Cloud Computing Security - its challenges and suggestions.

Mrs. Devyani Ranadhir Patil
C/o – Milind B. Tupe. "Nirmal" , 201, Sadhu Nana Vasti, Sadesatra Nali , Hadapsar, Pune.

Acknowledgments:

I thank to **Dr. Nilesh Mahajan** , IMED BVDU for his valuable advice and guidance at the start of the research paper, and for his constructive feedback throughout this work. I really appreciate his interest and enthusiasm during this research paper.

Abstract:

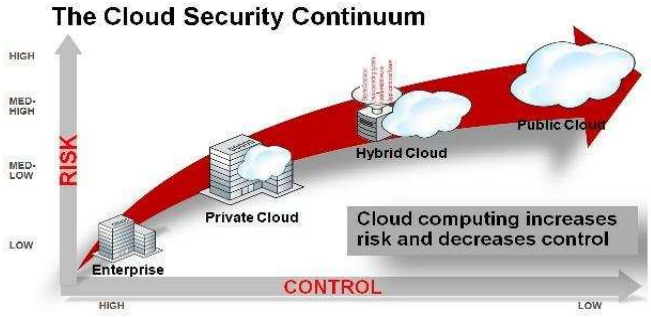
Cloud Computing is one of the important technology in the field of computer, Information and Electronic related domain. Cloud Computing is dedicated to flexibility of sharing resources and hence it is also treated as resource sharing technology. In Cloud computing it is possible to share hardware and software to its dedicated peers. Use of cloud computing makes your work very easy at anywhere, anytime on internet. Cloud delivery is suitable for a wide range of security services for basic needs such as malware, security monitoring, and policy compliance and application security. Organizations use the Cloud in a variety of different service models (SaaS, PaaS, IaaS) and deployment models (Private, Public, Hybrid). There are a number of security issues,concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers. This paper highlights some issues related to cloud security and suggest solutions.

Keywords: *Cloud Computing, Cloud Security, Private Cloud, Public Cloud, Hybrid Cloud.*

Introduction:

Cloud Computing is the combination of technology, platform that provides hosting and storage service on internet. Many companies developing and offering cloud computing products and services but have not properly implications of processing, storing and accessing data in a shared and virtualized environment [1]. Cloud computing let you access all your applications & documents from anywhere in the world, freeing you from confines of desktop and make it easier for group members in different locations to collaborate [2]. This cloud infrastructure roughly categorizes into either private or public. In private cloud, infrastructure is managed and owned by customer and located on premise. Customers data is under his control and is only granted to trusted parties. On the other hand in case of public cloud the infrastructure is owned and managed by cloud service provider and customer data is outside his control and cloud potential be granted to untrusted parties[2]. So here security will come into picture. Cloud is classified into three major segments:

1) **Saas** – Software–as-a-service, service provided as applications to consumer using standardized interfaces. e.g.- Google applications, Facebook, Youtube etc.
2) **Paas** – Platform-as-a-service, service provided as operation and development platform to consumers. e.g. Microsoft Azure, Google AppEngine,Amazon Simple DB/S3.
3) **Iaas** – Infrastructure-as-a-service e.g. Amazon EC2. GoGrid FlexiScale [3].



As shown in above figure there are mainly three types of cloud computing **Public cloud, Private cloud** & **Hybrid cloud.** The Private Cloud is used by single organization but public cloud is used by more than one. So in comparison, private cloud gives better control & more flexibility. Hybrid cloud is combination of both private & public cloud & it is mostly used by industries. Cloud Computing is an evolution of on-demand information service. The applications of cloud are increasing in many sectors like in IT, agriculture, automobile, medical etc. There are lot of advantages of using cloud services but we should always consider the major security issues in cloud computing. There are multiple techniques used in cloud like Public cloud computing, Private cloud computing, Internal, External cloud computing. But data is not 100 % secured in any of these techniques. The major benefits of cloud are

a) Cost Efficient
b) Almost Unlimited Storage
c) Backup and Recovery
d) Easy Access to Information

Objective:

The paper focuses on Cloud Computing Security issues and provides Suggestions.

The major issues in cloud computing security are

a) Technical Issues- It is possible for you to retrieve information at any time any where there is Internet connection, if there is no any dysfunction related to your service provider.
b) Prone to Attack- There is a possibility of lurking of data because nothing on Internet is completely secure.
c) Data Security- This is an important part in cloud computing security. To avoid data loss there are multiple techniques used which is briefly listed in this paper.
d) Host security.
e) Network Security [15]

As there are so many challenges in cloud computing then why it is necessary for industries to use it, because on cloud it is very easy to store large and secure data for small as well as large organizations. It is also easy to categories your data in the form of software, platform of infrastructure by using cloud category.

Research Gap:

Now a day's cloud computing is an increasing craze in IT world. It is useful for multinational companies as well as small organizations. Organizations are completely depends on service providers (cloud). This paper just list out problems in today's cloud computing security but do not discuss on future problems that may arises like below.

Hardware capability improvements: The inevitable improvements in processor speed and increased memory capacities across IT infrastructure will mean that the cloud will be able to support more complex environments with improved performance capabilities as standard.

Tackling complexity: Despite the efforts of multiple technology vendors this challenge of complexity remains unresolved. IT architectures continue to be difficult to implement, under-utilized and expensive to operate. The massive scale of cloud computing only strengthens the need for self-monitoring, self- healing and self-configuring IT systems comprising heterogeneous storage, servers, applications, networks and other system elements

Increasing use of mobile devices: Laptop sales have overtaken desktops over the last few years and the trend will continue as an increasing range of mobile devices such as notebooks. Mobile phone incorporates many of features found on desktop based PC only. .[14]

Here is a comparison between the situation before the cloud computing and after the cloud computing. Before the use of cloud computing it was very difficult to store large data. To store large data required increase in size and number of servers and it was very complicated to maintain the networking between the servers. If anyone server has failed then whole network will be collapsed. Automatically it will affect on cost estimation of that organization. You need a whole team of experts to install, configure, test, run, secure, and update data. It will be manageable for small scale industry but what about large scale industry. After cloud computing concept was evolved it is very easy to maintain this data because there is another service provider who will store and protect your data and it is very helpful for small as well as large scale industry. With a cloud app, you just need to open a browser, log in, customize the app, and start using it. So this is a part of research gap in this paper.

Literature Review

1) Security threats on cloud users are both external and internal.

An application level security is depends on cloud user first and secondly provider is also responsible for the providing physical security and for enforcing external firewall policies. Security for intermediate layers of the software stack is shared between the user and the operator. The lower level of abstraction exposed to the user, the more responsibility goes with it. Cloud providers must guard theft or denial-of-service attacks by users. In other words, users need to be protected from each other. Virtualization is widely used in today's clouds because of its powerful defense and protection against most of the attempts by users to attack each other or the underlying cloud infrastructure [5].

2) Architecture of a Cryptographic Storage Service.

Cloud architecture consists of three components: a data processor (DP), that processes data before it is sent to the cloud; a data verifier (DV), that checks whether the data in the cloud has been tampered with; and a token generator (TG), that generates tokens to enable the cloud storage provider to retrieve segments of customer data; and a credential generator that implements an access control policy by issuing credentials to the various parties in the system (these credentials will enable the parties to decrypt encrypted files according to the policy) [2].

3) There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management [1].

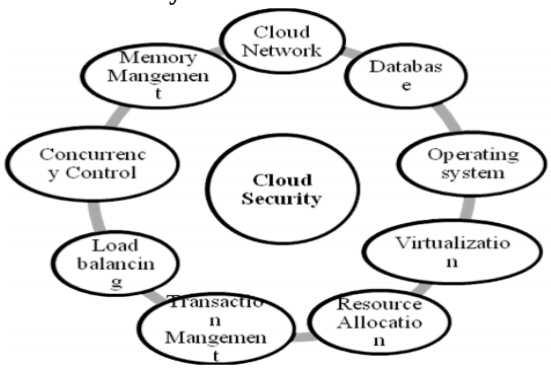
4) Four Major Trends That Impact Cloud Security- 1) Changing attackers and threats 2) Consumerization of IT. 3) Evolving architecture technologies. 4) Dynamic and challenging regulatory environment [6].

5) As data security is an important issue in cloud computing then multiple techniques are used for this problem like Access Control Techniques, Data Categorization and the Use of Data Labels, Application of Encryption for Data at Rest and in Motion etc.[15].

Challenges & its Suggestions:

The major Cloud Computing challenges related to security are as below.

1) **Data Protection** – Security of data is important when it is in rest and when it is in transfer that data should be encrypted in all time and that should be decrypted at relevant clients only those having own encryption keys[7].
2) **User Authentication** – Data must be used by authorized users only so that providers have data access logs and to verify that only authorized users are accessing the data. These access logs and audit trails additionally need to be secured and maintained by companies for as long as the company needs or legal purposes require [7].
3) **Contingency Planning** – Companies should have contingency plan if their cloud provider will be corrupt or fail.
4) **Parameters affecting on cloud security** –



5) **Costing Model -** Use of Cloud can significantly reduce the infrastructure cost, and increases the cost of data communication, i.e. the cost of transferring an organization's data to public cloud and community Cloud .The cost per unit of computing resource used is likely to be higher. This problem will be avoid if the consumer uses the hybrid cloud deployment model where the organization's data is distributed amongst a number of public/private (in-house IT infrastructure)/community clouds and intuitively, on demand [8].
6) **Charging Model-** For SaaS cloud providers, the cost of developing multi-tenancy to single-tenancy. include: re-design and redevelopment of the software that was originally used for, cost of providing new features allow for intensive customization, performance and security enhancement for concurrent user access, and dealing with complexities induced by the above changes. Therefore, a strategic and viable Charging model for SaaS provider is crucial for the profitability and sustainability of SaaS cloud providers.[8]
7) **Service Level Agreement (SLA)-** It is vital for consumers to obtain guarantees from providers on service delivery. Typically, these are provided through Service Level Agreements (SLAs) negotiated between the providers and consumers. SLA is a way that has an appropriate level of granularity, namely the tradeoffs between expressiveness and complicatedness, so that they can cover most of the consumer expectations [8].
8) **Host Security-** The host running the job, the job may well be a virus or a worm which can destroy the system from malicious users

9) **Network security issues-**Denial of Service**:** where servers and networks are brought down by a huge amount of network traffic and users are denied the access to a certain Internet based service. Like DNS Hacking, Routing Table "Poisoning through congestion, delaying or dropping packets, or through resource hacking [15].

Suggestions in cloud:

Cloud Security is highly important - This means that organizations with cloud security and other tools will be able to adopt and protect next-generation IT trends without too many complications [9].

1) **The big data-enabled feature**- Now a days big data is not a phenomenon but it is rapidly increasing phenomenon as organizations continue to use tools like social media and mobile devices that produce mountains of information per use. In the coming years, leveraging big data will be a necessity to remain competitive because the information gathered will allow firms of all sizes to reduce costs, improve customer service and efficiency in the workplace [10].

2) **Cloud data protection methods**- In order to protect data you can use following techniques.

2.1. Authentication and Identity- Authentication is usually predicated on an underlying identity infrastructure. If file is used by single user then it is secure but same file is used by multiple users then it is not possible to protect it [15].

2.2. Access Control Techniques-Access control mechanisms are a key means by which we maintain a complex IT environment that reliably supports separation and integrity of different levels or categories of in format ion belonging to multiple parties. But access controls do not stand on their own; they are supported by many other security capabilities, access control is dependent on an identity management capability that meets the needs for the implementation.[15]

2.3. Data Categorization and the Use of Data Labels - In identifying and categorizing data, what we face is a multifaceted problem. Besides identifying classes of information that are sensitive or otherwise have value and labeling such information according to its characteristics, we need to protect such data, usually by means such as file permissions, encryption, or more sophisticated container approaches. We also need identity-based access controls to support organizational access policies. Data or information labeling is one information security technique that has been used to great success for classified information such as the hierarchical categories of Unclassified, Confidential, Secret, Top Secret, and Compartmented [15].

2.4. Application of Encryption for Data at Rest and in Motion-Encryption is a key component to protect data at rest in the cloud. Employing appropriate strength encryption is important: Strong encryption is preferable when data at rest has continuing value for an extended time period. If such long-term value encrypted data is obtained by a third party and if they have an extensive period of time to break or *crack* the encryption, then the reward can be well worth the effort. There are multiple ways of encrypting data at rest

Full Disk: Encryption of data at the disk level—the operating system, the applications in it, and the data the applications use are all encrypted simply by existing on a disk that is encrypted.

Directory Level (or File system): In this use of encryption, entire data directories are encrypted or decrypted as a container. Access to files requires use of encryption keys. This approach can also be used to segregate data of identical sensitivity or categorization into directories that are individually encrypted with different keys.

File Level: Rather than encrypting an entire hard drive or even a directory, it can be more efficient to encrypt individual files.

Application Level*:* The application manages encryption and decryption of application-managed data. [15]

2.5 Data Masking -This technique is aimed at reducing the risk of exposing sensitive information. Data masking has also been known by such names as data obfuscation, de-identification, or depersonalization. These techniques are intended to preserve the privacy of records by changing the data so that actual values cannot be determined or re-engineered. [16]

3) Increase communication- The more conversation that exists within IT teams, Service Providers, organization - the more effective data protection can be. Centralize data and monitoring keeps cloud security efforts is very good work . While it remains key to equip IT employees with the tools necessary for secure data within the cloud, a staff-wide culture of awareness of data and email security best practices can be an invaluable asset, too.[11]

4) Always backup your data - One of the most overlooked aspects of and one of the easiest way to increase the control of your data is to make sure that whatever happens, you have a secure backup of that data.

5) Get references from other clients - When in doubt, ask your cloud provider for client references to check out that, they are also facing the same problems related to security. Financial, healthcare, insurance, or government organizations are a good start. References don't guarantee anything. Be sure to contact these references directly when possible to see what these companies are using the cloud services for the same purpose.

6) Consider a hybrid security model - Incorporate a mix of services delivered in-the-cloud and on premises. This can help allay data security and privacy concerns as well as leverage legacy investments.

7) Choose wisely - When selecting a partner to deliver services via the cloud, select a partner with a heritage in both IT and security services. Verify that risk mitigation is part of the provider's security practice. Pick a service provider that can integrate IT, security and network services, as well as provide robust service-performance assurances [13]

Conclusion:-

This Paper introduce security challenges and provide suggestions in cloud computing. Also give brief information about various useful data security methods used in cloud. In the future, we will extend our research by providing implementations and producing results to justify our concepts of security for cloud computing.

References:

[1] Prince Jain, "Security Issues and their Solution in Cloud Computing", International Journal of Computing & Business Research Available From: http://pdf-release.net/852553/Security-Issues-and-their-Solution-in-Cloud-Computing on 17 Dec 2013

[2] Joshi Mahima & Moudgil Yudhveer Singh, "Security Cloud Storage" , International Journal Of Computer Science & Communication Networks. Available From : *http://*ojs.academypublisher.com/index.php/jnw/article/download/.../6549 on 22 Jan 2014

[3] Qi Zhang · Lu Cheng · Raouf Boutaba University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1 "State –of-the-art and research challenges" Available from :.blog.com/Cloud-computing-**state-of-the-art-and-research-challenges**. On 25 Dec 2013

[4] https://blogs.oracle.com/OracleIDM/entry/addressing_the_top_5_cloud

[5] Kazi Zunnurhain1, and Susan V. Vrbsky ,Department of Computer Science ,The University of Alabama"Security in Cloud Computing ",

[6] Intel IT Center Planning Guide | Cloud Security Available From : www.**intel**.in ***cloud****-computing-****security-planning-guide****2.pdf*

[7]http://www.webopedia.com/DidYouKnow/Hardware_Software/cloud_computing_security_challenges.html

[8] Kuyoro S O.& Ibikunle F & Awodele O. "Cloud Computing Security Issues and Challenges". Computer Science Journals (CSI) Available From: www.researchgate.net on 26 Jan 2014

[9] Available On http://blog.gogrid.com/2013/04/19/cloud-is-key-to-unlocking-security-opportunities/

[10] Available On http://blog.gogrid.com/2013/03/20/as-big-data-evolves-cloud-comes-into-focus/

[11] Available On http://www.proofpoint.com/about-us/security-compliance-and-cloud-news/articles/3-tips-to-improve-cloud-security-549324

[12] Available On http://www.onlinetech.com/resources/e-tips/cloud-computing/top-5-tips-for-cloud-computing-securityhttp://www.onlinetech.com/resources/e-tips/cloud-computing/top-5-tips-for-cloud-computing-security

[13] Available on http://www.net-security.org/secworld.php?id=9442

[14] Available on http://www.academia.edu/3276145/Cloud_Computing_Challenges_and_Future_Trends

[15] Rawat Satyendra Singh Rawat & Mr. Soni Alpesh, "A Survey of Various Techniques to Secure cloud storage" , National Conference on Security Issues in Network Technologies (NCSI-2012) August 11-12,2012 Available From: http://webcache.googleusercontent.com

******