ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

A Survey on Security Challenges in Cloud Computing

Dr.K.Ratna Babu [1], Dr.G.Charles Babu [2]

Lecturer, Department of Computer Engineering, Government Polytechnic, Addanki, Prakasam Dt, A.P.India[1]

Professor, Department of C S E, Malla Reddy Engineering College(Autonomous), Hyderabad, Telangana, India[2]

ABSTRACT: The importance of the cloud is increasing exponentially and people start realising the reliability, scalability, and efficiency of the cloud computing. In recent generation since around 2008 the hype increasing like anything. Dramatically the cloud size increasing, and the problems also in the same fashion. Despite the potential advantages of cloud the organizers are slow down accepting the cloud services provided by service providers. In cloud the organizations store their data by handover it to service providers or third party who own the infrastructure. In this way the data is most vulnerable in cloud network it is obvious that there is lots of security issues need to be concern both for the normal client and business oriented client. Although the service providers guarantee the security in terms of technical aspects, but it is very difficult to achieve clients trust. In the present paper a review on security issues, how to challenge them and cloud manageability is presented.

KEYWORDS: Cloud, security issues, cloud networks, cloud services, cloud computing.

1. INTRODUCTION

Cloud services become more popular for even for a normal person because people can access social networking sites, photo sharing sites, email and chatting. The Cloud computing refers internet services which allow the clients to save their data at remote locations instead of using home hard disk or any other home devices. In cloud the client uses some others resources to store their data and applications. Here the clients store their personal data or business data or both in the remote systems. The clients need not to purchase any infrastructure or need not to upgrade their infrastructure at home or their organizations. That means client utilises some others infrastructure which are placed domestic or foreign whereabouts. The cloud not only provides data storage facility it provides lot of shard base pool of sources. Like grid computing the clients can share all the resources of the cloud. Heterogeneous systems and platforms can share all the resources. The cloud provides different resources like networks, softwares, and operating systems. The client need not to spent money on purchasing all these resources to process all their current and future requirements. The cloud user can use third party infrastructure to store all the data or to process the data. The cloud can take the data as input from the client and implement some operations on the data as per the client requirement and updates the results back to client, which are obtained from the operations done in cloud. These operations are done with the help of softwares available on cloud. So the clients need not to install the softwares on systems. So, the client can avoid unnecessary software installations time, and upgrading new software configurations. Indirectly the user is hiring required software and hard ware from service provider.

In this way the cloud extends the services for an organization or individual to increase their capabilities. They need not to spent heavy expenditures to renew their software licence, investing in up gradation of hardware, save time in training to run softwares. The statistics are saying that cloud computing has grown enormously than any other segment in IT. Day by day the number of organizations and individual clients is drastically increasing in cloud segment. Although the companies and users are more enthusiastic in amalgamation to cloud, still users are more concern about their privacy and security. Despite of their interest towards cloud services they are more anxiety about data security and privacy.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Still Cloud services are popular because of their reliability, efficiency, and scalability. The cloud provides unlimited storage capacity, more reliable to access the day from anywhere in the universe, and more efficient because it allows the companies to run their applications successfully more accurately even in the absence of their products. Despite of their fear clients are excited to used cloud services because it drastically reduces infrastructure maintenance cost and complex in networks. Clouds can also provide extra services in which providers are expertise to some small companies, such as email systems, along with data maintenance.

The cloud computing has been defined by the U.S. National Institute of Standards and Technology (NIST) as, "the cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". [1][2].

Cloud has potential benefit of providing high security to clients by storing all the data in highly secured control rooms. Cloud has less prone of loss of data from their data management systems. The data will be stored in highly technical infrastructure located in one domicile or domestic they can be retrieved even in case of natural calamities. The multinational companies can serve their clients throughout the world by sharing their data into different cloud servers located at different nations. Social networking sites, multinational organizations run their operations successfully with the help of cloud providers. But the locating and sharing of data between servers may raise the scale of exposure to possible breaches both accidental and deliberately [3]. Some cloud providers sharing their customer personal information to business organization or some other adverting agency for their benefit without providing full information to the customer. The client them self must be vigilant while sharing their data to cloud to whom it is shared and on what network and on what type of condition. Only the client need to be assured by them to which provider they are sending and in this context there must be transparency between a client and cloud provider.

Hence, the clients are more stimulating to reduce capital cost and divert that amount for the future expansion and research. But, finally the standards are immature and insufficient to handle current technologies [4]. A user has to consider many factors while moving into cloud. They have to check the availability of good internet connections to avoid data latency. In natural calamities, network failures, clients need to confirm how cloud service providers are able to secure clients data and how the cloud providers giving privacy to their cluster of data.

II. ARCHITECTURE OF CLOUD COMPUTING

As per NIST the cloud is composed of five essential characteristics, three service models, and four deployment models [1][4]. Typical cloud architecture looks as shown in figure 1. It contains clients accessing cloud resources through terminals and various cloud service providers [7].

2.1 Essential Characteristics

2.1.1 Resource Pooling: It describes about the clients selects a service or multiple services from pooled resources available at the service provider or third party who own the infrastructure. The pool of resources contains storage, software, and network infrastructure resources. Broad network access allows sharing services to different organizations via internet or private networks. These resources are pooled as part of service delivery. This type of pooling system services are provided as tenant to serve their services through various resources.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

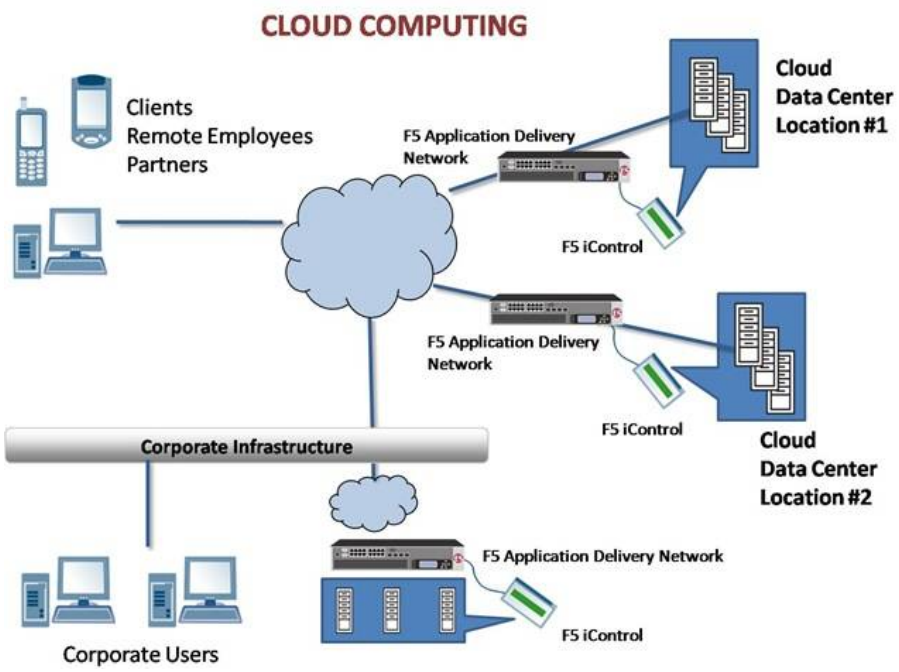

Figure 1: Basic Cloud Architecture [7]

2.1.2 **Resource Egalitarianism:** This labels that any user on the cloud can access all types of cloud services. All the pooled resources made available by the service provider, and grant authentication to all clients on the network to access the resources by standard methods.

2.1.3 **Service oriented Architecture:** As the abstraction of infrastructure from cloud application yields that cloud resources are allowed to access but not management of infrastructure by cloud democratic clients. On-demand self-service means usually organizations can request and manage their own computing resources.

2.1.4 **Rapid Elasticity:** This indicates the size of the cloud service. The client can select the number of services and the scale of the cloud. According the scale of the cloud the client pay bill to the provider. For instance, the domain owner will pay the maintenance bill to the service provider according to the size of the resources in terms of the storage, software, and server services allocated to the client that to for a stipulated time period. The client at any time can increase his requirement level capacity. Dynamically the service provider must be able to provide all the extra resources demanded by the client. Since all resources are pooled at the cloud the client can achieve maximum services that they demanded.

2.1.5 **Utility model of consumption and allocation:** The rapid elastic nature of cloud tightly automated. The automated cloud has a provision of self service provider. It allocates services dynamically depends upon the utilization scale of the customer. The utilization scale is representing the client previous usage and demanded for resources. These measurements help the customer a lot to predict the current usage level. Hence the client will pay only for the required level of services. For instance the mobile network utilizer can select appropriate plan based on the reviews and predictions produced by automated software provided by network provider.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

2.2 Service Models

The service of the cloud is deployed to client in three model forms. Service providers may also include systems integrators that build and support data center hosting private clouds and they offer different services. The cloud user has no idea and worry about the internal arrangement of the cloud service provider network [4][5][6][8]. Service models allow the clients to develop complete Software Devolopment Life Cycle. The cloud computing service models used to deploy client services are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). IaaS is the base layer for all service levels, and SaaS building upon PaaS as shown in figure 2.

2.2.1 Software as a Service (SaaS): In this model a complete pre- defined application along with any required software is provided to the client. On the user side the users no need to invest for software up gradation and purchase new software. Only a single application needs to be installed and managed by the customer. The customer has no rights to control network, operating system, servers, and infrastructures. SaaS is accessed via web browsers over internet. So Web browser security is important. Startups and business people can run their ideas on SaaS with collaboration of service providers.

2.2.2 Platform as a Service (PaaS): In this model system software is provided as service to create a development environment. The customer has a freedom to design their own application which runs under cloud infrastructure. The Virtual machines provide the PaaS layer in cloud computing. Virtual Machines must be protected by malicious software by accurate authentication throughout the network.

2.2.3 Infrastructure as a Service (IaaS): This model providing all storage services and computation capabilities to the client. Some cloud providers are providing this service with free of cost up to certain storage limit which is more help full for researchers, startups, and other small scale clients. IaaS allows startups and other business clients to consume the infrastructure without worrying to spend expenditures on core infrastructure developments. The Cloud is compelled to spend more expenditure on IaaS but now many of the providers came out from this problem as the IaaS tenants number is growing. The History of cloud computing is shown in figure 3 [7].

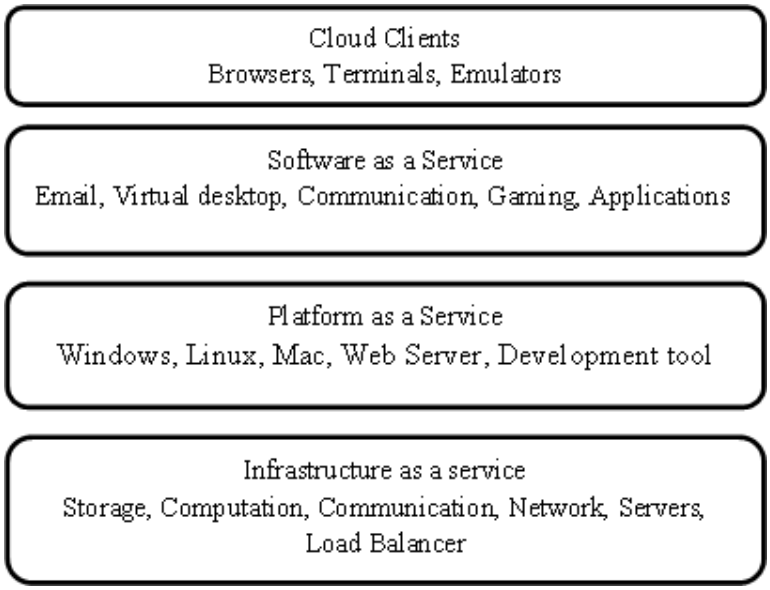

Figure 2: Levels of Cloud service Delivery models

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

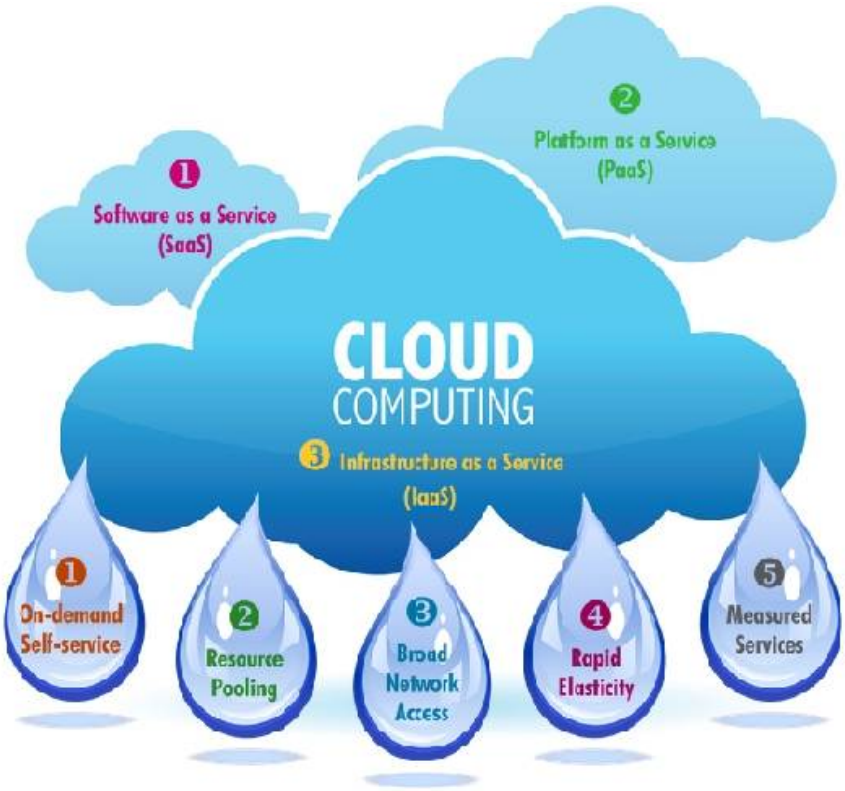

Figure 3: History of Cloud Computing

2.3 Deployment models

There are four ways of how a cloud provider deploys the services to the client. They are Public, Private, Community, and Hybrid cloud [4][8].

2.3.1 Public Cloud: Pubic cloud is designated by cloud provider and services are offered by internet. Public clouds are operated with multi-tenant and offers benefits of elasticity and the accountability/utility model of cloud [4]. Public clouds are less secure and less privacy when compared with other clouds, because the documents in the cloud are accessible and manageable by different clients.

2.3.2 Private Cloud: The private cloud is designated for an organization or few organizations. The data is setup for that organization only. It provides high security and privacy, but costs more to deploy separate architecture for an organization. That means it allows only those organizations can access pool of resources in the cloud. There is possibility of security threat for private cloud because of possibility of malicious software attacks and hackers from outside competitors.

2.3.3 Community Cloud: This cloud is created between know people. In recent days people are complaining about their data security and privacy. They are managed by cloud providers. As the community cloud network increasing enormous problems are facing by clients and as well as by the cloud provider. There is problem of losing sensitive data in community cloud. There is chance of hack the client data base for misuse or steal the information of an person or organization. They have a large benefit of elasticity and the accountability/utility model of cloud.

2.3.4 Hybrid Cloud: It is the combination of both public and private 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 [9]. It provides virtual IT solutions through a mix of both public and private clouds [8]. It allows different clients to access the cloud services through different gadgets and networks. In hybrid cloud, a service

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

provider utilizes third party services to increase flexibility of computing. Here the clients need to ensure the authentication of the third party service provider. The cloud provider must be transparent in providing the details of third party.

III. SECURITY AND PRIVACY ISSUES IN CLOUD

The cloud includes various technologies like database, network, operating system, softwares, virtualisation, and storage management. So, security issues of these systems are applicable to cloud. Also virtualization leads many security concerns. Data security is highly essential while copying data from virtual machines to physical machines. Data base systems must effectively work in detecting malware software systems and intruders [4][10][11][12]. Mainly there are four types of issues need to be considered while discussing security issues. They are Data issues, Privacy issues, infected applications, and Security issues.

III.1 Data Issues

In the cloud from anywhere and anyone can fetch the data in the cloud. It is very embarrassing if somebody sees or acquires one's sensitive data. It is a very big challenge in cloud to provide security from intruders and avoiding accessing one's account by some other or un known person. In some cases the cloud providers does not store the data directly in their systems. The cloud providers store the data at third party vendors to save their infrastructure or to reduce expenses or to provide high security. This may lead data steal in the cloud. In this case it is very important for a client to know third party location. During data transition there may be a chance of data loss. The data loss may occur due to network failure on the cloud infrastructure, power failures, natural calamities, or due to legal problem. Some cases the cloud provider receives the data and computation on the data is done at some third party agencies. After the computation the results again store at cloud provider to allow the client to access the results. During the data transition there is a chance o misuse the sensitive data by intruders.

III.11Privacy Issues

It mainly deals with customer personal and sensitive information. The community cloud there is a chance of external people interference in their account. Although there is proper and secure authentication other will intrude into the cloud because of client mistakes or innocence.

III.III Infected Applications

This is mainly deals with malicious software. This type of problem may severely damage the client system but also cloud service models. The providers and client must be aware of the softwares they are using and downloading. This method can prevent downloading unknown and malicious software.

III.IV Security Issues

The cloud computing service provider makes sure that there service is secured and less threatened. Although the service providers provide security the clients need to be ensuring that there is no loss in the data or steal. A service provider is said be successful only if they able to provide a secure data and creates trust in client minds.

IV. TECHNIQUES TO FACE SECURITY ISSUES IN CLOUD

The data issues can be managed by providing proper authentication while logging into cloud. While using third party vendors it is very important to see that they are providing their services under government rules and regulations. There must be a regular government committee to see all cloud activities and third party activities at regular intervals of time. The privacy of a customer can be maintained by regular monitoring of the server provider and be sure who is maintaining server. Proper anti-virus softwares must be installed both in client and at cloud provider side. Cloud provider must ensure these softwares must be regularly upgraded. Typically the virtual machines provide high security with the help of virtual network separator.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

V. CONCLUSIONS

The cloud is creating wonders and revolutions in the internet world. Although it has many advantages it is also highly essential to think about challenges in the cloud computing securities. The scale of cloud services are radically increasing but still it need have improvement in the scale when compared with size of network. The cloud service providers need to be very cautious who is uploading and what content on the cloud. It is highly essential for the service providers to scan their data base with high and efficient softwares. For accessing sensitive data client authentication is highly essential to login and accessing the data. Service providers also need to check their virtual machines locations and who is operating those machines. The service providers need to check their cloud network throughout their network regularly, for identifying intruder, malwares, port disconnections, power loss, wavering of hardware, and local disasters. Finally for cloud providers, it is very important to offer their services within the national legal issues and obligations to gain the client trust. Before all, the client prime responsibility is use cloud by knowing the service providers details. It is highly secure to use standard cloud service providers, genuine and who are registered organizations. Still many governments are framing rules for cloud to face security issues and other obligations in critical situations.

REFERENCES

[1] NIST cloud definition, version 15 http://csrc.nist.gov/groups/SNS/cloud-computing/
[2] Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2011). Draft Cloud Computing Synopsis and Recommendations. National Institute of Standards and Technology (NIST) Special Publication 800-146. US Department of Commerce. May 2011. Available online at: http://csrc.nist.gov/publications/drafts/800 -146/Draft-NIST-SP800-146.pdf.
[3] Casola, V., Cuomo, A., Rak, M. and Villano, U. (2013). The CloudGrid approach: Security analysis and performance evaluation. Future Generation Computer Systems, 29, 387–401. doi:10.1016/j.future. 2011.08.008.
[4] Jaydip Sen, "Security and Privacy Issues in Cloud Computing", Technical Report, Innovation Labs, Tata Consultancy Services Ltd., Kolkata, India.
[5] Rabi Prasad Pet al., "Cloud Computing: Security Issues and Research Challenges", IJCSITS, Vol. 1, No. 2, December 2011.
[6] Monjur Ahmed et al., "Cloud computing and security issues in the cloud", IJNSA, Vol.6, No.1, January 2014, pp25-36.
[7] Technical report by http://america.pink/cloud-computing_1024784.html
[8] Kuyoro S. O, "Cloud Computing Security Issues and Challenges", (IJCN), Volume (3) : Issue (5) : 2011, pp247-255.
[9] Global Netoptex Incorporated. "Demystifying the cloud. Important opportunities, crucial choices." pp4-14. Available: http://www.gni.com [Dec. 13, 2009].
[10] Sen, J. & Sengupta, I. (2005). Autonomous Agent-Based Distributed Fault-Tolerant Intrusion Detection System. In Proceedings of the 2nd International Conference on Distributed Computing and Internet Technology (ICDCIT'05), pp. 125-131, December, 2005, Bhubaneswar, India. Springer LNCS Vol 3186.
[11] Sen, J., Sengupta, I., & Chowdhury, P.R. (2006b). Architecture of a Distributed Intrusion Detection System Using Cooperating Agents. In Proceedings of the International Conference on Computing and Informatics (ICOCI'06), pp. 1-6, June, 2006, Kuala Lumpur, Malaysia.
[12] Sen, J., Ukil, A., Bera, D., & Pal, A. (2008). A Distributed Intrusion Detection System for Wireless Ad Hoc Networks. In Proceedings of the 16th IEEE International Conference on Networking (ICON'08), pp.1-5, December 2005, New Delhi, India.
[13] Irena Bojanova et al., "Cloud Computing", IT Pro, IEEE Computer Society, doi: 1520-9202/13, March/April 2013.
[14] Ting Wang, "Rethinking the Data Center Networking: Architecture, Network Protocols, and Resource Sharing", Journal for Rapid open acces, IEEE Access, Vol 2 2014, pp1481-1496.