International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol. 9, Issue.2, February 2021 E-ISSN: 2347-2693

Cloud Computing: Models, Issues and Challenges

Komala R.[1*], Pranavi B.V.[2]

[1,2]Department of Computer Applications, Sir MVIT, Bengaluru, Karnataka, India

DOI: https://doi.org/10.26438/ijcse/v9i2.5759 | Available online at: www.ijcseonline.org

Received: 28/Jan/2021, Accepted: 04/Feb/2021, Published: 28/Feb/2021

Abstract— In modern days, Cloud storage service is being increased tremendously for storing the data. Cloud computing is the new development in the IT industry now a days. The main advantage of cloud storage service is that the data can be downloaded from any location and at any time without any limitation. But, data security is considered as main issue in the cloud computing. Mainly sharing of resources will have major issue in the data security. Cloud deployment models, delivery models are High level cloud architecture is being explained with its four levels. Various challenges and security issues in this cloud computing has been stated clearly in this paper.

Keywords—Secuirty, Storage, Cloud Services, Data Center, Deployment Models.

I. INTRODUCTION

The business as and when it expands, the data grows in and demands more storage area for the accumulated data. In traditional data whenever we wanted to add some data, we start add more disk arrays into the control. It becomes very difficult to access and we also make use of secondary system for the backup of data to protect the data. We used to have idea on where all the data is being sent. If there exists branches, then there will be one acceleration which will be made available to branch offices giving those branch offices access to all the data which is being stored in primary data centre. If there exist mobile workers then another layer is created which will then increase the complexity. To overcome these complexity and security a storage controller with an integrated component called cloud is being used. Cloud is used not only in storing the data but also as an efficient and flexible alternative to computer. Here in the cloud, the data and applications are stored on collection of web servers called cloud and computers. In most of the cases the cloud will be owned and maintained by the third parties. Using the cloud computing systems interface software the data can be accessed from the cloud. It is really important to understand how cloud storage works from cloud computing providers, by demand via internet Cloud service does any service made available to users. Cloud is a service delivered over internet. Here, in this cloud service that data can be backed up, managed and accessed remotely. In the enterprise level, cloud storage is mainly used in DevOps projects, Archiving files and data, disaster recovery and data backup. Cloud has three important features like it has unlimited capacity, data is not supposed to backup regularly as it has its own protection mechanism they will automatically backup the data and cloud can store any kind of data.

II. CLOUD STORAGE

For any type of cloud storage, there exists two parts called front end and back end. These both will be connected through internet. Front end will be the computer that we use as a client. We are required to access the cloud computing system through an internet browser or by using unique interface software. The backend will have Computer servers, computer networks, Database storage systems. Backend is considered as main part as all the required work will be done here. There will be a central server in the backend that administrates client demands, traffic and system monitoring. This central server ensures that everything is running smoothly. There exist some protocols called set of rules for it to run smoothly. A middleware which is software will be used by the central server. Here, this middle ware allows the network computers, to communicate with each other. But there always exits some issues in data privacy in cloud storage devices.

III. CLOUD DEPLOYMENT MODELS

Following are the cloud deployment models.

1. **Public cloud:** This private cloud will be existing beyond the company firewall. This cloud infrastructure will be available to many customers and will be managed by the third party. At the same time, many companies can work on the infrastructure provided, these clouds are completely facilitated furthermore, oversaw by the cloud supplier and completely duties of establishment, the board, provisioning, and support. If there is any under utilization, the charge for that will be eliminated and charged only for the resources being used. Using the web applications, the resources are provided dynamically from the public cloud services. There will not be any authorization or authentication techniques and cannot impose any access restrictions. Some of the examples of this public cloud services are Google App Engine, Microsoft Azure and so on.

2. **Private Cloud:** This private cloud exists in companies on premises or off premises. This private cloud can be owned, rented or leased by the organization. This can

be managed by organization by themselves or by the third party. When compared to public cloud, private cloud is more expensive and is more secured. As there exists some restrictions in public cloud like additional security regulations, legal requirements, limit on bandwidth usage, there are no such restrictions on private cloud services. Since there is restriction on user's access and networks, they will have optimized control towards infrastructure and its improved security. Examples of private cloud services are Eucalyptus systems.

3. **Hybrid Cloud:** Services of both public and private are available in this hybrid cloud services as this is a combination of public and private cloud. Both public and private cloud providers will manage the hybrid cloud. A structure of at least two cloud sending models, connected such that information move takes place between them without influencing one another. Goals and needs of a company can be outlined. Amazon Web services (AWS) is the example of hybrid cloud services.

IV. CLOUD DELIEVERY MODELS

1. **Software as a Service (SaaS):** Different software applications that can be provided by Application service provider (ASP) over the internet is known as SaaS. Providing support and safeguarding, operation continuation, load of software maintenance will be eliminated with the SaaS and there will not be any need of installing other software. To run and manage the full solution of IT infrastructure and processes will be responsibility of SaaS vendor. Example of SaaS is Cisco WebEx, Drop box, sales force.

2. **Platform as a service (PaaS):** PaaS allows its clients to have platform access. Here, the clients can put their own applications or software's. To implement and test the cloud applications, PaaS provides the high level integration. Deployed applications and its Configurations can be controlled by the user but cannot manage the infrastructure. Windows Azure, OpenShift and so on are considered as examples of PaaS.

3. Infrastructure as a service (IaaS): Using the visualization technology, sharing the hardware resources for executing the services is known as IaaS. Resources like servers, storage and so on must be readily accessible by the applications and software. User can control the storage and deployed applications, operating systems but cannot manage the underlying hardware in the cloud. Some of the examples of IaaS are Cisco Metapod, Google Compute Engine (GCE). Data location will also cause issue in security in cloud.

V. CLOUD SECURITY ARCHITECTURE

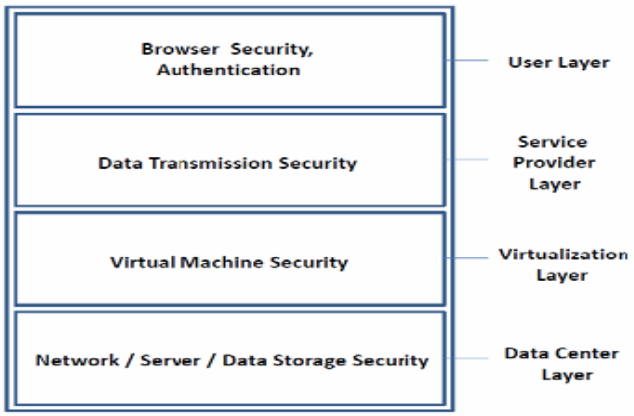

Fig.1. Cloud computing: Security issues and research challenges (Rabi Prasad, 2011)

The above figure depicts the high level system architecture of the cloud. Here we will have four layers called data centre layer, virtualization layer, service provide layer and user layer. User layer is the first layer in the high level security architecture. This is the layer where user can access their data or store the data in the cloud. Other than storage and access, user will have browser security for the data and also authentication of the data being stored in this level. Next level in the high level system architecture is service provider layer where complete data transmission security will be taken care. The third layer is virtualization layer. Here the data will be provided with virtual machine security. The last layer is Data centre layer where all the security issues regarding network, server or data storage will be taken care in this layer.

VI. CLOUD SECURITY AND CHALLENGES

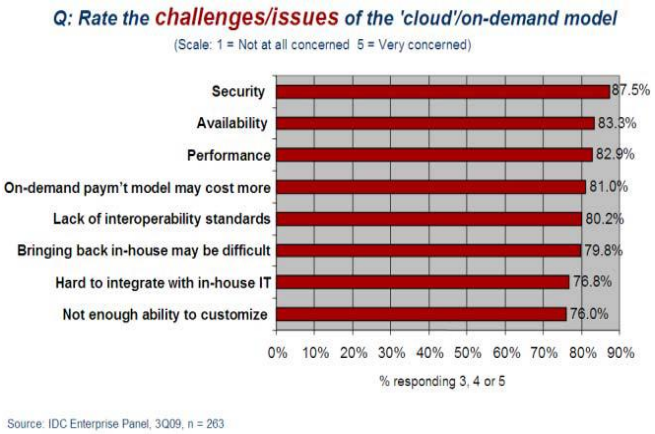

Fig.2. Cloud computing security issues and challenges (kresmir popovic,2010)

In order to build trust in the customers, many challenges and risk on data loss must be taken care. The main issue is that the devices that service is being provided does not belong to the user due to this the user will not have any knowledge on what is going on with his data and he cannot control it. As many users store their private and personal

information the cloud service providers must ensure the users regarding the safety of information. The main security concerns of cloud are: User will not have any idea on who will be doing the encryption and decryption of keys through which the user will not have any control over it. If the user wants to change from one cloud service provider to another some data may be lost as all the cloud providers are not always compatible. The data will be shared between the companies in the cloud model with which the physical security for the data will be lost. There may be many updates in the future for increasing the security for which the user must be updating the application up to date. The integrity sometimes will be changed even with unauthorized transaction which will have chances of data loss or security issues. If the user think about the cost and chooses the public cloud service, then there will be privacy risk for their data. In public cloud there is lot of chances for accessing the sensitive information. If the information is stored long time then there will be more chances of hacking the data by hackers easily. The user will not have control over the data life cycle and cannot be restored if it is deleted or removed or erased mistakenly. There sometimes will be any assurance on backup of data in the cloud.

VII. FUTURE ENHANCEMENT

Cloud computing is an emerging technique, but many issues have been remained to solve them. There are many open issues that need to be solved at earliest. Instead of these older techniques, new techniques need to be developed to work securely with the cloud services. Clients or the user must be made known regarding the issues like access control, data transmission and steps to control these issues. The high level system architecture does not solve the security issues related to access control and needs to give importance on this issue in future.

VIII. CONCLUSION

Cloud service is the most used storage process now-a-days. In cloud computing, the major issue is considered to be data security. The biggest security issue is sharing the resources. We have discussed cloud deployment models, cloud delivery models, high level system architecture and challenges and issues of cloud services is being explained clearly in this paper. Security issues like Data management, access control are highlighted in this paper.

REFERENCES

[1] https://en.wikipedia.org/wiki/cloudstorage

[2] https://www.researchgate.net/

[3] https://www.sciencedirect.org/

[4] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE Int. Conference on High Performance Computing and Communications, Dalian, China, **pp. 825-830, Sep. 2008,** ISBN: 978-0-7695-3352-0.

[5] Ronald L. Krutz, Russell Dean Vines "Cloud Security A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, Inc., **2010.**

[6] Aderemi A Atayero, Oluwaseyi Feyisetan, "Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption", Journal of Emerging Trends in Computing and Information Sciences, **Volume 2, Issue 10, pp 546-552, 1st Oct 2011,** ISSN: 2079-8407.

[7] Kuyoro S. O., Ibikunle F. & Awodele O., "Cloud Computing Security Issues and Challenges", **pp 344-349, 24-28 May 2010,** print ISBN: 978-1-4244-7763-0.

[8] Traian Andrei, "Cloud Computing Challenges and Related Security Issues", **May 2012.**

[9] Suba Surianarayanan, T.Santhanam, "Security Issues and Control Mechanisms in Cloud", International Conference, **pp 74-76, 2012,** ISBN: 97 8-1-4673-4416-6 /12.

[10] Eystein Mathisen, "Security Challenges and Solutions in Cloud Computing", International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011), Daejeon, Korea, **pp 208-212, 31 May -3 June 2011,** ISBN: 978-1-4577-0872-5.

[11] Anas BOUA Y AD, Asmae BLILA T, Nour el houda MEJHED, Mohammed EL GHAZI, "Cloud computing : security challenges", Information Science and Technology(CIST) 2012 Colloquim, Fez, **pp 26 - 31, 22-24 Oct. 2012,** print ISBN: 978-1-4673-2726-8, DOI: 10.1109/CIST.2012.6388058.

[12] Padhy, R.P., Patra, M.R. and Satapathy, S.C., 2011. Cloud computing: security issues and research challenges. International Journal of Computer Science and Information Technology & Security (IJCSITS), 1(2), **pp.136-146, 2011.**

[13] Rachana, S.C. and Guruprasad, H.S., 2014. Emerging Security Issues and challenges in cloud computing. *International Journal of Engineering Science and Innovative Technology*, ***3*(2), pp.485-490, 2014.**

[14] Alvi, F.A., Choudary, B.S., Jaferry, N. and Pathan, E., 2012. A review on cloud computing security issues & challenges. *iaesjournal. com*, *2*.

[15] Popović, K. and Hocenski, Ž., 2010, May. Cloud computing security issues and challenges. In *The 33rd international convention mipro*, **pp. 344-349, 2010.** IEEE.

[16] Kuyoro, S.O., Ibikunle, F. and Awodele, O., 2011. Cloud computing security issues and challenges. *International Journal of Computer Networks (IJCN)*, *3*(5), **pp.247-255, 2011.**

