

Fundamental and Comparative Study of Secure Cloud Computing

Mahmood

Dept. Computer Science and Engineering
Gargi College,
Bhopal, INDIA

GUIDE

Dept. Computer Science and Engineering
Gargi College,
Bhopal, INDIA

Abstract— To reduce the cost of computing, Cloud computing has now one of the booming researching area. Currently, the services that the Cloud computing is providing to its users are on demand over the internet, hence it is very persuading technology. As it stores data and the resources are distributed in the environment, so the security of the resources and data has become the major issue that is restricting the deployment of cloud computing environments. Various users are now using the cloud to store their data, such that the security of data storage is needed on these medium of storage. Basic objective of the cloud computing environment is providing security while storing the data on server of cloud. This paper is to review various techniques of security and issues from the aspect of both software and hardware for securing data in cloud and targeted at improving the security of data and privacy preservation for the reliable environment of cloud. In this paper, it provides a approximate analysis research of the previous researches related with the security of data and techniques of privacy preservation that are used in cloud computing.

Index Terms—Cloud, Security, Services, Issues, Architecture.

I. INTRODUCTION

The description of the concept “Cloud Computing” is the services of computing in IT such as platforms, infrastructure, or software can be organized and used via internet. [1] Framework is a large scaled distributed infrastructure on which cloud is based, consists of shared group of resources normally are virtualized, and the services provided are distributed to the clients in aspect of deployment environment, virtual machines, or application. Therefore it may be concluded easily that associated with the current workloads and requirements, the cloud services can be dynamically measured. Since various resources are used, as they are scaled and then made the payment based on the utilization of the resources.

Cloud computing allows the user to online access the resources via internet, at any time and from anywhere

without considering about the physical and technical management or issues of maintenance for the basic resources. In addition with this, the resources of the cloud computing are scalable and dynamic. Cloud computing is an autonomous type of computing and it is fully different from utility and grid computing. One of the best example of Cloud computing is Google Apps it allows to access the services through the browser and may be deployed on the various machines on the Internet. All the resources are accessible in the cloud from any place and at any time across the world by the use of the internet. Cloud computing is less expensive as compare to other models of computing.

Cloud Computing allow universal, on - demand network access, convenient to a distributed group of computing resources that are configurable for example, servers, networks ,storage, services and applications which can be very quickly provided and released with few effort of management or interaction of service provider.

Cloud computing may be taken as a recent prototype of computing which may provide on demand services at a less cost. The main three commonly used and well-known service models in cloud pattern are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). In the SaaS, software associated with the data gets deployed by the cloud service provider, and the users may use it via web browsers.

In the platform as a service, a service provider provides services to users along with the set of programs of software which can solve the particular tasks.

In infrastructure as a service, the provider of cloud service provides services to users with the virtual machines and storage to enhance their capabilities of business. This paper facilitates the information about the cloud

computing power to IT industry by referring the global issues. This paper describes the problems which can occur and suffer in the implementation of the cloud computing.

- To gather statistics and information of surveys conducted by various famous and standard organizations; such as International Data Corporation (IDC).
- A precise review on the trust, security & privacy issues of the cloud computing.
- Refer the issues of security and disputes suffered by the CSP to apply cloud service, few moderation steps and the negligence of the security model which can solve few issues of security in cloud the environment.

II. Cloud Architecture

The Cloud Computing architecture consists of various components of cloud communicating with each other regarding several data that they are carried on too, hence providing help to the user to reach to the needed data on a quicker rate. As when it reached to the cloud it is targeted on the frontend and back end.

The front end is the user who needs the data, while the various data storage device are the backend, or the server that build the cloud [4].

Architecture of cloud computing is split into the bottom layer which consists of virtualized resources and the upper layer includes particular services to the users [2]. The architecture is present in Fig. 1.

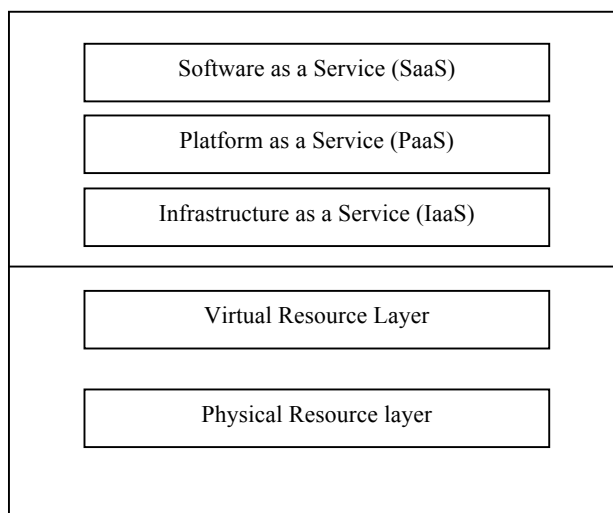


Fig. 1 Architecture of Cloud computing

Cloud computing architecture consists of the two main components i.e. hardware and the application. These components must have to perform work in a combined form aimlessly or the cloud computing will never be possible. It needs a complicated communication with hardware that is needed to assure application's uptime. If the application failed, then the hardware will never be capable to send the data and execute some processes.

On the contrary, the failure of hardware will result in stoppage of the functions. Architectures of Cloud are required, sometimes momentary or repetitive, through facilitating the maximum consumption and reliable bang for the buck. In place of designing software on the constant and severe framework, the architectures of cloud allow a fresh way to design software in the on demand infrastructures.

Normally, cloud computing is a wide-range shared network system applied dependents on the various servers in the data centers. The services of cloud are normally categorized dependent on the layer concept. The upper layers consists of this pattern, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are arranged in stack.

- **Data centers layer:** This layer enables the hardware facilities and framework for the clouds. In this layer, various servers are connected with the high-speed networks to allow the services for the users. Normally, data centers are made in less known places, with heavy supply of power steadiness and less risk of the disaster.

- **Infrastructure as a Service (IaaS):** It is made up on the top of data center layer. IaaS allows the facility of storage, servers, and hardware and components of networking. The users may normally charge on the per-use basis. Hence, clients may secure cost in the form of payment is the only dependent on how much the resource they use really.

- **Platform as a Service (PaaS):** It provides an advanced combined environment for testing, building and deploying changeable software. If anyone is using PaaS will observe a service that encapsulated to show them via an API. The customer communicate with platform via an API, and the platform perform what is essential to scale and manage it to enable a preferred level of service

- **Software as a Service (SaaS):** It supports the distribution of software with particular needs. The users in this layer, may access an application and the information of a remote

area through the Internet and charge only for those that they use.

III. Cloud Services

Around the whole computing spectrum the services of cloud computing are provided. Currently, companies and organizations are extending their business by the use of the cloud computing to reduce their cost. This can facilitate to free maximum man-powers to work on building strategic discrimination and division of labor is clearer.

Cloud service providers allow their services based on the three traditional models [3].

3.1 Software as a Service (SaaS):

It is also called as a Service or an Application Clouds. This model hosts the application or software as a service to their several users of the cloud through the internet. The applications or software are accessed by several client terminals via web browser, or an interface of program. The user does not control or manage the fundamental infrastructure of cloud consists of servers, network, storage, operating systems or capabilities of a particular application, with the available exception of configuration settings of few particular user application. It facilitates with the less expensive and relevant applications to organization.

3.2 Platform as a Service (PaaS):

It provides resources of computation through a platform on which the services and the applications can be modernized and hosted. The user never monitors or manages the cloud architecture involving the network, operating systems, or server, but they have the control over the implemented applications and also on the settings of configuration for the hosting environment of application.

3.3 Infrastructure as a Service (IaaS):

It is also called as the Resource Clouds normally facilitate the resources that are arranged and can be scaled up easily, as services to the various users. There is no need for the user to control the internal framework of cloud but they have the access on the storage, operating systems and applications; and also have the restricted control on the selected components of networking (for example - host firewalls).

IV. Cloud Security Issues

The privacy of the combined data in cloud is complicated, as it allows various services such as Network as a service (NaaS), Software as a service (SaaS), Infrastructure as a service (IaaS) and Platform as a service (PaaS). Every service has separate issues for security [5]. Some issues of security are mentioned below:

4.1 Privileged user access: Other than the resource, the data which is processed consists of a basic risk, such as services deployment, preventing the mortal, constant and human resource controls IT shops tasks on the programs.

4.2 Data Locations: The users are not aware about the location and the place where the data is stored which they are using. Service providers are required to be questioned if they will finish the storing and modification of data in specific mediation, and based on their users they will make a reliably completed to follow the local requirement of privacy[6].

4.3 Data Recovery: By accidentally lost data, or corrupted data can be restored in this process.

4.4 Trust Issue: Trust is another vast problem in the cloud computing. Trust should be established in between machine to human, human to machine, machine to human, human to human.

4.5 Data Security: This is referred as an integrity, confidentiality and availability which are the basic issues for the vendors of cloud. The term confidentiality is explained as the data privacy. It is designed to protect the private information from the illegal or unauthorized user.

V. Literature Review

The literature explained three major broad models of service for the cloud computing:

- *Software as a Service (SaaS)*, in which software are hosted and delivered online through a web browser providing fundamental functionality of desktop like Google Docs, and Gmail.

- *Platform as a Service (PaaS)*, in which the cloud offers the software platform for the systems such as adverse to just a software, the best example is the Google App Engine.

- *Infrastructure as a Service (IaaS)*, in which a group of resources of virtualized computing, like server, storage and capacity of computing, are hosted in cloud, the user deploy and execute their own application stacks to attain the services.

This literature also discriminates the cloud computing branches by the scope. In the private clouds the services are offered extensively to the trusted users through a single-tenant operating environment. Consequently, a data centre of an organization delivers the services of cloud computing to the clients which may or may not be in the area [7]. Public clouds are of opposite types, the services are provided to users and the organizations that want to maintain accountability and elasticity without consuming the complete costs of the in-house framework [7]. The users of public cloud are by default considered as the unreliable. There is another type of cloud also found called as hybrid clouds, combining both the public and private cloud service offerings [8].

In the paper [9] it is suggested that how to secure the outsourced private data as a service is one of the major challenges for security of data in the cloud computing. To refer these challenges of data security, it is suggested an effective data encryption to encrypt the private data before forwarding in the cloud server. This describes the data encryption of block level by the use of 256 bit symmetric key with the rotation. Additionally, the users of data can construct again the data requested from the cloud server by the use of shared secret key. It is analyzed the privacy preservation of the outsourced data by the use of experiment is taken out on the storage of the text files with the different size. The performance and security analysis presents that the suggested method is very efficient as compared to the performance of previous methods.

In paper [10] it has been suggested a business model for the cloud computing for the security of data by the use of data encryption algorithms and decryption algorithms. In this method the service provider of cloud is responsible for the data storage and the encryption and decryption functions that take more overhead of computation for process of the data in cloud server. The major drawback of this method is, no control is there of data for the data owner that is, the owner of data has fully trusted with the cloud service provider and has more overhead of computation.

VI. Conclusion

The biggest security issue in the cloud computing structure is the storage of the private data/information. Cloud service providers required to aware their users on the level of security which they are offering on their cloud. In this paper several models of the cloud computing have been described, also the issues of security and research problems

in the cloud computing. Security of data is a major issue for the Cloud Computing. In this paper, all the issues of cloud computing have been highlighted. Some new security methods required to be introduced and existing security methods required to be tweaked radically to be capable to operate with the architecture of clouds. The cloud computing technology development is still at an initial stage. So, the new improved infrastructure required to be developed for the purposes of security. Here, it has also been discussed the problems associated to the storage, integrity, data location, availability and security. Building the trust is a way to recover these issues of security as it builds the relationship between the entities safely and quickly. These problems explained above will be the hotspot of research of the cloud computing. As there is no doubt that the cloud computing has the excellent future.

REFERENCES

- [1] Kant, Dr Chander, and Yogesh Sharma. "Enhanced Security Architecture for Cloud Data Security." *International Journal of Advanced Research in Computer Science and Software Engineering* 3.5 (2013): 571 -575.
- [2] Dean and S. Ghemawat; (2010), "MapRduce: Simplified data processing large clusters", *communication of the ACM*, Vol.51, pages 107-113.
- [3] Voorsluys, William; Broberg, James; Buyya, Rajkumar (February 2011) "Introduction to Cloud Computing". *Cloud Computing : Principles and Paradigms*. New York, USA: Wiley Press.pp.1-44.ISBN978-0-470-88799-8
- [4] [Jianfeng Yang](#); [Zhibin Chen](#), "[Cloud Computing Research and Security Issues](#)", *Computational Intelligence and Software Engineering (CiSE), 2010 International Conference*, 2010, ISBN: 978-1-4244-5391-7, IEEE.
- [5] B.R kandukuri, R.Paturi V, and A.Rakshit, "cloud security issues", 2009 IEEE International Conference on Services Computing, sep. 21 -25, 2009, Bangalore, India, pp. 517-520.
- [6] Feng-Tse Lin, Teng-San Shih, "Cloud Computing: The Emerging Computing Technology," *ICIC Express Letters Part B: Applications (ISSN: 2185-2766)*, v1, September 2010, pp. 33-38.
- [7] Adamov, A ; Erguvan, M.; (2009),"The Truth about Cloud Computing as new Paradigm in IT",IEEE International Conference on Application of Information and communication Technologies, AICT 2009.
- [8] Dikaiakos, M.D; Katsaros, D.; Mehra, P.; Pallis, G.; Vakali, A.; (2010), "Cloud Computing Distributed Internet Computing for IT and Scientific Research".Vol.13 ,pp 10, Sept.-Oct. 2009.
- [9] Peter Mell, Timothy Grance, *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology Special Publication 800-145 7 pages (September 2011)
- [10] Hanumantha Rao.Galli etc(2013 October)."Data security in cloud using hybrid encryption and decryption" *International*

IJO-SCIENC

(INTERNATIONAL JOURNAL ONLINE OF SCIENCE)

ISSN: 2455-0108

VOLUME II ISSUE IV 2016

journal of advanced research in computer science and software
engineering vol3.