International Journal of Research in Advent Technology, Vol.5, No.4, April 2017
E-ISSN: 2321-9637
*Available onlin*e at www.ijrat.org

Addressing Data Security Challenges in Cloud Computing

Pavan R Jaiswal [#], B D Zope [$], M M Shingare [*]
Dept of CE, PICT, Pune [#$]*
pavan.jaiswal85@gmail.com [#], bdzope@pict.edu [$], mmshingare@pict.edu [*]

Abstract - Cloud computing is fastest growing trend. It has got technology connection with grid computing, distributed computing and utility computing. Big cloud service providers – Google, IBM, Microsoft, Amazon etc provides application to the users along with on demand access. This includes remote data storage as well. Now the concern comes for how to secure remotely stored data on cloud-based? This article focuses on understanding cloud computing, its services, deployment models. More to this focus is made on highlighting various cloud data security challenges and solution is provided by applying data encryption mechanism.
Index Terms - Cloud computing, data security, multi-tenancy, ISV

I. INTRODUCTION

Cloud computing security more often referred as cloud security; is a broad set of technologies, controls and set of policies deployed to protect application, its data and associated infrastructure of cloud. Pressure is always there on organization to consider moving cloud based services and solving security issues [1]. There are different cloud-based deployment models, including private, public or hybrid cloud which can be chosen by respective organization as per the requirements [w1].
Security design and its implementation can be influenced by kind of service models organization selects. Most popular cloud service models are: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS).

IaaS: are self-service models for accessing, monitoring, and managing remote datacenter infrastructures, such as compute (virtualized or bare metal), storage, networking, and networking services (e.g. firewalls) [w2].

PaaS: are used for applications, and other development, while providing cloud components to software.

SaaS: represent the largest cloud market and are still growing quickly. SaaS uses the web to deliver applications that are managed by a third-party vendor and whose interface is accessed on the clients' side. Most SaaS applications can be run directly from a web browser without any downloads or installations required, although some require plugins.

Cloud is known to deploy confidential information and critical IT resources. This fact leads to make a concerns about vulnerability to attack. Especially this happens because of multi-tenant and anonymous nature of cloud computing. Applications and storage volumes often reside next to potentially hostile virtual environments, leaving information at risk to theft, unauthorized exposure or malicious manipulation [2]. Few surveys indicates that vendors do not recycle storage devices securely. There are some governmental regulations for data privacy and location which applies additional concerns of legal and financial consequences if data confidentiality is breached [w1].

II. CLOUD COMPUTING DEFINED

NIST definition [w3] - Cloud computing is a model for enabling ubiquitous, convenient, on- demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Essential characteristics:

- ***On demand self-service*** – A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- ***Broad network access*** – Capabilities are available over a network and accessed through standard mechanism.
- ***Resource pooling*** – The provider's computing resources are pooled to serve multiple consumers using multi-tenant model.
- ***Rapid elasticity*** – Capabilities can be elastically provisioned and released. In some cases automatically to scale rapidly outward and inward commensurate with demand.

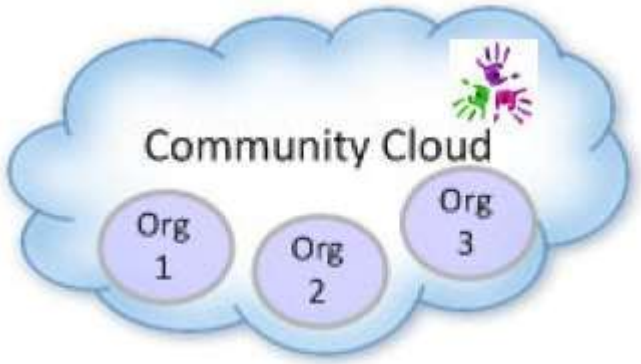
- ***Measured service*** - Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts).

III. DEPLOYEMNT MODEL

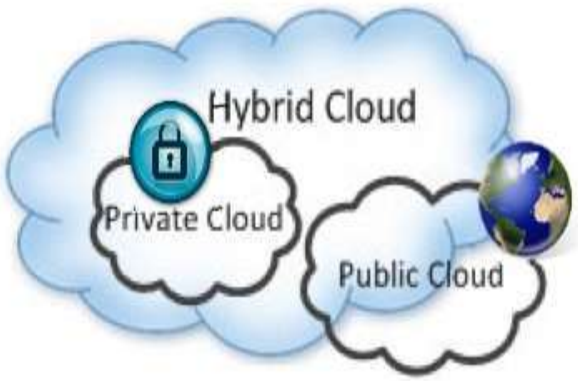
Private cloud - A private cloud is one in which the services and infrastructure are maintained on a private network [w4,w5]. These clouds offer the greatest level of security and control, but they require the company to still purchase and maintain all the software and infrastructure, which reduces the cost savings.

Public cloud - A public cloud is one in which the services and infrastructure are provided off-site over the Internet. These clouds offer the greatest level of efficiency in shared resources; however, they are also more vulnerable than private clouds.

Community cloud - The model type community cloud shares the cloud infrastructure across several organizations to support specific community having common concerns [w4,w5]. In this model, cloud infrastructure is provided on the premises or at the data center owned by third party. This is managed by participating organizations or third party.



Hybrid cloud - A hybrid cloud includes a variety of public and private options with multiple providers. By spreading things out over a hybrid cloud, you keep each aspect at your business in the most efficient environment possible. The downside is that you have to keep track of multiple different security platforms and ensure that all aspects of your business can communicate with each other.



IV. CLOUD COMPUTING SECURITY CHALLENGES

In traditional datacenters, IT managers put procedures and controls in place to build a hardened perimeter around the infrastructure and data they want to secure. This configuration is relatively easy to manage, since organizations have control of their servers' location and utilize the physical hardware entirely for themselves.

1. Multi-tenancy

Multi-tenancy [w6] is an architecture in which a single instance of a software application serves multiple customers. Each customer is called a tenant. Tenants may be given the ability to customize some parts of the application, such as color of the user interface (UI) or business rules, but they cannot customize the application's code.

- ***Potential cost of re-architecture*** [w7] – Let's face it, no IT service provider has a magic recipe to automatically make your on-premise product into on-demand product. So an ISV (Independent Software Vendor) that is thinking about SaaS has two options – either re-build the

entire architecture from the ground up or weave in multi-tenancy into the existing product. Either way, it is going to be costly.

- ***Security*** **–** One of the most often touted concerns from a customer perspective – is my data going to be secure? Often times, a lot of extra design and development needs to happen around the product and database to keep sensitive data safe since the data all resides in the same database in different schemas.
- ***Hosting*** **–** Even if an ISV is not hosting their own product, hosting for multi-tenant architectures needs a lot of prep work and that is why not all hosting providers can be a good fit for multi-tenant products. The database configurations, the shared infrastructure and other related issues can make it complicated sometimes to find the right hosting company.

2. Data mobility and control

Moving data from static physical servers onto virtual volumes makes it remarkably mobile, and data stored in the cloud can live anywhere in the virtual world. Storage administrators can easily reassign or replicate users' information across data centers to facilitate server maintenance, HA/DR or capacity planning, with little or no service interruption or notice to data owners. This creates a number of legal complications for cloud users. Legislation like the EU Privacy Act forbids data processing or storage of residents' data within foreign data centers. Careful controls must be applied to data in cloud computing environments to ensure cloud providers do not inadvertently break these rules by migrating geographically sensitive information across political boundaries.

3. Data privacy

It is well-known that cloud computing has many potential advantages and many enterprise applications and data are migrating to public or hybrid cloud [w8]. But regarding some business-critical applications, the organizations, especially large enterprises, still wouldn't move them to cloud. The market size the cloud computing shared is still far behind the one expected. From the consumers' perspective, cloud computing security concerns, especially data security and privacy protection issues, remain the primary inhibitor for adoption of cloud computing services.

4. Data remanence

Although the recycling of storage resources is common practice in the cloud, no clear standard exists on how cloud service providers should recycle memory or disk space. In many cases, vacated hardware is simply re-purposed with little regard to secure hardware repurposing. The risk of a cloud tenant being able to gather pieces of the previous tenants' data is high when resources are not securely recycled. Resolving the issue of data remanence can frequently consume considerable negotiating time while establishing service agreements between an enterprise and a cloud service provider.

V. SOLUTION TO DATA SECURITY CHALLENGES

Encryption is suggested as a better solution to secure information [3,4]. Before storing data in cloud server it is better to encrypt data. Data Owner can give permission to particular group member such that data can be easily accessed by them. Heterogeneous data centric security is to be used to provide data access control. A data security model comprises of authentication, data encryption and data integrity, data recovery, user protection has to be designed to improve the data security over cloud [w9]. To ensure privacy and data security data protection can be used as a service.

To avoid access of data from other users, applying encryption on data that makes data totally unusable and normal encryption can complicate availability [5,6]. Before uploading data into the cloud the users are suggested to verify whether the data is stored on backup drives and the keywords in files remain unchanged. Calculate the hash of the file before uploading to cloud servers will ensure that the data is not altered. This hash calculation can be used for data integrity but it is very difficult to maintain it. RSA based data integrity check can be provided by combining identity based cryptography and RSA Signature. SaaS ensures that there must be clear boundaries both at the physical level and application level to segregate data from different users. Distributed access control architecture can be used for access management in cloud computing. To identify unauthorized users, using of credential or attributed based policies are better. Permission as a service can be used to tell the user that which part of data can be accessed.

Fine grained access control mechanism enables the owner to delegate most of computation intensive tasks to cloud servers without disclosing the data contents [4]. A data driven framework can be designed for secure data processing and sharing between cloud users. Network based intrusion prevention system is used to detect threats in real-time. To compute large files with different sizes and to address remote data security RSA based storage security method can be used.

VI. CONCLUSION

Although cloud computing is the new emerging technology that presents a good number of benefits to the users, it faces lot of security challenges. In this article data security challenges and solutions are provided for these challenges to overcome the risk involved in cloud computing. In future concrete standards for cloud computing security can be developed. To provide a secure data access in cloud, advanced encryption techniques can be used for storing and retrieving data from cloud. Also proper key management techniques can be used to distribute the key to the cloud users such that only authorized persons can access the data.

REFERENCES

1. "*The Need for Cloud Computing Security*" in: A Trend Micro white paper, July 2010
2. R Velumadhva Rao, K Selvamani, "*Data Security Challenges and its Solution in Cloud Computing*", in: ICCC-2015, p204-209
3. Eystein Mathisen. "*Security Challenges and Solutions in Cloud Computing"*, in:International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011),2011.p.208-212
4. Dimitrios Zissis, Dimitrios Lekkas, "*Addressing Cloud Computing Security Issues"*, in: Elsevier - future generation computer systems 28 (2012) 583-592
5. Kui Ren, Cong Wang, Qian Wang "*Security Challenges for Public Cloud*", in IEEE Internet Computing, Vol 16, Issue 1, p69-73
6. Qi Zhang, Lu Cheng, Raouf Boutaba "*Cloud Computing: State-of-the-art and Research Challenges*", in Journal of Internet Services and Applications, Vol 1, Issue 1, p7-18
7. Chunming Rong, Son. T. Nguyen, Martin Gilje Jaatun "*Beyond Lightening: A Survey on Security Challenges in Cloud Computing*" in Computers and Electrical Engineering, Vol 39, Issue 1, p47-54

WEB REFERENCES

1. https://social.technet.microsoft.com/wiki/contents/articles/3801.cloud-security-introduction.aspx
2. https://apprenda.com/library/paas/iaas-paas-saas-explained-compared/
3. http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf
4. http://www.dummies.com/programming/networking/comparing-public-private-and-hybrid-cloud-computing-options/
5. http://www.rfwireless-world.com/Tutorials/public-cloud-vs-private-cloud-vs-hybrid-cloud-vs-community-cloud.html
6. http://whatis.techtarget.com/definition/multi-tenancy
7. https://sumanchaudhuri.wordpress.com/2008/06/02/problems-with-multi-tenancy/
8. http://ieeexplore.ieee.org/abstract/document/6187862/
9. https://www.nasuni.com/news/26-top_5_security_challenges_of_cloud_storage/