IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 3, March 2016.
www.ijiset.com
ISSN 2348 – 7968

Cloud Computing Security and Outsourcing

Deeksha chaudhary
School Of Information and Communication Technology
Gautam Buddha University
Greater Noida
Deeksha300692@gmail.com

Vimlesh kumar
School Of Information and Communication Technology
Gautam Buddha University
Greater Noida

ABSTRACT

Cloud computing is a cyclic form of pattern made for computing the data or the information. If we talk about some cloud servers the data is outsourced due to which some of the concerns are included like security and privacy.

In this paper we are discussing about the need and the demands of cloud computing. It is now a necessary and important part for everyone. it is now an easily access device which is used flexibly and it is having an increasing demands day after day which reduces the costing and usage of counting or countable resources.

Basically it is a service provider which gets advanced from the virtualization technology and it is the combined with the self-service gives the function of computing with the help of internet services.

It is the process which works in the cyclic form i.e. it allows the data and the information to be accessed through a network.

INTRODUCTION

The revolutionary theory of sharing of data to someone or some party through the internet such a process is called cloud computing. In other words it is a phenomenon in which the data shared to someone which are present their in the cloud.

Figure-1

In the modern era the Computer and Information Technology has become an indispensible part. Now-a-days cloud computing has made a very good place in the IT industries and becomes the most promising business concept and it is the fastest growing segment. Now many of the companies are adopting the cloud computing program for their fast growth and access to business application or boost their infrastructure resources all at the negligible cost or small cost.

If we go through the history, in 1970's time sharing was invented then in 1990's the telecommunication is being established which gives the quality of services and at lower cost. This is some way the history of communication services.

Cloud computing is the software program which is very must profitable due to which it become the part of attraction among the industries and the academia. But as far as we are concern that the part of data confidentiality is very must important as if the data confidentiality is not there it is difficult for the user to access it. Privacy is the major aspect it is not just the privacy of the contents it is something beyond it which is much important aspect. In this the privacy issue risk are there because there are some chances of illegal inspect and can access the sensitive information of the user.

Secondly it is the program in which the personal information are at risk because the ones personal identity can be authenticated for the access control from the given information. In this the identity needs to be protected. So we can say that in the privacy issue cloud computing should be resilient so that we can comprise the data from the attackers.

Some of the encryptions and techniques have been proposed to protect the contents privacy and access controlling, for example Identity based encryption, and Attribute based encryption and so on.

CLOUD ARCHITECTURE

The services offered in the cloud computing is a consumer/ delivery model, which can be accessed with an internet services and can be handled anywhere and anytime.

ISSN 2348 – 7968

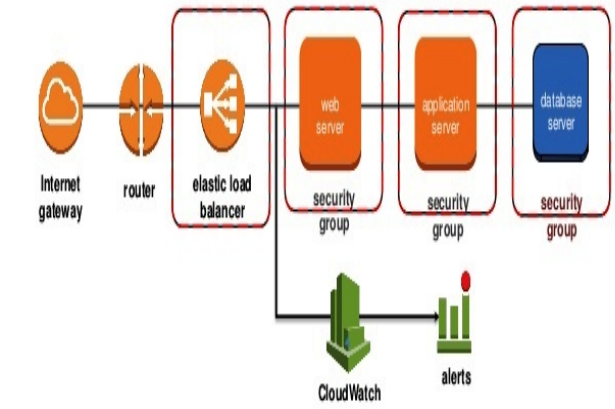

Figure 2

CHARACTERSTICS

The cloud architecture has following characteristics:-

- Maintenance of application is very easy as it can be accessed from any place and need not to be installed for each user's Computer.
- Multitenancy is there due to which we can share the cost and resources across a large cloud of users. It centralized the infrastructure at low cost. It also helps in increasing the efficiency and the utilization of system. Peak load capacity also increases with the help of this application.
- If we talk about Performance the web services is used as the system interference and it is monitored, it is consistent and loosely coupled architectures are constructed.
- Device & location independence it is meant that it can be easily access from anywhere by using a web browser as it can be access with the help of internet only.
- Agility is the important factor that improves the user's ability to re-provision technological infrastructure resources.
- Cost is reduced as it need a fewer IT skills to be implemented.
- It may increases the Productivity as multiple users the same data at a time and can work on it which vanishes the time of waiting for one another due to which user can not have to save or emailed it.
- The application improves the reliability of the system which makes well designed computing for business purpose and problems recovery.
- It is elastic in nature as it scale up or down according to needs.
- Measuring services is pay as you go billing.
- It is having an on demand self service facility which help in the consumer to provision computing facilities without the requirement of human interaction with this service.

ISSUES OF SECURITY IN CLOUD COMPUTING

Security is the major issue in cloud computing as the number of moving parts are increasing and that are under our control but they can be interoperated by other which are not under our control.
The main factor which influence the security issue is:-

- The unawareness of user that how the services is provided.
- The control is lost is implied in cloud computing
- The network security border is not well demarcated.
- It is risky with the compromise the confidential or secret information & intellectual property.

LEVEL OF COMPUTING

For knowing more about the cloud computing one should the types of computing are:-

1) Grid Computing:- It is in the form of grid that work in form of distribution and parallel computing.

2) Fog Computing:- It is a type of distributed paradigm that provides data & application services close to the client and also handles the level of network in smart & end user client side devices.

3) Dew Computing:-In the existing computing hierarchy it is a ground level of computing.

4) Utility Computing:-The packaging of computation and storage i.e. computing resources, as a metered service similar to a traditional public utility.

ISSN 2348 – 7968

5) Peer-to-Peer: - It is a client server network in which the participants are both the suppliers and the consumer of the resources.

Figure -3

ROLES IN CLOUD COMPUTING

There are five main positions in cloud computing:-

1. The one that provide the cloud known as cloud provider. This entity is responsible for many of things like requested software/platform/infrastructure services and also handling of the security and protection issues. It is also responsible for availability of service to the consumer. It also helps in the management of three service layers, physical resources & portability etc.
2. The one who is the ultimate stake holder known as cloud consumer or user.
3. The one that manages delivery of cloud services and helpful in negotiating the relationship between the provider and user is known as cloud broker. Generally a cloud broker is being contacted by the user for the services.
4. The one that carries assessment of services, performance and security independently and is known as cloud auditor.
5. The one that is intermediate which is responsible for the connectivity and transportation of cloud services and is known as cloud carrier.

SERVICE MODEL

This service model helps in differentiating the services provided by the cloud. So that the organization can easily decide that which type of services they are required. The service models are:-

1. IaaS (Infrastructure as a Service)
2. PaaS (Platform as a Service)
3. SaaS (Software as a Service)

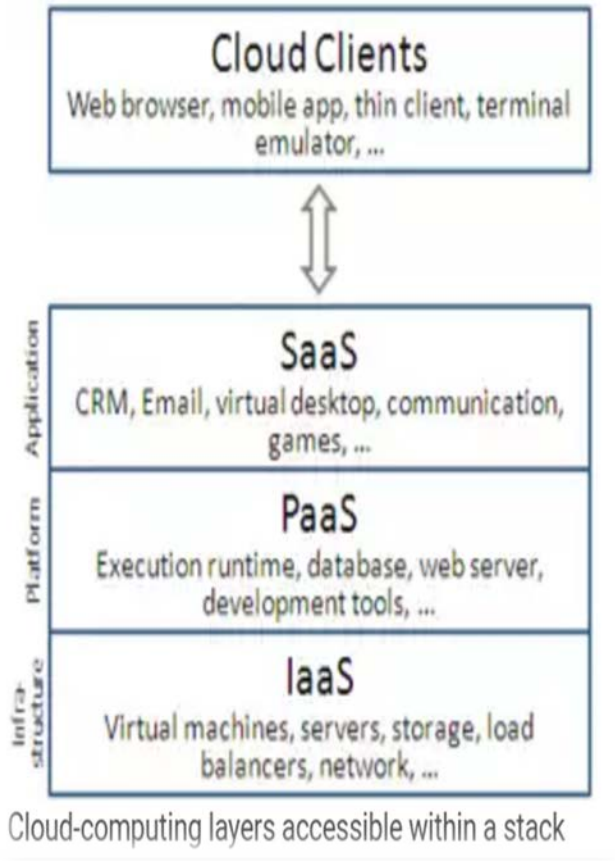

Figure -4

SECURITY ISSUES IN SERVICE MODELS:-

- **Infrastructure as a Service:-**
  The sensitive data & critical applications contain by virtual machine creates security challenges for organizations off premise to public and shared cloud premises that it relied on network perimeter which is a method to

ISSN 2348 – 7968

protect their data centre. In Iaas OS security issues alive. Revoke compliance and breach security policies revoke.

- **Platform as a Service :-**
  The network intrusion prevention and host are below the application level which is given by the provider to the people to build application on the top of the platform is the scope of provider.

  `

- **Software as a Service :-**
  There are many security issues as data security, network security, data locality, data integrity, data access, data segregation, authorization & authentication, data confidentiality, web application security, data breaches, virtualization vulnerability, availability, back up & identity management on sign-on process.

SOLUTION APPROACHES

3 types of public cloud service providers are:-

1-Amazon Web Services

2-Windows azure

3-Google AppEngine

There are many solutions for the dealing of problem in the security system in cloud computing. Many of them are as follows:-

1- Firewall: - It is the solution in which one has to remember there is a private cloud i.e. entire cloud infrastructure which belongs to the organization and can't be shared with any other organization. The cloud service provider provides the pooled resources that are shared by multiple organizations. If we are having a private cloud which is dedicated or linked to a single organization it does not mean that there aren't going to be multiple business units to see their stuff there is always a privacy with the outside world and the world of the organization.

2- Intrusion detection and prevention:-we can detect the problem in the system by adapting the preventing intrusion or even and detecting the techniques on different layer of an information system. It is taken as network layer (network IDS/IPS) to the operating system layer (host IDS), or even application or middleware layers (database IDS, firewall). If we are analyzing the apache server logs for the detection intrusion or discovery attempts is also a kind of IDS this IDS function can be implemented to any application generated log/ information.

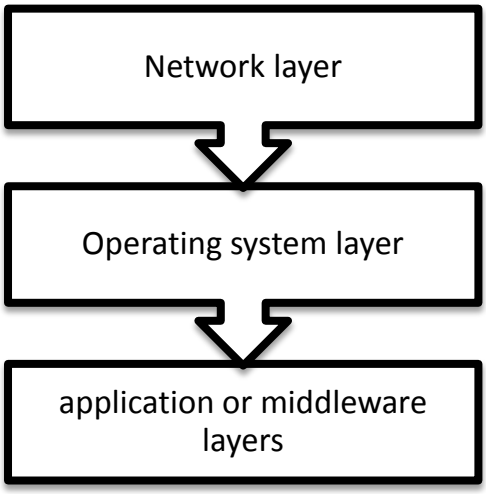

Figure 5

3- Integrity Monitoring: - Both the file and configuration integrity is being monitored by the file integrity. Looking at:-
   * Raw file contents
   * Permissions
   * Registry settings
   * Security setting

It is impartment to maintain back up to both on & off. We use to accommodate rapid recovery of recent data from onsite as well as long term off-site storage.

4- Log inspection: - The event correlation and log aggregation is quickly and efficiently identifies and resolves potential security threats with the sophisticated process. For security events the log inspection collects and analysis operating system & application logs.

ISSN 2348 – 7968

Its rules are being optimized important security events identification which is buried in the multiple entry logs. These types of events can be sent to a standalone security system but its maximum visibility is contributed when it is being forwarded to –

1. Security Information and Event Management, or
2. Centralized logging server

For correlation, reporting and achieving. As at virtual machines the integrity monitoring, inspection capabilities must be applied.

This software on cloud resources enables: -

1- Suspicious behavior detection
2- Collection of security related administrative actions.
3- Optimized collection of security events across your data centre.

ACKNOWLEDGEMENT

In today's world the cloud computing is being used by millions of people all around the world but still some work needs to be done on this for the betterment of the program. There is still works needs to be done to facilitates its use instill confidence in its promised manner and capabilities, address users security and privacy this issue should be kept in mind to encourage innovation. Some of the research issues that should be done for security and the question arises how to:-

* Secure cloud While maintaining availability
* Provide secure keys assignment scheme for cloud users
* Make browser secure against various types of attacks
* Develop secure API for cloud users
* While putting the business on cloud the security issues are very necessary to kept in mind of the user
* And so on…….

Figure 6

CONCLUSION

From this research paper we can conclude that the security outsourcing issues of cloud computing. This issue is big enough to solve that which of the cloud computing security is necessary and easy to be done and in which manner it should be done.

Now I we talk about the problems i.e. critics of cloud computing we can take some example in which the part of the things grasp by the different person seems to be different to the persons because they don't see the whole thing. So it concluded that the cloud computing is not just a new model to work on it is also an IT service delivery.

There are lots of things that help in resolving problem because there are lots of challenges for research about security issue. The cloud user are being provided by security as a service.

ISSN 2348 – 7968

REFERENCES:-

[1]. US NIST SP 500-291, " NIST Cloud Computing Standards roadmap" –V 1.0, July 2011 www.csrc.nist.gov/

[2]. Department of Electronics and Information Technology (Deity), Government of India's "GI Cloud (Meghraj) strategic Direction Paper", April 2013. www.deity.gov.in

[3]. Security and privacy issues in cloud computing, Lakshmi Narayan tatwani, Research scholar, mewar University, India

[4]. Institute of Electrical and Electronics Engineering 'IEEE Cloud Computing" Quarterly Magazine; May 2014. http://cloudcomputing .ieee.org/

[5]. Control Cloud Data Access Privilege And Anonymity With Fully Anonymous Attribute-Based Encryption.

[6]. A. Shamir, "Identity-based cryptosystems and signature schemes,"in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 1985,

[7]. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag,

[8]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryptionfor fine-grained access control of encrypted data," in *Proc. 13thCCS*, 2006, pp. 89–98.

[9]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Proc. IEEE SP*, May 2007, .

[10]. M. Chase, "Multi-authority attribute based encryption," in *Theory of Cryptography*. Berlin, Germany: Springer-Verlag, 2007