JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Cloud Computing Access: A Major Security Issue in Digital World

Dr. Banta Singh Jangra
Asstt. Professor of Computer Science
Govt. College, Hansi (Hisar) Haryana, INDIA

Abstract

In this paper I, have reviewed and elaborated cloud computing techniques which are used in large scale by the end users worldwide. Cloud computing is used by many of the organizations for storing the huge amount of data on the clouds i.e. text file, audio and video etc. Cloud computing is the on demand availability of various types or format computer system resources, especially in data storage and management, every end user may access their electronic resources from anywhere, everywhere. Cloud computing relies on sharing of resources to achieve coherent and typical uses pay as you go which is help to reducing capital expenses for unexpected operating and computing expenses for users.

Keywords: Cloud Computing, Database, Operating System, Remote Access

1. INTRODUCTION:

Cloud computing has defined by National Institute of Standards and Technology is comprehensive and recent rising technology in the digital world for end users to provide on demand web services like networks, data storage, remote servers and applications with flexibility and cost efficient. Software Developers describe Cloud in a different way than a System Administrator, while a Database Administrator may have different definition. Cloud means a wide range of scalable services that users can access via an Internet connection. Cloud computing is the on-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user physically. The cloud computing techniques often have functions distributed over multiple remote locations, each of which is a data center or service provider's entire world. Cloud computing relies on sharing of resources to achieve coherence and typically uses a pay-as-you-go model, which can help in reducing capital expenses but may also lead to unexpected operating expenses for users.

Cloud computing is a modern technology that increase or reduce the storage capacity as peruse without investment in new infrastructure by the each and every end users. The major process of cloud computing storage contains different layers newly storage layer that store data on cloud remote data center, management layer which ensures privacy & security of remote cloud storage, application interface layer that provide cloud application service platform, and finally cloud access layer which provide accessibility to all the cloud computing user.

2. CLOUD INFRASTRUCTURE AND ARCHITECTURE

The cloud computing technique basically comprises two major modular i.e. service and deployment. The services like platform, networking, storage, and software infrastructure are provided as services that scale up or down

depending on the demand. The deployment model also further divided in to three models:

- **Private**

Private cloud model is a new technology that some vendors have recently used to describe offerings that imitate cloud computing on private networks. It is implemented within an organization's internal enterprise data center. This architecture is implemented and executed exclusively for an implemented organization and is only utilized and used by their workers at the authoritative level and is managed and controlled by the organization or third party. The cloud infrastructure in this model is installed on organizational premise or off premise. Thus in deployment model, management and maintenance are easier, security is very high and the organization has more control over the infrastructure and accessibility. In the private cloud, adaptable resources and virtual applications are pooled together and made accessible for cloud service consumers to share and utilize. It varies from the public cloud model in that all the resources and application services on the private cloud are managed and maintained by the organization itself, like Intranet functionality in an organization. Working on the private cloud can be much more secure than that of the public cloud because of its specified predefined internal secured exposure in an organization. In private cloud only, the organization and assigned stakeholders may have access admittance to work on resources.

- **Public**

Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provided on a self- service, fine grained 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. Generally, the service is 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. 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. Data and communication protection plays a vital role in Cloud computing. Services can be accessed through a thin client, laptop or mobile phone. The reasons that your data is easily accessible through these channels are your data is transferred across multiple networks, when your cloud service provider is extremely far away from your location.

- **Hybrid**

The hybrid cloud model is a merger of two or more kinds of cloud deployment models such as private, public or hybrid. The participating clouds are bound together by a standard set of protocols. It enables the involved organization to serve its requirements in their own private cloud and in the case of critical needs cloud bursting for load-balancing occur they can avail services from the public cloud. It caters the virtual IT enabled services through a mixture of both public and private clouds services. Hybrid cloud provides more secure control of the data & applications and allows various clients to access data/information over the Internet. The hybrid cloud has an open architecture that allows interfaces with other management systems. Hybrid cloud can describe configuration combining a local computing device, such as a Plug computing system with cloud working administrations. It can also depict configurations combining virtual and physical, collocated virtualized environment that requires physical servers, routers, or other hardware components.

3. CLOUD COMPUTING: SERVICE MODELS

Cloud Computing may be accessed through a couple of IT Remote services. These cloud computing services are designed to exhibit certain characteristics and to satisfy the organizational requirements. From this, a best suited service can be selected and customized for an organization's use. Some of the common distinctions in cloud computing services are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS),

Infrastructure-as-a-Service (IaaS), Hardware-as-a-Service (HaaS) and Data storage-as-a-Service (DaaS). Service model details are as follows:

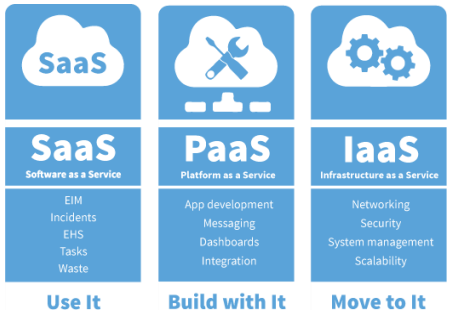

Figure-1: Cloud Service

- **Software as a Service (SaaS):** The service provider in this context provides capability to use one or more applications running on a cloud infrastructure. These applications can be accessed from various thin client interfaces such as web browsers. A user for this service need not maintain, manage or control the underlying cloud infrastructure (i.e. network, operating systems, storage etc.).

- **Platform as a Service (PaaS):** The service provider in this context pro- vides user resources to deploy onto cloud infrastructure, supported applications that are designed or acquired by user. A user using this service has control over deployed applications and application hosting environment, but has no control over infrastructure such as network, storage, servers, operating systems etc.

- **Infrastructure as a Service (IaaS):** The consumer is provided with power to control process, manage storage, network and other fundamental computing resources which are helpful to manage arbitrary software and this can include operating system and applications. By using this kind of service, user has control over operating system, storage, deployed applications and possible limited control over selected networking components.

- **Hardware as a Service (HaaS):** The idea of buying a hardware or an entire datacenter with a pay-as-you-use scheme which can scale up and down as per user requirements can be termed as Hardware as a Service (HaaS).

- **Identity as a Service (IDaaS):** This service is targeted for third party service providers who provide Identity and access control functions (including user's life cycle and sign-on process). This can be used in combination with various other services (software, platform or infrastructure services) and also for public and private clouds.

- **Data storage as a Service (DaaS):** This service allows user to pay for the amount of data storage he/she is using. With this service there is a separate cloud formed which provides storage as a service.

- **Security as a Service (SaaS):** This service allows users to create their own security policies and risk frameworks. In this kind of service cloud users must identify, assess, measure and prioritize system risks.

4. MAJOR SECURITY TECHNIQUES

- **OTP Authentication and Verification Process**

In the current scenario, many of banks are providing authentication through One Time Password (OTP) method which is generated through random under generation and used to verify the cloud user sometime it is used for one time authentication called as system factor authentication that is shown in figure 3. While sometime it is used for two time authentication called as Multiple Authentication Factor.

Figure-2: OTP Authentication and Verification Process

- **Proper Integrity Verify**

The integrity of cloud data is a guarantee that cloud data can only be changed or accessed by an authorized user. In simple terms, it is a cloud-based data verification process ensures that the data is unmodified, correct and the basic techniques of data integrity are Provable Data Procession (PDP) is a technique to ensure the integrity of cloud data on a remote server and the technique Proof of Retrivebility (POR) to obtain and verify the evidence that cloud data is stored by the user on the server is not changed.

- **Remote Access Control**

Access control means cloud data owner can execute some restrictive permission to access their data outsource to cloud and data owner's authorized user can access cloud data while unauthorized user can't due to access control cloud data are protected from modification or unauthorized disclosure of data.

- **Encryption and Decryption Technique**

Cloud security provides data encryption service to encrypt cloud data before transfer from local storage to cloud storage and it is impossible to understand from any system, database or file to decrypt data without decryption key and encrypted data is only possible to access with an authorized user with the decryption key and separation of encrypted data and encryption key is necessary for keeping cloud data secure.

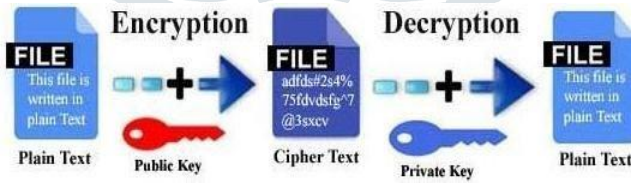

Figure-3: Data Encryption and Decryption

- **Data Hiding and Masking**

Data hiding and masking is a process of securing and hiding cloud data from unauthorized attackers and theft and it also insure that the information is changed with realistic but not real information. While people interchangeably use terms such as data de recognition, data cleansing and understanding the term defining the confusing process. Data hiding and masking is not only algorithm but also a public data set.

5. CONCLUSION AND FUTURE SCOPE

In the modern access technique of cloud computing the end user may access anytime, anywhere of remote data stored on word wide remote locations on 24x7 with as virtual access techniques to realize the local drive access. Data hiding and masking technique for unauthorized access control is the major concern for cloud users and maintain their personnel data security.

For the future researches the recommendations are as to reconnect the ideas of cloud computing is to increase access speed with network bandwidth for end users.

REFERENCES

1. Kumar Jaydip, Cloud Computing Security Issues and Its Challenges: A Comprehensive Research, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-1S4, June 2019
2. Jagli Shankar Dhanamma, Rohan Jathanna. Cloud Computing and Security Issues, Int. Journal of Engineering Research and Application ISSN : 2248-9622, Vol. 7, Issue 6, (Part -5) June 2017, pp.31-38
3. Vaikunth Pai T. & P. S. Aithal, Cloud Computing Security Issues Challenges and Opportunities, International Journal of Management, Technology and Social Sciences (IJMTS), ISSN: 2581-6012, Vol. 1, No. 1, 2016.
4. https://en.wikipedia.org/wiki/Cloud_computing
5. Mohamed Magdy Mosbah, "Current Services in Cloud Computing: A Survey ," International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.3,No.5,October 2013
6. R. Choubey, R. Dubey, and J. Bhattacharjee, "A survey on cloud computing security, challenges and threats," Int. J. Comput. Sci. Eng., vol. 3, no. 3, pp. 1227–1231, 2011.
7. R. P. Padhy, M. R. Patra, and S. C. Satapathy, "X-as-a- Service: Cloud Computing with Google App Engine, Amazon Web Services, Microsoft Azure and Force.com," Int. J. Comput. Sci. Telecommun., vol. 2, no. 9, pp. 8–16, 2011.