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

A REVIEW ON DATA STORAGE AND SECURITY ISSUES IN CLOUD COMPUTING

[1]Sunita Patil,[2] Shubhangi Suryawanshi ,[3] Vanita Kshirsagar
[1]Asst. Prof., [2]Asst. Prof,[3]Asst. Prof
Computer Department, D.Y.Patil Institute of Technology,Pimpri,Pune
India

Abstract : This review paper discusses data storage and security issues in cloud computing. Data security was discussed mostly because the validity of data is so essential to cloud customers. The cloud computing does not deliver control above the stored data in cloud data centers. The cloud service providers have full of control above the data, they can achieve any malicious tasks such as editing, copy, deleting, updating etc. Data security was discussed mostly because the validity of data is so important to cloud customers. This paper gives a detailed summary of the security issues of several aspects that affect cloud computing. Confirming that stored data is kept private and secure from unauthorised users as well as free from malicious or unintentional alterations is difficult task.

***IndexTerms* –Data Integrity, Malware and Worms, anonymity.**

I. INTRODUCTION

In a few earlier years, the idea of cloud computing was the fast increasing idea in the IT professional. Cloud computing provides provision and training for new persons. Cloud computing provides amazing potential for providing its clients and end users with the services they requisite in a flexible manner and at least cost. Because of cloud easiness everyone is selecting data and application software to cloud data centers. However, when businesses place their data in the cloud, they are so conscious of the environment that it is secure compared to their on- premises data centers.The only encryption doesn't offer full control over the stored data but it offers somewhat well than plain data. The characteristics of cloud computing are virtualization and multi tenancy also has various options of attacks than in the common cloud model.

Cloud computing is an effective process for quickening performance or increasing ability without adding new setup. The key necessity for the end user is to have entrée to reliable data in the shortest possible time. Security is the primary concern of this new vision of computing power.

Components of Cloud Computing: It consists of a many services that we can usage across the internet.

- **Virtualization:** This component makes a major function in deploying the cloud. It is the strategic component in the cloud computing, which allows the physical resources shared by several consumers. It develops and creates the virtual instance of each resource such as network resources, servers, operating system and storage devices.
- **Cloud Network:** Cloud networking is essential for secure and effective sharing network and storage devices. Internet connection is required which allows the users to access the printers, storage devices or any other application in a secured location. It consists of many data centers. A number of servers are existing in a data centre.
- **Multi-Tenancy:** The Multi-tenant situation have a large number of users who have no access to get the data of each other but users can share the application and resources in an execution situation, although did not belong to the similar business institute. The results of Multi-tenancy environment are best and there is maximum consumption of data storage techniques and hardware.
- **The Hypervisor:** It monitors and manages the many operating systems, which run in a common physical system. This manager or virtual machine monitor is an important key module of virtualization. It permits many Virtual Machines to run on a single hardware host.

II. LITERATURE REVIEW

Cloud computing states to both the applications sent as services over the Internet and the hardware and systems software in the data centres that provides those services. Cloud Service Delivery Models and their Security Issues: Internet and Big Data Cloud Computing technology raise. After a huge number of researches, the service delivery models are PaaS, IaaS and SaaS.

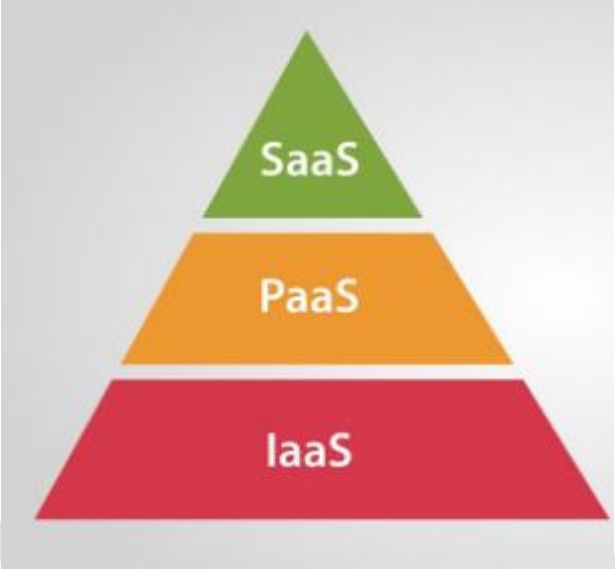

Fig.1 Cloud Delivery Models

Software as a service (SaaS): SaaS is a platform of remote cloud services.It is at the top of list. It allows the users to use the facilities of cloud infrastructure via the internet. In this model, cloud suppliers work the software in the cloud and also users have the access of application .It is not the duty of Cloud users to achieve the platform where the software and application runs. Thus there is no prerequisite to install the applications on the customer's personal computer or Laptop. This is a clean process for the user. Client is fully reliant on on the provider of service for data accuracy and correct security.

Security

Problems in SaaS: Following are the main areas where we can measure security.

Security of Data in cloud computing is key concern because data storage is the essential of every organization. Data security is a big problem in distributed system and online application and software. Each association stores its sensitive data within its border. SaaS service supplier must ensure security checks. This dimension includes the encryption procedures for the security of data. Data is very important for everyone and the main goal of cloud service is also to ensure high availability of data to the client.

Platform as a service (PaaS): Platform as a service is a middleware of service model. A well-known PaaS source is Google App Engine. Google App Engine is a Development Set which provides a platform that supports Java, Python etc. The client regulate the applications but do not know that how the resources are managed. It may be so helping where number of developers is working at different places but they work together.

Security problems in PaaS: In PaaS, the supplier of service switches the control to the user to plan applications at this platform. So Application security level such as network and host will be in the scope of the service supplier. The service supplier has to make sure that the data will never be accessible to other applications. This method makes allow to developers to design their own applications by this platform.

Infrastructure as a service (IaaS): It is the bottom of Service Delivery Model. IaaS contain with hardware (Data Center, Processor, virtual Server Machine ,Network Storage and Memory) as a service. Cloud infrastructure does not regulate by the consumer but it possesses control over applications.

Security Problems of IaaS: In IaaS the application designer has trustworthy control over the security. Owner of data should hold and control over data. Dissimilar techniques are used to gain the trust on the security offered by a cloud service provider. For example, it's a vendor duty to provide security from each side. The second stage is reliable data which is protected in hardware of service provider.

III. DATA STORAGE

Cloud Storage is used to save data on offsite storage system maintained by third-party and is made available by a web services API.Types of Storage Devices. Storage devices can be classified into two categories:

- Block Storage Devices
- File Storage Devices

Block Storage Devices:-Block storage splits big volumes of data into minor units called blocks. Each block is linked with a unique identifier (ID) and located on one of the system's storage drives. With object storage, data can be stored in its native plan with huge scalability. To retrieve data, the user provides the ID to the system and the data is collected with all its metadata, security and authentication. Object storage systems permit metadata to be modified, which can modernize data access and analysis.

File Storage Devices:-File storage arranges data in a hierarchical manner of files and folders. It is normally used with personal computer (PC) storage drives and network-attached storage (NAS). Information in a file storage system is stored in files and the files are stored in folders. Directories and subdirectories are used to establish the folders and find files and information.

IV. ISSUES IN DATA CLOUD STORAGE

Anonymity:-Anonymity is a method to ambiguous the published data and key information preventing the associated identity of the owner of data.Data anonymity has different vulnerabilities such as the hidden identity of adversary threats, gaps in the process of re-identification.

Account Traffic Hijacking: -It is typically done with stolen credentials (ID & Password) and remains a highest hazard. With stolen credentials, attackers (hackers) can often access dangerous zones of deployed cloud computing services, permitting them to concession the integrity, confidentiality and availability of those facilities.

Availability:- The important goal of cloud service is to deliver high availability to the user. Its intention is to confirm that a client can get information anywhere any time. The cloud storage wants in availability quality because of flooding attack in the network.

Data Loss and Leakage:-Data loss may occur when disk drive expires without creating any backup.It is the loss of confidentiality, belief and has a direct result on the Service Level Agreements (SLA) policy, which are the main worries of cloud users.

Integrity and Confidentiality Issues: -Integrity is the most critical part in the information system in order to defend the data from unauthorised alteration or deletion. The security issue occurs when wrongly defined security parameters or wrongly configured VMs and hypervisor are used with malicious intent.

Malware and Worms: -This includes an e-crime attack to insert malware into cloud storage called 'Botnets' turning them into 'zombies' targeting at attacking bigger network servers' computers.

V. CONCLUSION

Cloud computing results the beginning of a new platform in the pitch of data and communication technology as it transfers with an development ideal which has the possible to change the way in which computing was done.The cloud computing architecture supplies data and application software with minimal management effort and provides on demand services to customers through internet. But with cloud management customer don't have faith worthy promises.This will clue to many security problems with data storage such as confidentiality, integrity, privacy and availability. This review paper focused on data storage security problems in cloud computing and paper provided service models of cloud, deployment models and variation of security problems in data storage in cloud background.

.

REFERENCES

[1] A. Abbas, K. Bilal, L. Zhang, S.U. Khan, A cloud based health insurance plan recommendation system: a user centered approach, FutureGener. Comput. Syst. (2014)
[2] P. Mell, T. Grance, The NIST definition of cloud computing (draft), NIST Special Publ. 800 (145) (2011) 7.
[3] J. Che, Y. Duan, T. Zhang, J. Fan, Study on the security models and strategies of cloud computing, Proc. Eng. 23 (2011) 586–593.
[4] R. Chandramouli, M. Iorga, S. Chokhani, Cryptographic key management issues and challenges in cloud services, in: Secure CloudComputing, Springer, New York, 2014, pp. 1–30.
[5] C. Wang, Q. Wang, K. Ren, N. Cao, W. Lou, Toward secure and dependable storage services in cloud computing, IEEE Trans. ServicesComput. 5 (2)(2012) 220–232.
[6] M. Balduzzi, J. Zaddach, D. Balzarotti, E. Kirda, S. Loureiro, A security analysis of amazon's elastic compute cloud service, in: Proceedingsof the 27th Annual ACM Symposium on Applied Computing, 2012, pp. 1427–1434.
[7] Duncan, Adrian, Sadie Creese, and Michael Goldsmith. "Insider attacks in cloud computing." Trust, Security and Privacy in Computing andCommunications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012.
[8] https://www.entrepreneur.com/article/335155
[9]MazharIqbalNoor, "Security Problems in Service Delivery Models of Cloud Computing - A Survey"VFAST Transactions on Computer Sciences, January-December, 2020
[10]Sunita R Patil, SandeepKadam," RS-MONA: Reliable and Scalable Approach for Secure Multi-Owner Data Sharing For Dynamic Groups in the Cloud", International Journal of Computer Applications (0975 – 8887) Volume 102– No.3, September 2014.