International Journal of Engineering & Technology, 7 (2.21) (2018) 355-357

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Cloud computing security: a survey

P. Sheela Gowr[1*], N. Kumar[2]

[1]Department of Computer Science & Engineering, Vels Institute of Science, Technology & Advanced Studies(VISTAS), Chennai, India.
[2]Department of Computer Science & Engineering, Vels Institute of Science, Technology & Advanced Studies(VISTAS), Chennai, India.
**Corresponding author E-mail:sheela.se@velsuniv.ac.in*

Abstract

Cloud computing was a hasting expertise which has innovated to a collection of new explores. A sub-ordinate device for Information services, it has an ability towards encourage development by feeding convenient environments for a choice of forms of development is different sequence. Clouds usually consider being eco-friendly, however keep it has open to the diversity of some security issues to can change together the feeder as well as users of these cloud services. In this issue are principally associated to the protection of the information flow throughout also being store in the cloud, with simple problems along with data ease of use, data right to use and data confidentiality. Data encryption and service authentication scheme has been initiated by the industries to deal with them. In this paper analyse and examine different issues on security beside with the different procedure worn by the industries to solve these effects.

Keywords: *Cloud computing, cloud service provider, and cloud service consumer.*

1. Introduction

The cloud computing provides the different services (like storage, server, database, network, software, hardware) to the consumers with minimum cost. A cloud make available various services (Figure 1): SaaS, in cloud service the consumer can use applications which are already available in the cloud environment through the internet. User can access these applications from anywhere at any time. PaaS, consumers use the platform services from the cloud provider where he can able to handle its application and utilize it without controlling cloud environment. IaaS, consumer can use infrastructure from the cloud provider where the he can deal with its platform beside through application for the purpose. There are four deployment model available in Cloud computing. Private cloud, single organization or single business can use public cloud for their own use. Private cloud has high protection as compared to the public cloud. Public cloud, the general public as well as organization use the cloud infrastructure owned through the cloud service provider. This model has variety of security risk. While the hybrid cloud communications has grouping of two or more divergent cloud environment (private and public).

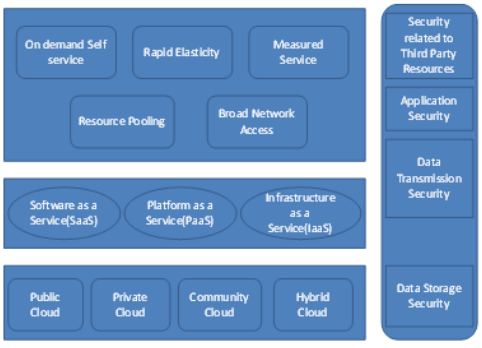

Figure 1: Introduction to cloud computing

This paper speaks and delivers to recognize and explore issues of security and challenge faced by the cloud system, current moderately in prime knowledge, along with concept working in industry to warfare these struggles. To achieve this target, we have to clearly know the concept of following this technology, in addition to its essential road and rail network.
There are now a lot of services presented by vendor which enclose the label "cloud" add to them, via this now trendy term to attract member of the common public who might not essentially make out at all better.
Here the preliminary part, plan towards speak and analyse on the security issues.

Features of security system

The following five characteristics in its operation specified by the NIST

On demand self service

CSC can access as an online interface for computer resource similar to further computers or set of connections bandwidth devoid of human taking part through the cloud service provider.

Broad network access

CSC is able to right to use compute resources in excess of network for instance the Internet beginning a selection of compute strategy.

Resource pool

CSPs are able to make use of collective compute resources to provide cloud services to the various consumers. Virtualization along with multi-tenancy system is classically used to mutually separate out with secure data.

Rapid elasticity

The immediate and routine evaluation of the quantity of accessible computer processing, storeroom in addition to network bandwidth while necessary through client insists.

Pay per use deliberate facility

These involve clients barely paying for the computer resources to facilitate essentially use along with being capable towards examine their procedure. The service purchase beside consumers is able to exist quantified along with calculated.

2. Related work

Khalid et al. [6] the security of cloud by manipulative an anonymous authentication and sanction protocols using unidentified public key certificates solution along with yardstick strong authentication.
The proposed model is divided into two phases one is authentication and second is authorization. The authors have only decisive on web attack on the data.
Govinda et al. [7] anticipated a technique for characteristics anonymity in private cloud group digital signature. On the other hand the mechanism uses RSA algorithm for encryption and decryption.
Salama et al. In [8] have delivered the relative analysis of six symmetric key algorithms blowfish, RC6, AES, DES, 3DES, RC2 for wireless device. The authors have compare all these algorithms to check power consumption of devices Further, the power consumption of all these algorithms has been compared and blowfish have been found to consume lesser percentage of battery.
The paper delivered R, Mishra and et al.[9] the depot everywhere the information sharing services be able to do updating of records in addition to manage the access through restrictive the usage payment to the data. The storerooms help to control data owner used for his effort on data elect completed on server with no disclose data. Not sheltered enough achieve all issues of security.
J.Singh et al. [10] Proposed RC5 encryption algorithm to protected storage information. An organization uses the encryption as well as decryption key of user's records and stores it on top of remote server.
Salvatore J. et al. [11] new the offensive decoy tools call while fog computing. Methods speak about monitor the access privileges by means of detect data access pattern along with when illegal access is originate after that it gets confirmed using dispute questions in addition to launch disinformation attack by means of returning the huge amount of data to the attacker. Protect next to mishandling of information.
Ali et al. [12] proposed the SeDaSC move towards, which is a cloud storage protection method designed for collection of information. The anticipated tactic provide data privacy, protected data contribution devoid of re-encryption, right to use manage for malevolent insiders.

3. Cloud security related concepts

Data security considerations

At compute dealing out of information into consequential information. While the processing as well as storage of such records is out sourced towards environment own and maintain beside a third party, that lead to a swarm of issues. Those issues be particularly more well-defined into the public cloud encompass to distribute this abovementioned infrastructure. These are various properties should be present ensure through data while utilising the cloud:

Isolation

Isolation is most common problem towards deal among in the cloud as well as here network security is common. Isolation ensures to facilitate the personal data along with identity of CSC to illegal user.

Confidentiality

This totally data isolation while this property ensure to facilitate the information belong to a CSCs not exposed to every illegal parties. In this public cloud, the cloud service providers are most responsible intended for securing CSC information. It is mainly hard due to Multitenancy; while various consumers have right to use the similar hardware to facilitate a CSC stores its information. But generally providers utilize virtualization to exploit the use of hardware [Latif 8]. In these two methods permit attacker to encompass complete right to use the host as well as cross- Virtual Machine side canal attack to take out information since an intention Virtual Machine taking place the same machine.

Integrity

The reliability of information refers towards the self-assurance to the information stored inside the cloud that is not changed into various approach through not permitted parties while it's being retrieved. Cloud Service Provider should make sure that the third party has no rights to use information while transferring or storage the information. Only authorised people can access and make changes.

Availability

In this property ensure to the CSC has right to use to their data, as well as is not denied way in inaccurately or due to malicious attacks through some component. Attacks similar to denial-of-service are normally used towards refuse accessibility of information.

4. Information phase

Clouds go throughout different separate stages; with each one phase require one or more of the earlier property to be maintain. They follow:

Information passage

Information is the progression of being transmit also to the cloud environment or to the compute device use through the CSC. Information is dangerous threat of being intercepted, therefore violate privacy. Use the encryption technique to prevent information.

Information respite

Information's are stored in to the cloud environment. The most important problem through in this step for the CSC is to defeat of organize over the information. The obligation of protecting beside attacks on this phase thus falls in the Cloud service provider.

Information exploit

Data is being process into information. Now, the issue may lie down by way of corrupted information even as it is being processed. In direct to prevent the reliability of information departure into the process should be ensuring through any one of the appropriate method. In adding to these three stages, the information missing out in the case of information transmits or information deletion too wants to be measured. Security issues

occurred in the case of public cloud and offerings CSC, information is not properly deleted from a CSC.

5. Security risk in the cloud

The different risks faced while using clouds, in addition to get a short look at the strategy employ towards explain the other secondary issues. In this section, provide a brief summary of different technique used into diligence to protect choose issues in these problem areas.

Managerial protection risks

Malicious Intruders-The risk of having malicious human resources in the Cloud service provider staff be able to mitigate besides put exacting authorized constraint into contracts while hiring people. A complete review of Cloud service provider by the third party, with a robust protection violate announcement process will also begin an extended to prevent this.

Physical protection risks

Physical violation- The threat of intruder acquisition physical rights to use campaign used in the provision of cloud services be able to reduce besides have well-built physical security deterrents within place such as equipped guards, input card access and biometric scans to control access to sensitive location in the information centred.

Technical protection risks

Virtualized protection as well as repute base trust organization [14]. Cloud Service Provider might use the subsequent formation: a ladder of DHT-base transfer networks, by means of exact responsibilities to be performed by each layer. The lowest layer deals among reputation aggregation and penetrating colluders. The highest layer deals through various attacks.
Conviction model for interoperability and protection- There must be separate domain for provider as well as user, every one with a particular trust agent. The trust agent is a self-determining party to collect security data used to validate an end point. There have to besides different trust strategy for cloud service provider and customer.

Compliance and audit risks

In this region mainly deal with authorized issues, such as both CSPs as well as CSCs have to recognize authorized and authoritarian obligation and make sure that at all contract made gather these obligation. The CSP must ensure that its invention capabilities do not compromise security and privacy of information. In (Figure 2) Sketch out of the cloud customer risk classify in front of cloud service customers. In cloud computing facility, the infrastructure is constantly provided through the cloud service provider.

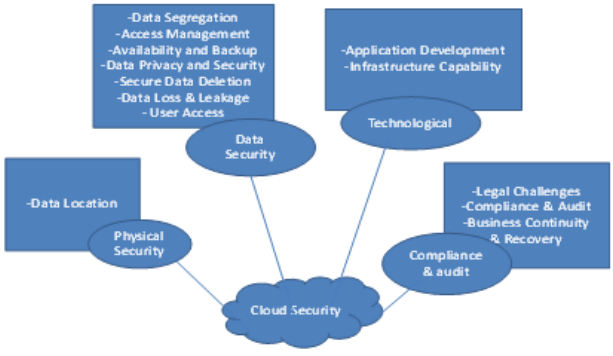

Figure 2: Cloud customer risk categories

6. Conclusion

In this paper, primarily aims to emphasize the main security issues in the cloud computing environment. We proceeded to summarize as well as observe the different security issues that come into analysis even as an outcome of the structures worn in the growth of a variety of cloud computing solutions. We realize the bulk of issue arise in the public cloud. Above paper highlights the major security and privacy oriented issues in existing current cloud system and tends to guide the user to recognize the tangible and intangible threats associated with their uses. Paper deals with 2 main aspects of security and privacy, main aim of this paper is aspect of security and privacy.

- Surveying the most relevant privacy and security issues
- Analyzing the method that may be addressed to omit these potential security and privacy threats, and provide a high secure, trustworthy, and dependable cloud computing environment.

References

[1] Khalid U, Ghafoor A, Irum M & Shibi M, "Cloud based secure and privacy enhanced authentication and authorization protocol", *International Conference in Knowledge Based and Intelligent Information and Engineering System*, (2013), pp.608-688.
[2] Govida K & Sathiyamoorthy E, "Identity anonymization and secure data storage using group signature in private cloud", *Procedia Technology*, (2012), pp.495-499.
[3] Salama D, Kadar H & Hadhoud M, "Studying the effects of most common encryption algorithms", *International Arab Journal of e-Technology*, Vol.2, No.1, (2013), pp.1-10.
[4] Mishra R, Dash S & Mishra D, "Privacy Preserving Repository for securing data across the Cloud", *3rd International Conference on Electronics Computer Technology*, Vol.5, (2011), pp.6-10.
[5] Singh J, Kumar B & Khatri A, "Securing the Storage Data using RC5 Algorithm", *International Journal of Advanced Computer Research*, (2012).
[6] Stolfo SJ, Salem MB & Keromytis AD, "Fog Computing: Mitigating Insider Data Theft Attacks in Cloud", *IEEE CS Security and Privacy Workshop*, (2012).
[7] Ali M, Dhamotharan R, Khan E, Khan SU, Vasilakos AV, Li K & Zomaya AY, "SeDaSC: secure data sharing in clouds", *IEEE Systems Journal*, Vol.11(2), (2017), pp.395-404.
[8] Latif R, Abbas H, Assar S & Ali Q, "Cloud computing risk assessment: a systematic literature review", *Future Information Technology*, (2014), pp.285-295.
[9] Australian Government Cyber Security Operations Center, Cloud Computing Security Considerations, (2012).
[10] Jansen W & Grance T, "Guidelines on security and privacy in public cloud computing", *NIST Special Publication*, (2011).
[11] Jain R, "Network Access Control and Cloud Security", CSE 571s, Washington University in Saint Louis.
[12] Network Admission Control, Wikipedia: The Free Encyclopedia, Wikimedia Foundation.
[13] Ziao Z & Xiao Y, "Security and privacy in cloud computing", *IEEE Communications Surveys & Tutorials*, Vol.15, No.2, (2013), pp.843-859.
[14] Bhadauria R & Sanyal S, "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques", *Intl. Journal of Computer Applications*, Vol.47, No.18, (2014), pp.47-66.