Gurpreet Singh, kanwalpreet Kaur, Sandhya Vats / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 3, May-Jun 2012, pp.2820-2823

# Cloud Computing Services and Vulnerabilities

**Gurpreet Singh[#1], kanwalpreet Kaur[#2],Sandhya Vats[#3]**
Computer science department, Guru Nanak College, Budhlada(Mansa),Punjab India

**Abstract - Cloud computing is one of the rising trends in the in progress IT enterprise. Due to it's nature of on demand computing as service, it means whenever you need the service cloud is there to make available you those services that you can inhibit on your PC, laptop or work station. Cloud computing is providing services that organization necessitate to complete their business requirement with low cost and minimum management over head. It inhabits the advantages of an assortment of computing technologies such as cluster computing, grid computing, distributed computing etc. whereas there are various vulnerabilities in the cloud computing some of them are explored and some of them are still under the shells. These once triggered can loss to company reputation, customer data and code which is residing in cloud provider premises. So in this paper we discuss the vulnerabilities in the cloud which can cause this serious effect on the cloud.**

***Keywords*** **- cloud computing, security**

## I. INTRODUCTION

Cloud computing (cc) provides dynamically scalable & virtualized method to access the resources through internet. Cloud computing provides economics benefits over the traditional client server computing. This computing is introduced to deal with the existing computing problems, such as limited data capacities complicated business process and the scale of services and infrastructure in the enterprise. CC is able to fulfil these requirements, by combining the advantages of mainframe computers, distributed systems, grid computing etc.. Cloud computing is utilising the software advancement in various fields e. g network storage technique, virtualized techniques and low cost server construction techniques etc. to build the basic block of the cloud environment. CC reduces the capital expenditure by pooling the resources over the internet virtually. The motivation for setting up such a pool-based computing paradigm lies in two important factors: *economies of scale* and specialisation. The result of a pool-based model is that physical computing resources become 'invisible' to consumers, who in general do not have control or knowledge over the location, formation, and originalities of these resources (e.g. database, CPU, etc.) There are basically five services in the cloud these are as Software as a Service which uses the services of Platform as a Service, and PaaS uses the services of infrastructure as service. IaaS can include the Network as a service and Data storage as service.

Various techniques are used and combined to build cc system depending on the type of cloud IaaS, PaaS, SaaS, DaaS .

Cloud Computing is: A pool of scalable IT-enabled capabilities which can be utilised over the internet (Cloud) as a service. The idea of Cloud Computing is based on a very fundamental principal of re-usability of IT capabilities. The difference that Cloud Computing brings compared to traditional concepts of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to broaden horizons across organisational boundaries.

Forrester's definition of Cloud Computing

"A pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end-customer applications and billed by consumption ."

According to the IEEE Computer Society Cloud Computing is:

"A paradigm in which information is permanently stored in servers on the Internet and cached temporarily on clients that include desktops, entertainment centres, table computers, notebooks, wall computers, hand-held, etc."

A computing Cloud is a set of network enabled services, providing scalable, QOS guaranteed, normally personalised, inexpensive computing infrastructures on demand, which could be accessed in a simple and pervasive way.

On-demand self-service: [1] A consumer with an instantaneous need at a particular timeslot can avail computing resources (such as CPU time, network storage, software use, and so forth) in an automatic (i.e. convenient, self-serve) fashion without resorting to human interactions with providers of these resources.

## II. EXISTING WORK IN CLOUD

Cloud computing can be classified in the following service model according to service provided by the cloud to customers.

*Software as a service*: cloud provider release their applications on a hosting environment, which can be accessed through networks from various web clients, example of SaaS are as Gmail, Google docs, salesforce.com. most common SaaS are www.pdftoword.com . This provides a online conversion of pdf files to document files without the prior knowledge of the customer about the underlying hardware required. Also customer is also not concern about he web hosting details. as in the SaaS data is

uploaded to the hosting environment for conversion, means user have no control over the data regarding their access rights conflicts, as well as privacy policies of the network. These can lead to information leakage. There are various security issues related to the authentication and the authorisation to SaaS environment.

*PaaS* : provide a development platform underneath the full software life cycle which allows cloud customer to widen cloud services and applications directly on the PaaS cloud e.g. it may possible that Google mail may use another cloud model PaaS to develop the SaaS for the their customer rather than establishing their own infrastructure. PaaS in cloud provides various facilities such as programming environment tools, configuration management, compilers, linker, loaders, resource manager etc. . Example of PaaS is Google AppEngine. Main security issues related to the PaaS is data and the code residing on the provider premises, with out proper access and privacy policies on data, may lead to information loss. As well as any delay and performance loss occur to computation of customer data, due to chain supply can cause enterprise a lot, e.g. cost for contract violation.

*IaaS*: cloud customers directly use the infrastructure resources e. g processing, storage networks and other computing resources provided by the service provider according to their requirement. To implement the IaaS, virtualization is extensively used in IaaS; virtualization is used for meet the growing and shrinking resource demand from cloud customers. The basic strategy of virtualization is to set up independent virtual machines (VM) that are isolated from both underlying hardware and other VM. Such as various websites are hosted by Google or yahoo of small scale organisation. With this organisations are now free form overhead of controlling and managing the IT infrastructure just by paying the hosting charges to cloud IaaS provider. There are also some serious security concerns about the resource isolation failure, resource exhaustion, mapping, non-resistant. There are various vulnerabilities related to the virtual machines are as randomness chaos, virtualization impact on storage, VM sprawl and VM reset Vulnerabilities.

*Data storage as a service*: with the advancement in virtualized storage this is becomes a separate filed. It is also a part of the IaaS because indirectly we are using the storage hardware and network facilities of the provider. IaaS facilitates a customer to eliminate the cost involved to establishing a server, software license, in-house IT maintenance cost etc. this allow user to pay for what they are actually using rather then the site license for the entire data base. E.g. Amazon S3, Google Big Table and Apache HBase etc. there can be various security issues of different data base schema when both the service provider providing the same facilities to customer, uptime and download time which lead to unavailability of the customer data. Natural disaster of the data residing at the provider premises.

In [2] there is various security concerns which are common to the entire model discussed above which are as follow:

Because all the models discuss above uses the network as the backbone for the communication attack on the network are directly inherited in the cc model. These are phishing, malware, Trojan attacks, collaborative attacks, distributed denial of service etc. which leads to denial of service.

There is another security concern which is forensics of cloud as well as metering of what the customer uses on cloud environment, should be fair. Network vulnerabilities combined with the metering and forensics lead to the loss of the integrity of the cloud service provider. This include frauds in billings amounts .

Authentication and authorisation of the cloud customer related to all the models. Where some of the problems related to the password recovery is also an issue. Authorisation related to access polices related to the data and user of the cloud environment. cloud is dynamic in nature, requirement of the cloud user is changing dynamically which lead to change in access policies of the data and user also lead to serious problems.

Central point of the failure is also is a serious concern in the cloud models such as which lead to unavailability of the service.

## III DEPLOYMENT MODEL

Define what types of services are provided by the provider to various customers. Where a customer can be public users, an organisation or a firm, or it can be industry like medical sciences.

*Private cloud:* the cloud infrastructure is operated solely with in the single organisation or provided by a third party, regardless whether it is located within an organisation premises or off the premise from organisation. There are various motivation factor such as maximum utilisation of existing in-house resources and security concerns including data privacy and trust. Also make private cloud an option for many firms academics often build private cloud for research and teaching purposes.

*Community clouds*: These types of cloud constructed by various organisations jointly constructed and share the same cloud infrastructure as well as policies, requirements values and concerns. The advantages of community cloud are as e. g degree of economic scalability and democratic equilibrium. These type of services are hosted by the other within one organisation or by third party.

*Public cloud*: this is the dominant form of cloud computing in which provider deploy the model to facilities the customer requirements and charge for their services as per the provider profit e.g. EC2, S3, Google AppEngine etc.

*Hybrid cloud*: it is combination of two or more cloud models that remains unique entities but is bound together by

standardised or proprietary technology that enables data and applications portability. Organisation use the hybrid cloud model to optimise their resources to increase their core competences by merging out peripheral business function on to the cloud while controlling core activates on premise through private cloud.

## IV USER REQURIEMENT FOR SAAS:

There are various risk involved in the development of the SaaS. Classification of these risk can be e security, performance, availability, deployment etc. security concern involve the risk involve either on the cloud server side, or on client environment and can be communication links. Cloud computing is dynamic in nature and this extends the problem space of security to new dimensions. Cloud computing also extends the requirements of authentication and authorisation, encryption and decryption, key management etc. Authentication, in traditional computing environment is limited to user name and password but cloud computing expends this to new dimensions, user name and password are not suitable to define the user privileges to access the data stored on the cloud. Cloud also extend the password recovery to another extend where as in traditional computing it is not the serious concern. Whereas performance related risks are concerns with the efficient use of the underlying hardware because the performance parameters change when scalability matter. Because the cloud environment provide huge scalability for user at any instance of time. With the collaboration of infinite resources available on the cloud.

Availability, how data will be managed on the cloud server. Cloud should support the smooth access to the data which is stored on the cloud by cloud client. Whereas access policies should be defined for the cloud user, as well as for the cloud provider. Deployment of the services is also a major issue in case of cloud computing because in cloud computing, there are various heterogeneous servers present over the internet and when we connect them to form cloud there should be server interoperability issue, For the cloud manager. Due to infinite size of the cloud, metering issues are also a major concern. Tracking the availability and reliability of each component is also a concern.

Cloud provider may also import some services form other service provider's this increase complexity of the cloud manager with respect to data security and service security..

In brief all the security requirement of the cloud security, availability, deployment, performance etc. are concern on user assets which are there data, stored on the cloud environment. This data is processed by different cloud services and require security of data when travel between different services.

Classification of users

We can classify the user in two broad classes such as:

Individual user: this user which accesses the cloud software services for individual and for this user, availability is not the major concern, but lack of availability of software may lead to loss of business and reputation loss. Security requirements of this user may also be less as compare to other. Data confidentiality is highly required. Access and security policies must be defined at time of user start the serves.

Enterprise user: this includes the users which belong to a enterprise or a organisation which can be profit or non profitable. These enterprises may have different services requirements and access policies. Enterprise user uses the SaaS services to develop their own application and then theses develop services can further be licensed to other user so there should be good definition of access and security policies. Further enterprise also needs the authentication for Set of service they use with their performance related issues. Further enterprise user should be aware of regular update of the product. And it's the services provider that provide the information to the user at regular basis regarding updates and remove a service. Availability of the software is also the concern for the enterprise user because unavailability of the service may lead to loss of revenue due to delays in projects.

Software service provider: these are set of software service provider's that provide their software services to cloud data enters and these can be specific application of a general application according to the provider details. Etc.

The metering problem arises in SaaS when a cloud computing service is being used for huge search database. A client making a search query may hold reservations whether the server performed a complete search, scanning the table(s) in entirety before returning the results to the client According to [8], short of insight in billing and metering, this is one of the major challenges being faced by the IaaS, SaaS [4] users. Some cloud service providers such as Amazon's EC2 do not provide any kind of real time reporting or API for their cloud billing. This may lead to trust issues which arise when a client doubts whether the computation task provided by the cloud service was executed completely and correctly or whether the user was billed fairly for its service.

Lack of Audit ability and Compliance. The fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public audit ability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed[5].

Compliance refers to the user are bounded to obey the rules or request made by the cloud provider.[6]

Audit and compliance complexity is another side effect of the lack of control in the cloud.

Legalisation of cloud: the involvement of various law groups in cloud computing contract drafting & negotiations has taken care of both the Enders i.e. customer as well as service provider. But still there are some hard nuts to crack [7].

## V REQUIREMENTS FOR THE CLOUD COMPUTING ARCHITECTURE.

In [2], the fact that the client side is inherent to cloud computing leads to the implication that security risk assessments and solutions must be end-to-end rather than limited to service provider. Features of cloud computing architecture must enable the assurance of data transmission security from clients, via brokers and cloud managers, across to process-servers, and out to data-servers. The data that is stored and processed within the cloud must have assured data integrity and data access security, and that depends on special within cloud computing infrastructure.

Further, client-side infrastructure embodies a vast array of vulnerabilities, particularly in the case of consumer oriented devices and software , even more so in the case of devices that support user profiles

Other requirements of user's requirements depend on end-to-end, cooperative actions. In particular satisfactory levels of authentication need to be achieved, through identity authentication components or APIs. And by accepting externally managed identities e.g. shibboleth and Open id.

For application that support any form of personally identifiable data, components and features are necessary to support privacy protections as well as access protection. Application should also provide their authenticities that are corresponding to same service provider, using any sort of key management techniques.

There should be proper data auditing is required for the user to confirm that there data is always stored on the cloud data centre even user may not access the data frequently. Auditing also demand privacy preserving auditing mean no user data is leaked to the auditing part if this is third party.

There should be some sort of message encryption and decryption scheme to protect data from travelling over the network.

There is always certainty of data and information loss either form natural disasters or cloud provider mishandling or device failure this should be avoided for the smooth functioning of the cloud provider services to clients or consumers. Also there is need of tracking the services of the various cloud components is also require to understand that either the particular server is in condition to handle the queries or data requests of the user.

## VI. CONCLUSION

There are still unexplored securities breaches are there. Some of them we try to explore in this paper and , there are some issue that we elaborated require attention. There is no such model which addresses the all security issues of SaaS. We will come up with a model that will overcome these mentioned security issues with minimal over head and achieving the performance concerns. On cloud computing mostly work is conceptual , practical concerns are still lacking off. Because this is a new field and requirements of security and other issues are not completely defined in the problem space. So we will try to figure out some problems of the cloud computing with respect to SaaS.

## REFERENCES

[1] P. Mell and T. Grance, "Draft nist working definition of cloud computing - v15," *21. Aug 2009*, 2009 [2] M. Akay, *Time Frequency and Wavelets in Biomedical Signal Processing* (Book style). Piscataway, NJ: IEEE Press, 1998, pp. 123–135.

[2] Roger Clarke, 'user requirements for cloud computing Architecture' Proceedings in 2010 1oth ACM/IEEE international Conference on Cluster, Cloud, and Grid Computing.

[3] Tharam Dillon, Chen Wu Elizabeth Chang ,"cloud computing: Issues and Challenges", proceedings in IEEE 2010 24th international conference on advance information networking and applications.

[4] Jiyi WU, Lingdi PING, Xiaoping GE,Ya Wang, Jianqing FU , "Cloud Storage as the Infrastructure of Cloud Computing**",** IEEE 2010 International Conference on Intelligent Computing and Cognitive Informatics

[5] Preserving public auditing in cloud computing http://www.chennaisunday.com/MobileComputing/Privacy-preserving%20Public%20Auditing%20for%20Data%20Storage%20Security%20in%20Cloud%20Computing.pdf.

[6] Auditability and Compliance in the Cloud:John Soat http://www.informationweek.com/cloud-computing/blog/archives/2010/05/auditability_an.html

[7] A Cloud Computing Customer Bill of Rights Contribute By:**David** https://www.infosecisland.com/blogview/8738-A-Cloud-Computing-Customer-Bill-of-Rights.html

[8] Rituik Dubey, Muhammad Asim Jamshed, Xiaohui Wang, Rama Krishna Batalla: Addressing Security Issues in Cloud Computing

.[9] Morgan R L., Cantor S., Carmody S. Hoehn W., Klingenstein K. (2004) 'federated Security: The Shibboleth Approch educause Quarterly 27,4 (2004) at http://www.educause.edu/EDUCAUSE+Quarterly/EDUCAUSEQuarterlMagzineVolum/FederatedSecurityThe Shibboleth/157315.

[10] wikepedia entry, at http://en.wikepedia.org/wiki/OpenID..