Cloud Security Issues and Challenges

Prikshat Kumar Angra, Dr.Kavita, Dr.SahiVerma, AnupLalYadav
Research Scholar, Lovely Professional University, Email: prikshat.22305@lpu.co.inAssociate Professor, Lovely Professional University, Email: kavita.21914@lpu.co.in
Associate Professor, Lovely Professional University, Email: sahil.21915@lpu.co.in
Assistant Professor, SRMIET,AMBALA, Email: anupsaran@gmail.com
*Corresponding author kavita.21914@lpu.co.in**

Abstract

Itprovides a direct blaze to the shared pool of comfortable attached resources.These resources are used to access information with the help of service providers. Resources are provided in the form of IT-based capabilities.In this paper cloud computing security obstructions are

discussed related to cloud and its services.Cloud security can be improved with the help of many technologies that may use to secure data some times and also secure sometimes working of service providers.We have presented a review from different papers according to which many security issues are discussed.We explain trusted data sharing in which our data is easily accessible from different devices with the help of cloud services.For secure data access Service level Agreement(SLA) protocol helps for transparent communication between the end user and cloud.

Keywords:*Security, Cloud Computing,Service level agreement.*

Introduction

Cloud computer is a technology which can be executed by different design, and resources of other technology with distinct configurational approaches. Some cloud resources models are Infrastructure As a Services (IaaS), Platform As a Services (PaaS), and Software As a Services (SaaS). There is a free and open source software which is used to develop the cloud platform called Heroku. That supports many languages like JAVA, Node.js, Scala, Python and PHP, it can also be integrated with data services.

Cloud computing generally described either build on the host mode, or on services that cloud present if has. While discussing about deployment model, we can classify cloud as: Public, Private, Hybrid, Community Cloud and based on a services the cloud model is charity: IaaS, PaaS, SaaS, or storage, Database, Information, Process etc.

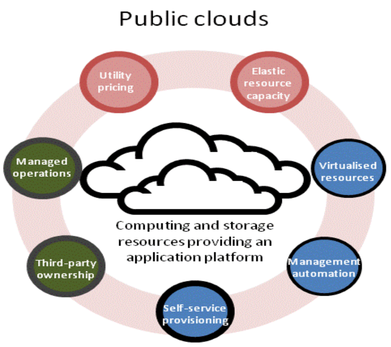
Public clouds
Utility pricing
Elastic resource capacity
Managed operations
Virtualised resources
Computing and storage resources providing an application platform
Third-party ownership
Management automation
Self-service provisioning

Figure 1:Public cloud [23]

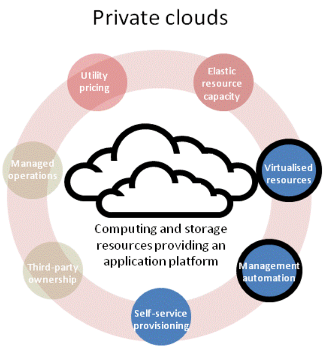
Private clouds
Utility pricing
Elastic resource capacity
Managed operations
Virtualised resources
Computing and storage resources providing an application platform
Third-party ownership
Management automation
Self-service provisioning

Figure 2:Private Cloud[23]

Cloud computing data security is the major challenge now a day to minimize the risks. These threats are directly like open cloud, distribute upload, and environment. Cloud computer is everywhere now because of some advantages like flexibility, accessibility and capacity as compare to other storage methods. The main seek of this study is to secure the client data over the cloud and ensuring the client that the data which has been uploaded by you is safe a secure.

Security is the main part of the cloud computing and it can be divided in to two main parts, Firstly, Security issued by the cloud provider and secondly Security excude faced by their customers. Customer has trust on cloud provider that's why they put data over this storage with trust; this is main reason the need of security. There are several algorithms has already been used like AES (Advance Encryption Standard) and this algorithm is symmetric block cipher. In cloud computing, the users are unaware the location of their confidential data, because the cloud service providers only manage the data centres at distributed location. The importance of this study is to address the basic requirement of the client like Authentication, integrity, transparency, confidentiality, availability etc.

Related Work

A Venkatesh et al[1] in their paper has demonstrate that make sure that data is stored on cloud storage by secure process but data securiy is major threat in cloud storage.To eliminate this, privately,uprightness,availability should be compressed in a Cloud Service Provider (CSP)'s Service- Level Agreement (SLA) to its customers.Dr. N.K.Joshi et al[2] in their paper has demonstrate that One of the main problem is the data security and privacy of information stored and processed at the cloud service grant systems.User's all data may be store on different locations for either problemliberalilsm or because the service is provided through different service providers.Prabal Verma et al[3] in their paper has demonstrate that Security in cloud computing is still in conception and required more inspect,cloud computing has been utilized and used in showing environments.This paper grant an overview of cloud computing, its power and categories.Victor Chang et al[4] in their paper has explain that review, thinking and essentials in the

(Cloud Computing Adoption Framework) CCAF to protect informationsecurity.CCAF multi-layered security could provide the additional protection for all 10 PB of data in 125 hours when the Data Center was under the security cause and slash. Data security in the Cloud is an important issue for Cloud adoption.Zhangjie Fu et al[5] in their paper has explain the standard theory of encryption makes the properuse of the data difficult.So it is tough to find the given set of keyin encrypted data set.Solution of this is use different cloud servers for encrypted retrieval and make hand outall on findrightness and regularity. For exceed correctness,develop the idea hierarchy to deliver the search perameters.Jong-Hoon Lee et al[6],in their paper has demonstrate that when the normal security systems arevirtualized in cloud party line, we build the SIEM design for cloud-based security utility Security Information and Event Management (SIEM) engine performs the data analysis super each user, it must see the retrieved data for each user.It also find out the gained data for each user.DIAO Zhe et al [8],in their paper has demonstrate that cloud storage fusion made very rapid, and cloud storage security technology is facing unprecedented issues.To achieve the security of cloud storage completely, academia,industry and government departments need to work together.

Deployement and Service Models

The cloud deployment model derivates in four types:-

(a)Private cloud model:-The infrastructure operated by only one organization and according to their private use.These are made by the organization for working of their own critical applications with no interferance of other organization.This service is only accessed by owners of the cloud.

(b)Public cloud model:-This kind of cloud storage is used by the general purpose users for uploading and downloading the data.Service supplier has all over ownership of cloud storage with their own attitude and model.Various cloud service provider areMicrosoft, Amazon EC2 and Google App Engine etc.

(c)Community cloud:-A cloud is togetherbuild by organization and equal cloud infrastructure is shared by them.

(d)Hybrid cloud model:-This kind of cloud infrastructure is combination of 2 or additional clouds it may be public,private or community.It is used for optimizing the resources of an organization.

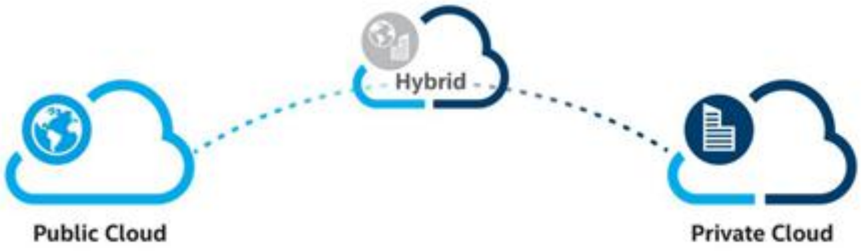

Figure 3:Deployment Model[22]

Cloud service model is differentiate to 3 main parts-SaaS(Software as a Service),PaaS(Platform as a Service) and IaaS(Infrastructure as a Service).

1)SaaS

Software as a service provides different types of softwares that are used to develop and host different web applications developed in high level programming and frameworks.All our hardware devices like mobiles,data servers and data base etc.

2)PaaS

Platform as a service gives different platforms used to develop application.Platforms are operating systems we use to develop application.

3)IaaS

All fundamental computing resourses like storage,server network etc.are used to provide services to the end user’s with proper relation with software and platform they need.Amazon EC2 is an example of IaaS.

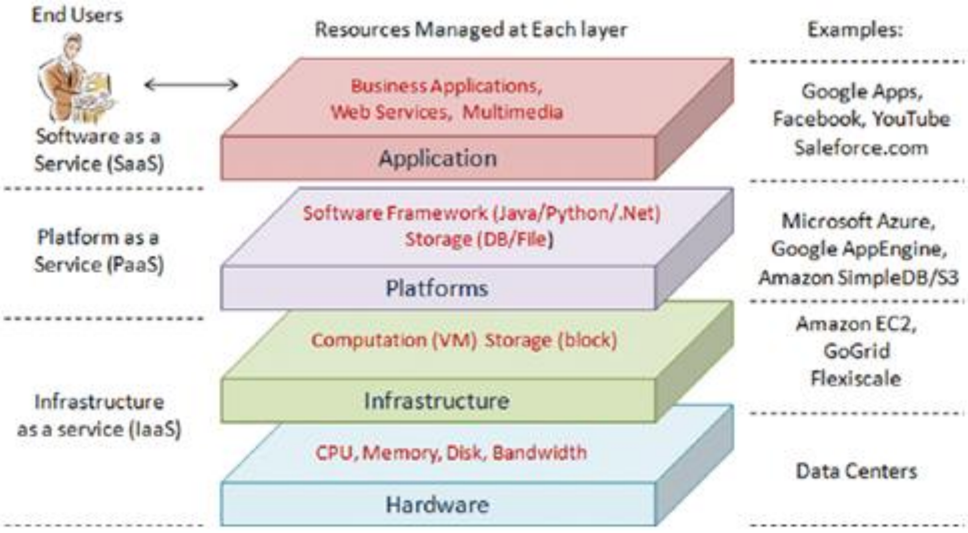
End Users
Resources Managed at Each layer
Examples:
Software as a Service (SaaS)
Business Applications, Web Services, Multimedia
Application
Google Apps, Facebook, YouTube Saleforce.com
Platform as a Service (PaaS)
Software Framework (Java/Python/.Net) Storage (DB/File)
Platforms
Microsoft Azure, Google AppEngine, Amazon SimpleDB/S3
Computation (VM) Storage (block)
Infrastructure
Amazon EC2, GoGrid Flexiscale
Infrastructure as a service (IaaS)
CPU, Memory, Disk, Bandwidth
Hardware
Data Centers

Figure 4:Service Model Architecture[21]

Major Security Issues In Cloud Computing

There are manyissues and challenges that should be taken in to premier for gain full benefit from this new design.Some of major concern are
1)It is difficult to maintain the cohesion to ensure the auditability of dynamic data molten nature of cloud computing service model.
2) There should be a common standard that all the service provider used for store end user valueable information.
3)Userknow they are safe and updated with required application.
4)Violation of law of data attach by government.

Conclusion

Uses of cloud computing reduce operating cost for companies and increasing efficiency of working.We have presented issues connected to security in cloud computing.After that the problems related to security in cloud computing model how can be exceed is discussed.The ongoing working on Service level agreement (SLA) is outlined in this paper. Also we have shown a solution to provide security for user’s information reside on private clouds since safe information stored on cloud nature is a consequentialfact that prevents number of peoples from using the cloud.The need for future work on account ability mechanism in public and private clouds,to provide clear service that can be trusted by every user is also highlighted in this paper that’s why we working for secure access of data from the cloud service providers.

Reference

1. A Venkatesh *1, Marrynal S Eastaff 2,”A Study of Data Storage Security Issues in Cloud Computing,”International Journal of Scientific Research in Computer Science, Engineering and Information Technology,January-February-2018
2. ShivamSharma,Dr. N.K.Joshi,”CLOUD COMPUTING SECURITY CHALLENGES AND
SOLUTIONS,”February 2018
3. PrabalVerma 1 , Aditya Gupta 2 , Rakesh Singh Sambyal 3,”Security Issues and Challenges in Cloud Computing: A Review,”CSEIT411832 | Published - 25 April 2018 | March-April-2018
4. Victor Chang, MuthuRamachandran,”Towards achieving Data Security with theCloud Computing Adoption Framework,”1939-1374 (c) 2015 IEEE
5. ZhangjieFu,Lili Xia Xingming Sun Alex X. Liu,GuowuXie,”Semantic-aware Searching overEncrypted Data for Cloud Computing,”1556-6013 (c) 2018 IEEE
6. Jong-HoonLee,YoungSooKim,Jong Hyun Kim,Ik Kyun Kim,”Toward the SIEM Architecturefor Cloud-based Security Services,”2017 IEEE

7. Bih-Hwang Lee,ErvinKusumaDewi, Muhammad Farid Wajdi,"Data Security in Cloud Computing Using AES Under HEROKU Cloud,"2018 IEEEE
8. DIAO Zhe, WANG Qinghong, SU Naizheng, ZHANG Yuhan"Study on Data Security Policy Based On Cloud Storage,"2017 IEEE
9. David S. Linthicum,"Emerging Hybrid Cloud Patterns,"2016 IEEE
10. Mohamed Al Morsy, John Grundy and Ingo Müller,"An Analysis of the Cloud Computing Security Problem,"
11. Syed NoorulhassanShirazi, Antonios Gouglidis, Arsham Farshad, and David Hutchison,"The Extended Cloud: Review and Analysis of Mobile Edge Computing and Fog From a Security and Resilience Perspective,"NOVEMBER 2017 IEEE
12. Gentry Craig. A fully homomorphic encryption scheme. Ph.D. thesis, Stanford University; 2009.<http://crypto.stanford.edu/craig/craig-thesis.pdf>[retrieved 21.04.11]
13. Microsoft. Microsoft Windows Azure.<http://www.microsoft.com/windowsazure/>
14. RongChunming, Nguyen Son T. Cloud trends and security challenges. In: Proceedings of the 3rd international workshop on security and computer networks (IWSCN 2011); 2011
15. X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," IEEE Trans. Parallel Distrib.Syst., vol. 25, no. 9, pp. 2386–2396, Sep. 2014.
16. T. Jiang, X. Chen, and J. Ma, "Public integrity auditing for shared dynamic cloud data with group user revocation," IEEE Trans. Comput.,vol. 65, no. 8, pp. 2363–2373, Aug. 2016.
17. J. Shen, S. Moh, and I. Chung, "Identity-based key agreement protocol employing a symmetric balanced incomplete block design," J. Commun.Netw., vol. 14, no. 6, pp. 682–691, Dec. 2012.
18. Office of Management and Budget. 2016. Strengthening Federal Cybersecurity. Meeting Our Greatest Challenges: The President's Fiscal Year 2017 Budget. Fact Sheet. Last accessed May 31, 2016.https://obamawhitehouse.archives.gov/omb/budget/key-issue-fact-sheets
19. ShaluMall, Sushil Kumar Saroj,"A New Security Framework for Cloud Data,"Procedia Computer Science 143 (2018) 765–775
20. RongChunming, Nguyen Son T. Cloud trends and security challenges. In: Proceedings of the 3rd international workshop on security and computer networks (IWSCN 2011); 2011.
21. JafarMuzeyinWorku,"DEFINING AN EFFECTIVE SECURITY POLICY FOR COMPANIES USING CLOUD COMPUTING,"23 July 2017
22. Intel. Intel Dam Cloud.<https://www.intel.com/content/dam/>
23. Global Dots<https://www.globaldots.com/cloud-computing-types-of-cloud/>