PROFILE

Indu Sharma.is a M.tech student in Rayat and Bahra college Sahuaran. Her areas of interest are Operating System Cloud Computing.

Mandeep Kaur Kang is a Assistant Professor in Rayat and Bahra college Sahuaran. Her area of interest is Digital Image processing, Cloud computing.

