International Journal of Pure and Applied Mathematics
Volume 116 No. 9 2017, 403-408
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

A SURVEY ON SECURITY ISSUES FACED BY CLOUD DATA OWNERS

[1],K.ShanmugapriyaI. [2] Mary Linda
[1,2]Assistant Professor, Department of CSE, BIST,BIHER, Bharath University, Chennai
[1]shanmugapriya.cse@bharathuniv.ac.in, [2]marylinda.cse@bharathuniv.ac.in

Abstract: Cloud Computing is the newest speedy growing generation in the modern-day generation due to its easy practicable offerings. Now a day's Cloud computing is emerging subject because of its Performance, high availability, at low fee. Data keep is principal future that cloud service offers to the corporations to shop massive amount of garage capability. But nevertheless many agencies aren't ready to put into effect cloud computing generation because of lack of proper security control policy and weak spot in protection which cause many assignment in cloud computing. In this paper we've got represented the survey on one of a kind troubles associated with records garage safety in cloud.

Keywords: Cloud Computing, Cloud Service Models, Deployment Models, Cloud Security,.

1. Introduction

Cloud Computing refers to manipulating, configuring, and accessing the hardware and software resources remotely. It gives on line data storage, infrastructure, and application. Cloud computing is an internet based totally era and provide services over internet. Because of online base computing it provide huge quantity of data storage and resources to the local device and get rid of the neighborhood gadget to renovation separate statistics. As a end result, users are grateful in their cloud service companies for the provision and integrity of their information. The protection of information is crucial within the components of great of provider. Cloud computing whenever invitations the new challenges of safety thread for variety of motives. This paper deeply analyses the Cloud Computing Data Storage security Service Models consisting of IaaS, SaaS, PaaS and Deployment fashions together with Public, Private and Hybrid cloud environments [12]. Fig.1 represents the cloud computing providers for the availability and integrity of their data. The security of data is important in the aspects of quality of service. Cloud computing every time invites the new challenges of security thread for number of reasons. This paper deeply analyses the Cloud Computing Data Storage security Service Models such as IaaS, SaaS, PaaS and Deployment models such as Public, Private and Hybrid cloud environments [12]. Fig.1 represents the cloud computing.

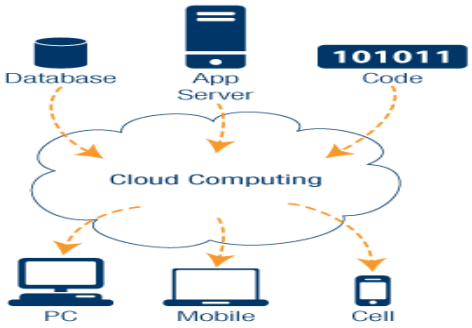

Figure1. Cloud computing

2. Literature survey

2.1 Cloud architecture :

Distributed computing offers many focal points, for example, expanded use of equipment assets, adaptability, decreased expenses, and simple organization. Therefore, all the real organizations including Microsoft, Google and Amazon are utilizing distributed computing. In addition, the quantity of clients moving their information to cloud administrations, for example, iCloud, Google Drive, Dropbox, Facebook and LinkedIn are expanding each day.The Cloud Computing structure joins of many cloud added substances We can generally partition the cloud structure into components[3-6]:

Front End: The front end is the part noticeable by the shopper foundation, i.e., the PC individual, which consolidates the buyer's pc and the projects used to get section to the cloud through a purchaser interface comprising of a web program or any device application [14].

Back End: Refers to the cloud itself. It includes all of the sources required to provide cloud computing services. It incorporates of huge facts garage, infrastructure, safety mechanism, services, deployment fashions, Cloud Runtime, Application and so on.

3. Literature survey:

3.1 Cloud Architecture:

The Cloud Computing architecture comprises of many cloud components We can broadly divide the cloud architecture into two parts:
Front End: The front end is the part seen by the client infrastructure, i.e., the computer user, which includes the client's computer and the applications used to access the cloud via a user interface such as a web browser or any system application [14].
Back End: Refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It comprises of huge data storage, infrastructure, security mechanism, services, deployment models, Cloud Runtime, Application etc.

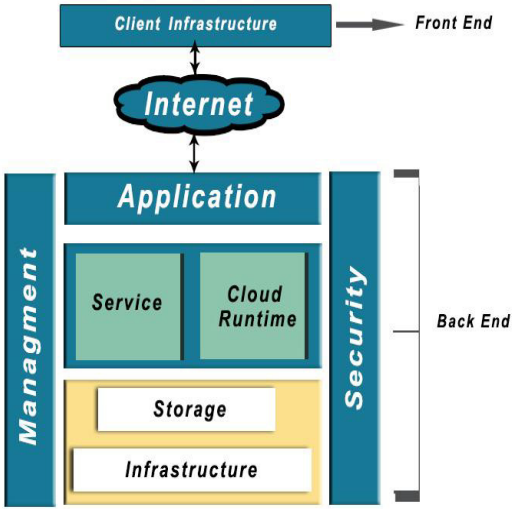

Figure 2. Cloud Architecture

3.2 Service Models:

Cloud computing [4] providers offer their services according to following fundamental models:

3.2.1 Software as a Service (SaaS):

It is a software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet[5].

3.2.2 Platform as a Service (PaaS):

It is a cloud computing model that delivers applications over the Internet. In a PaaS model, a cloud provider delivers hardware and software tools usually those needed for application development to its users as a service[6].

3.2.3 Infrastructure as a Service (IaaS):

Capability for clients to utilize the provider's processing, storage, networks and other fundamental computing resources to deploy and run operating systems, applications and other software on cloud infrastructure[2].

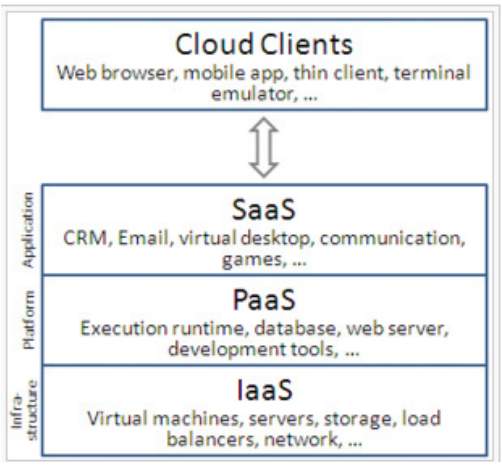

Figure 3. Service models level

3.3 Cloud Deployment Models:

A cloud deployment represents a selected type of cloud condition, in most cases, by large exceptional by means of ownership, length, and get affirmation.

3.3.1 Public Clouds :

A public cloud is an unreservedly accessible cloud condition guaranteed by an outcast cloud provider. The IT resources on open fogs are regularly provisioned through the officially depicted cloud transport models and are all things considered offered to cloud purchasers at a cost or are advanced by methods for various streets, (for instance, promotion).

3.3.2 Community Clouds :

A people group cloud is much similar to an open cloud aside from that its inspire admission to is limited to a specific group of cloud buyers. The system cloud can be commonly claimed by the group members or by methods for an outsider cloud backer that arrangements an open cloud with compelled get right of section to.

3.3.3 Private Clouds:

A non-open cloud is claimed through an unmarried organization. Private mists enable an association to apply distributed computing innovation as a method for bringing together get admission to to IT sources by way of extraordinary elements, places, or departments of the agency.

3.3.4 Hybrid Clouds:

A hybrid cloud is a cloud surroundings made from or greater distinct cloud deployment models.A cloud deployment model represents a specific type of cloud environment, primarily distinguished by ownership, size, and access[7].

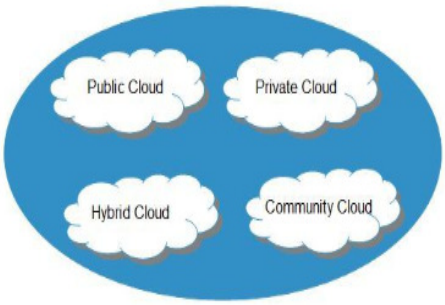

Figure 4. Cloud Deployment Models

4. Problem statement

4.1 Cloud data storage :

In cloud information stockpiling framework, clients store their information in the cloud and never again have the information locally. Consequently, the rightness and accessibility of the information documents being put away on the circulated cloud servers must be ensured [21].

Distributed storage is a model of information stockpiling in which the advanced information is put away in legitimate pools, the physical stockpiling traverses different servers (and regularly areas), and the physical condition is commonly claimed and overseen by a facilitating organization.

4.2 Security threats:

Cloud computing security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use.

Data security from cloud service providers is a concern today and there is no easy to use solution available today that will encourage data owners to take preventive steps such as encryption before moving data to cloud[30-31].

4.3 Threats in cloud computing:

In this segment the significant threats for distributed computing are investigated. These are: i) information threats including information ruptures and information misfortune, ii) organize threats including record or administration breaches, also, foreswearing of administration, and iii) cloud condition particular dangers including unreliable interfaces and APIs, pernicious insiders, manhandle of cloud administrations, lacking due constancy, and shared innovation vulnerabilities.

Denial of Service: Denial of Service (DOS) assaults are done to keep the genuine clients from getting to cloud organize, capacity, information, and different administrations. DOS assaults have been on ascending in distributed computing in recent years and 81 percent clients consider it as a noteworthy danger in cloud. They are generally done by trading off an administration that can be utilized to expend most cloud assets, for example, calculation power, memory, and system data transmission. This causes a postponement in cloud operations, and now and then cloud can't react to different clients and administrations.

Dispersed Denial of Service (DDOS) assault is a type of DOS assaults in which various system sources are utilized by the assailant to send an expansive number of solicitations to the cloud for expending its assets. It can be propelled by misusing the vulnerabilities in web server, databases, and applications bringing about inaccessibility of assets.

Information is thought to be one the most vital profitable asset of any association and the quantity of clients moving their information to cloud is expanding each day. Information life cycle in cloud contains information creation, travel, execution, stockpiling and obliteration. Information might be made in customer or server in cloud, moved in cloud through system and put away in distributed storage. At the point when required information is moved to execution condition where it can be handled. Information can be erased by its proprietor to finish its obliteration[24].

The greatest test in accomplishing distributed computing security is to keep information secure. The significant issues that emerge with the exchange of information to cloud are that the clients don't have the deceivability of their information and neither do they know its area. They have to rely upon the specialist organization to guarantee that the stage is secure, and it

executes important security properties to protect their information. The information security properties that must be kept up in cloud are secrecy, trustworthiness, approval, accessibility and protection. Nonetheless, numerous information issues emerge because of inappropriate treatment of information by the cloud supplier[26].

The real information security dangers incorporate information breaks, information misfortune, unapproved access, and honesty infringement. These issues happen much of the time on cloud information. In this paper, we concentrate on information ruptures and information misfortune that are depicted as the two most serious dangers to distributed computing. Account or Service Hijacking: Account hijacking involves the stealing of user credentials to get an access to his account, data or other computing services. These stolen credentials can be used to access and compromise cloud services. The network attacks including phishing, fraud, Cross Site Scripting (XSS), botnets, and software vulnerabilities such as buffer overflow result in account or service hijacking. This can lead to the compromise of user privacy as the attacker can eavesdrop on all his operations, modify data, and redirect his network traffic. 1n 2009 a legitimate service was purchased from Amazon's EC2, and compromised to act as Zeus botnet

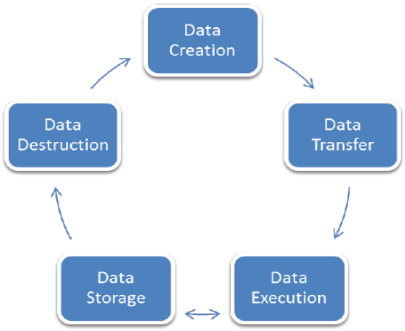

Figure 5

4. Conclusion

In this paper, we investigated the problem of data security in cloud data storage, which is essentially a distributed storage system. This paper is discussed various sections. The main purpose of this work is to survey the recent research done on single cloud as well as on multi cloud to solve the security issues faced by the data owners. By this survey I conclude that much research has been done to address the security issue in data storage in cloud but for multi cloud that much of research is not done and still it has some security issues like data integrity and correctness at the time of data retrieval in cloud. So, multi cloud data storage security needs more attention in area of data storage security in cloud computing.

References

[1] C. Wang, K. Ren, W. Lou, and J. Li, "Towards publicly auditable secure cloud data storage services," IEEE Network Magazine, vol. 24, no. 4, pp. 19–24, 2010.
[2] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE transactions on Services Computing, 06 May 2012.
[3] Singh, S. and Jangwal, T. (2012). Cost breakdown of Public Cloud Computing and Private Cloud Computing and Security Issues. International Journal of Computer Science & Information Technology, 4(2), 17-31.
[4] Rashmi, Sahoo, G. and Mehfuz, S. (2013). Securing Software as a Service Model of CloudComputing: Issues and Solutions. International Journal on Cloud Computing: Services and Architecture, 3(4), 1-11. Doi: 10.5121/ijccsa.2013.3401.
[5] Lee, K. (2012). Security Threats in Cloud Computing Environments. International Journal of Security and Its Application, 6(4), 25-32.
[6] Cong Wang, S.M. Chow, Qian Wang,Kui Ren, and Wenjing Lou "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE transaction,20 December 2011.
[7] Bisong, A. and Rahman, S.S.M. (2011). An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 3(1), 30-45. doi:10.5121/ijnsa.2011.3103.
[8] Westphall, C.B., Westphall, C.M., Koch, F.L., Rolim, C.O., Vieira, K.M., Schulter, A., Chaves, S.A.,Werner, J., Mendes, R.S., Brinhosa, R.B., Geronimo, G.A. and Freitas, R.R. (2011). Management and Security for Grid, Cloud and Cognitive Networks. Revista de Sistemas de Informação da FSMA, 8, 8-21.
[9]. Q. Wang, C.Wang, Wenjing Lou, Jin Li, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," IEEE transaction on parallel and distributed systems, VOL. 22, NO. 5, 2011.
[10] Rakhi Bhardwaj, VikasMaral, "Dynamic Data Storage Auditing Services in Cloud Computing", in the year of April 2013.
[11] Mircea, M. (2012). Addressing Data Security in the Cloud. World Academy of Science, Engineering and Technology, 66, 539-546.
[12] Kuyoro, S.O., Ibikunle, F. and Awodele, O. (2011). Cloud Computing Security Issues and Challenges. International Journal of Computer Networks, 3(5), 247-255

[13] S.Sajithabanu and Dr.E.George Prakash Raj, "Data Storage Security in Cloud" IJCST Vol. 2, Issue 4, Oct. - Dec. 2011
[14] Amazon.com, "Amazon Web Services (AWS)," Online at http://aws.amazon.com, 2008.
[15]KalpanaBatra, Ch. Sunitha, Sushil Kumar," An Effective Data Storage Security Scheme for Cloud Computing", in the year of June 2013.
[16] Udayakumar R., Kaliyamurthie K.P., Khanaa, Thooyamani K.P., Data mining a boon: Predictive system for university topper women in academia, World Applied Sciences Journal, v-29, i-14, pp-86-90, 2014.
[17] Kaliyamurthie K.P., Parameswari D., Udayakumar R., QOS aware privacy preserving location monitoring in wireless sensor network, Indian Journal of Science and Technology, v-6, i-SUPPL5, pp-4648-4652, 2013.
[18] BrinthaRajakumari S., Nalini C., An efficient cost model for data storage with horizontal layout in the cloud, Indian Journal of Science and Technology, v-7, i-, pp-45-46, 2014.
[19] BrinthaRajakumari S., Nalini C., An efficient data mining dataset preparation using aggregation in relational database, Indian Journal of Science and Technology, v-7, i-, pp-44-46, 2014.
[20]Khanna V., Mohanta K., Saravanan T., Recovery of link quality degradation in wireless mesh networks, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4837-4843, 2013.
[21]Khanaa V., Thooyamani K.P., Udayakumar R., A secure and efficient authentication system for distributed wireless sensor network, World Applied Sciences Journal, v-29, i-14, pp-304-308, 2014.
[22]Udayakumar R., Khanaa V., Saravanan T., Saritha G., Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction, Middle - East Journal of Scientific Research, v-16, i-12, pp-1781-1785, 2013.
[23]Khanaa V., Mohanta K., Saravanan. T., Performance analysis of FTTH using GEPON in direct and external modulation, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4848-4852, 2013.
[24]Kaliyamurthie K.P., Udayakumar R., Parameswari D., Mugunthan S.N., Highly secured online voting system over network, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4831-4836, 2013.
[25]Thooyamani K.P., Khanaa V., Udayakumar R., Efficiently measuring denial of service attacks using appropriate metrics, Middle - East Journal of Scientific Research, v-20, i-12, pp-2464-2470, 2014.
[26]R.Kalaiprasath, R.Elankavi, Dr.R.Udayakumar, Cloud Information Accountability (Cia) Framework Ensuring Accountability Of Data In Cloud And Security In End To End Process In Cloud Terminology, International Journal Of Civil Engineering And Technology (Ijciet)Volume 8, Issue 4, Pp. 376–385, April 2017.
[27]R.Elankavi, R.Kalaiprasath, Dr.R.Udayakumar, A fast clustering algorithm for high-dimensional data, International Journal Of Civil Engineering And Technology (Ijciet), Volume 8, Issue 5, Pp. 1220–1227, May 2017.
[28]R. Kalaiprasath, R. Elankavi and Dr. R. Udayakumar. Cloud. Security and Compliance - A Semantic Approach in End to End Security, International Journal Of Mechanical Engineering And Technology (Ijmet), Volume 8, Issue 5, pp-987-994, May 2017.
[29]Thooyamani K.P., Khanaa V., Udayakumar R., Virtual instrumentation based process of agriculture by automation, Middle - East Journal of Scientific Research, v-20, i-12, pp-2604-2612, 2014.
[30]Udayakumar R., Thooyamani K.P., Khanaa, Random projection based data perturbation using geometric transformation, World Applied Sciences Journal, v-29, i-14, pp-19-24, 2014.
[31]UdayakumarR., Thooyamani K.P., Khanaa, Deploying site-to-site VPN connectivity: MPLS Vs IPSec, World Applied Sciences Journal, v-29, i-14, pp-6-
[32] T. Padmapriya and V. Saminadan, "Improving Throughput for Downlink Multi user MIMO-LTE Advanced Networks using SINR approximation and Hierarchical CSI feedback", International Journal of Mobile Design Network and Innovation- Inderscience Publisher, ISSN : 1744-2850 vol. 6, no.1, pp. 14-23, May 2015.