Cloud Computing Security Issue

Joy Shalom Sona [2],Ravi Verma[2].Firdous Parveen [3].Pratikhsa Jadhav[4]

[1,2]Assistant Professor, PCEM, Bhilai CG India
joy.parhivi@gmail.com
raviverma7@gmail.com

Abstract:-*Cloud computing is a fully net dependent technology wherever consumer information is hold on and maintain within the data center of a cloud service provider. Cloud computing is associate design for providing computing service via the net on demand and pay per use access to a pool of shared resources particularly networks, storage, servers, services and applications, without physically getting them. So it saves managing value and time for organizations. The security for Cloud Computing is rising area for study and this paper provide security topic in terms of cloud computing supported analysis of Cloud Security treat sand Technical elements of Cloud Computing.*

Keywords: Cloud, Services, Cloud service user, Cloud service provider, Security Issues , License Risk, Data Availability

1. Introduction

The cloud computing is a new computing model which comes from grid computing, distributed computing, parallel computing, virtualization technology, utility computing and other computer technologies and it has more advantage characters such as large scale computation and data storage, virtualization, high expansibility, high reliability and low price service. The security problem of cloud computing is very important and it can prevent the rapid development of cloud computing. This paper introduces some cloud computing systems and analyzes cloud computing security problem and its strategy according to the cloud computing concepts and characters. The data privacy and service availability in cloud computing are the key security problem. Single security method cannot solve the cloud computing security problem and many traditional and new technologies and strategies must be used together for protecting the total cloud computing system. We are conducting research on secure cloud computing .Due to the extensive complexity of the cloud; we contend that it will be difficult to provide a holistic solution to secure the cloud at present. Therefore our goal is to make increment enhancements to securing the cloud that will ultimately result in a secure cloud. In particular, we are developing a secure cloud consisting of hardware, software and data . Our cloud system will

2. (a) Support efficient storage of encrypted sensitive data
3. (b) Store, manage and query massive amounts of data
4. (c) Support fine grained access control and
5. (d) Support strong authentication.

2.Cloud Computing Architecture

Cloud management system is split into four layers, respectively the Resources & Network Layer, Services Layer, Access Layer, and User Layer. every layer includes a collection of functions[1]:

- The Resources & Network Layer manages the physical and virtual resources.
- The Services Layer includes the most classes of cloud services, namely, NaaS, IaaS, PaaS, SaaS/CaaS, the service orchestration function and therefore the cloud operational perform.
- The Access Layer includes API termination perform, and Inter-Cloud peering and federation perform.
- The User Layer includes End-user perform, Partner perform and Administration perform.
- The Cross layer includes Management, Security & Privacy, etc. are thought of as that covers all
- the layers.

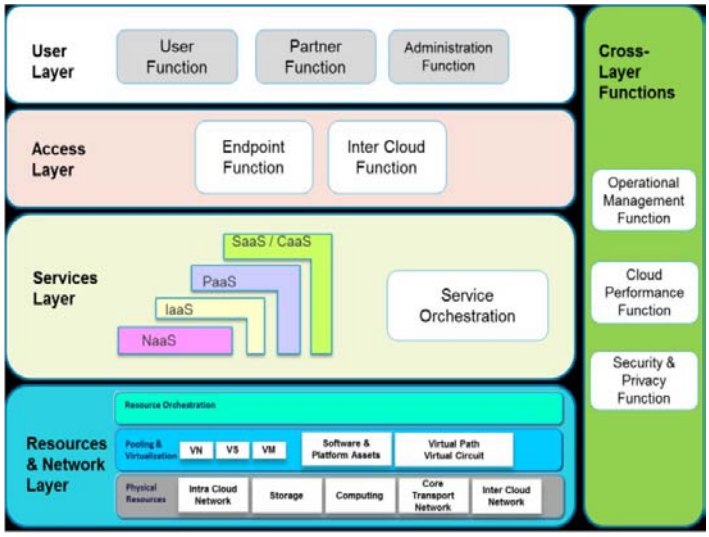

Figure. 1 The Cloud Computing Components

3. Services Provided

Generally cloud services are often divided into 3 categories:

- Software as a Service (SaaS),
- Platform as a Service (PaaS), and
- Infrastructure as a Service (IaaS).

3.1Software-as-a-Service (SaaS):

SaaS is delineated as a method by that Application Service supplier (ASP) offer totally different computer code applications over the net. This makes the client to get rid of installing and in operation the applying on own laptop and additionally eliminates the tremendous load of software system maintenance; continued operation, safeguarding and support .SaaS seller mindfully takes responsibility deploying and managing the IT infrastructure (servers, operating system

software package, databases, information center area, network access, power and cooling, etc) and processes (infrastructure patches/upgrades, application patches/upgrades, backups, etc.) needed to run and manage the total answer. SaaS options a whole application offered as a service on demand. Samples of SaaS includes: Salesforce.com, Google Apps.

3.2 Platform as a Service (PaaS):

PaaS is that the delivery of a computing platform and solution stack as a service while not software downloads or installation for developers, IT managers or end-users. It provides an infrastructure with a high level of integration so as to implement and check cloud applications. The user doesn't manage the infrastructure (including network, servers, in operation systems and storage), however he controls deployed applications and, possibly, their configurations. Samples of PaaS includes: Force.com, Google App Engine and Microsoft Azure.

3.3 Infrastructure as a Service (IaaS):

Infrastructure as a service (IaaS) refers to the sharing of hardware resources for execution services using Virtualization technology. Its main objective is to create resources like servers, network and storage additional readily accessible by applications and in operation systems. Thus, it offers basic infrastructure on-demand services and using Application Programming Interface (API) for interactions with hosts, switches, and routers, and therefore the capability of adding new instrumentality in a very easy and clear manner. In general, the user doesn't manage the underlying hardware within the cloud infrastructure, however he controls the in operation systems, storage and deployed applications. The service supplier owns the instrumentation and is chargeable for housing, running and maintaining it. The consumer usually pays on a per-use basis. Samples of IaaS includes Amazon Elastic Cloud Computing (EC2), Amazon S3, Go Grid.

4. Security Problems

4.1 Virtual Machine Security
4.2 Network Security
4.3 Information Security
4.4 Information Privacy
4.5 Information Integrity
4.6 Information Location
4.7 Information Availability

4.1 Virtual Machine Security:

Virtualization is one in every of the most elements of a cloud. Virtual machines area unit dynamic i.e. it will quickly be reverted to previous instances, paused and restarted, comparatively easily. Ensuring that different instances running on an equivalent physical machine area unit isolated from one another may be a major task of virtualization. They can also be readily cloned and seamlessly rapt between physical servers. This dynamic nature and potential for VM sprawl makes it tough to attain and maintain consistent security. Vulnerabilities or configuration errors could also be unknowingly propagated. Also, it's tough to keep up an auditable record of the protection state of a virtual machine at any given purpose in time. Full Virtualization and Para Virtualization are two sorts of virtualization during a cloud computing paradigm. In full virtualization, entire hardware design is replicated virtually. However, in para-virtualization, associate degree software system is changed so it may be run at the same time with alternative operating systems. VMM (Virtual Machine Monitor), is a software layer that abstracts the physical resources utilized by the multiple virtual machines. The VMM provides a virtual processor and alternative virtualized versions of system devices such as I/O devices, storage, memory, etc. several bugs are found altogether widespread VMMs that permit escaping from Virtual machine. Vulnerability in Microsoft Virtual laptop and Microsoft Virtual Server may permit a guest software system user to run code on the host or another guest software system. Vulnerability was found in VMware's shared folders mechanism that grants users of a guest system read and write access to any portion of the host's classification system together with the system folder and alternative security-sensitive files. Vulnerability in Xen may be exploited by "root" users of a guest domain to execute arbitrary commands. the other issue is that the management of administrator on host and guest operative systems. Current VMMs (Virtual Machine Monitor) don't supply excellent isolation. Virtual machine monitor ought to be 'root secure', meaning that no privilege inside the virtualized guest environment permits interference with the host system.

4.2 Network Security:

Networks area unit classified into many varieties like shared and non shared, public or personal, little space or giant space networks and each of them have variety of security threats to take care of. Problems related to the network level security comprise of DNS attacks, mortal attacks, issue of reused scientific discipline address, etc which area unit explained in details as follows. A Domain Name Server (DNS) server performs the interpretation of a website name to associate degree scientific discipline address. Since the domain names area unit much easier to recollect. Hence, the DNS servers area unit required. But there area unit cases once having referred to as the server by name, the user has been routed to another evil cloud rather than the one he asked for and thence mistreatment scientific discipline address isn't forever possible. Although mistreatment DNS security measures like: name System Security Extensions (DNSSEC) reduces the results of DNS threats however still there area unit cases once these security measures encourage be inadequate once the trail between a sender and a receiver gets rerouted through some evil connection. it's going to happen that even finally the DNS security measures area unit taken, still the route designated between the sender and receiver cause security problems[7]. Sniffer attacks area unit launched by applications which will capture packets flowing during a network and if the information that's being transferred through these packets isn't encrypted, it may be scan and there area unit possibilities that important data flowing across the network may be copied or captured. A mortal program, through the NIC (Network Interface Card) ensures that the data/traffic linked to alternative systems on the network conjointly gets recorded. It can be achieved by putting the NIC in promiscuous mode and in promiscuous mode it will track all information, flowing on an equivalent network. A

malicious sniffing detection platform supported Hans Arp (address resolution protocol) and RTT (round trip time) may be used to observe a sniffing system running on a network . Reused scientific discipline address issue are an enormous network security concern. once a selected user moves out of a network then the IP-address related to him (earlier) is allotted to a brand new user. This typically risks the protection of the new user as there is a sure pause between the amendment of associate degree scientific discipline address in DNS and therefore the clearing of that address in DNS caches. And hence, we will say that typically tho' the recent scientific discipline address is being allotted to a brand new user still the possibilities of accessing the data by another user isn't negligible because the address still exists within the DNS cache and therefore the information happiness to a selected user might become accessible to another user violating the privacy of the initial user .

4.3 Information Security:

For general user, it's quite straightforward to search out the doable storage on the facet that gives the service of cloud computing. To achieve the service of cloud computing, the foremost common utilized communication protocol is machine-readable text Transfer Protocol (HTTP). so as to assure the information security and data integrity, machine-readable text Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) area unit the foremost common adoption. In a traditional on-premise application readying model, the sensitive information of every enterprise continues to reside inside the enterprise boundary and is subject to its physical, logical and personnel security and access management policies. However, in cloud computing, the enterprise information is keep outside the enterprise boundary, at the Service supplier finish. Consequently, the service supplier should adopt further security checks to ensure information security and forestall breaches owing to security vulnerabilities within the application or through malicious employees. This involves the employment of sturdy encoding techniques for information security and fine-grained authorization to control access to information. Cloud service suppliers like Amazon, the Elastic reckon Cloud (EC2) directors don't have access to client instances and can't log into the Guest OS. EC2 directors with a business want area unit needed to use their individual cryptographically sturdy Secure Shell (SSH) keys to achieve access to a number. All such accesses area unit logged and routinely audited. whereas the information at rest in straightforward Storage Service (S3) isn't encrypted by default, users will encode their data before it's uploaded to Amazon S3, so it's not accessed or tampered with by any unauthorized party[3].

4.4 Information Privacy

The data privacy is additionally one among the key issues for Cloud computing. A privacy committee ought to even be created to help create choices associated with information privacy. Requirement: This will make sure that your organization is ready to fulfill the data privacy demands of its customers and regulators. Data in the cloud is sometimes globally distributed that raises issues about jurisdiction, information exposure and privacy. Organizations stand a risk of not obliging with government policies as would be explained more whereas the cloud vendors World Health Organization expose sensitive data risk legal liability. Virtual co-tenancy of sensitive and non-sensitive information on an equivalent host conjointly carries its own potential risks[2].

4.5 Information Integrity:

Data corruption will happen at any level of storage and with any type of media, therefore Integrity observance is important in cloud storage that is crucial for any information center. Information integrity is easily achieved during a standalone system with one information. Data integrity in such a system is maintained via information constraints and transactions. Transactions ought to follow ACID (atomicity, consistency, isolation and durability) properties to ensure information integrity. Most databases support ACID transactions and might preserve information integrity. information generated by cloud computing services area unit unbroken within the clouds. Keeping information in the clouds suggests that users might lose management of their information and believe on cloud operators to enforce access management.

4.6 Information Location:

In general, cloud users aren't attentive to the precise location of the datacenter and conjointly they are doing not have any management over the physical access mechanisms to it information. Most well-known cloud service suppliers have datacenters round the globe. In many a cases, this may be a difficulty. owing to compliance and information privacy laws in varied countries, neighborhood of knowledge is of utmost importance in several enterprise design. as an example, in many EU and South America countries, sure sorts of information cannot leave the country as a result of doubtless sensitive information. Additionally to the difficulty of native laws, there's conjointly the question of whose jurisdiction the information falls below, when an investigation happens. Next within the complexness chain area unit distributed systems. during a distributed system, there area unit multiple databases and multiple applications . In order to keep up information integrity during a distributed system, transactions across multiple information sources have to be compelled to be handled correctly during a fail safe manner. this may be done employing a central global group action container. every application within the distributed system ought to be ready to participate within the world group action via a resource manager.

4.7 Information Availability:

Data handiness is one among the prime issues of mission and safety crucial organizations. once keeping information at remote systems owned by others, information homeowners might suffer from system failures of the service supplier. If the Cloud goes out of operation, information can become unavailable because the information depends on a single service supplier. The Cloud application must guarantee that

enterprises area unit supplied with service round the clock. This involves creating subject field changes at the appliance and infrastructural levels to feature quantifiability and high handiness. A multi-tier design must be adopted, supported by a load balanced farm of application instances, running on a variable number of servers. Resiliency to hardware/software failures, as well on denial of service attacks, must be engineered from the ground up inside the appliance. At an equivalent time, an appropriate action arrange for business continuity (BC) and disaster recovery (DR) must be thought of for any unplanned emergencies.

5.Security Guidance

General security guidance to deal with the above threats can be found in:

• Encryption and Key Management: Encryption provides data protection while key management enables access to protected data. It is strongly recommended to encrypt data in transit over networks, at rest, and on backup media. In particular, data encryption at rest (e.g., for long-term archival storage) can avoid the risk of malicious cloud service providers or malicious multi-tenants abuse. At the same time, secure key stores (including key backup and recoverability) and access to key stores must be securely implemented since improper (or access to) key storage could lead to the compromise of all encrypted data.

• Identity and Access Management: Secure management nonidentity and access control is a critical factor to prevent account and service hijacking. It is strongly recommended to prohibit sharing of account credentials, to leverage strong (multi-factor) authentication if possible, and to consider delegated authentication and managing trust across all types of cloud services.

6. Conclusion

Cloud service suppliers have to be compelled to inform their customers on the level of security that they supply on their cloud. during this paper, we first mentioned numerous models of cloud computing, security issues knowledge security is major issue for Cloud Computing. There are many different security challenges as well as security aspects of network and virtualization. New security techniques have to be compelled to be developed and older security techniques required to be radically tweaked to be ready to work with the clouds architecture.

References

[1] Kundu, C. D. Banerjee, P. Saha, "Introducing New Services in Cloud Computing Environment", International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.

[2] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.

[3] R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.

[4] B. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[5] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing," Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[6] Pring et al., "Forecast: Sizing the cloud; understanding the opportunities in cloud services," Gartner Inc., Tech. Rep. G00166525, March 2009.

[7] Aman Bakshi, Yogesh B. Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine," ICCSN '10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.

Author Profile

Joy Shalom Sona received the B.E. degree in Computer Science & Engineering from Pt.R.S.S.U., Raipur(C.G.) in 2008 & M.Tech. degree in Computer Science Engineering with specialization in Computer Technology from CSVTU Bhilai (C.G.), India He is currently working as a Assistant Professor in Computer Science Engineering. He has published 4 research papers in reputed national and international journals. His research areas include Computer Technology, Software Engineering, Data Mining, Artificial Intelligence, Computer Network & Web Mining, Cloud Computing etc.