www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 4 April, 2013 Page No. 1361-1363

Aspects of Security in cloud computing

Anu Rathi, Yogesh Kumar Anish Talwar

Assistant Professor
Dronacharya Group of institutions,
Greater Noida anujaglan@gmail.com

UG, CSE
Dronacharya Group of institutions,
Greater Noida
M18nikhilkumar@gmail.com

UG, CSE
Dronacharya Group of institutions,
Greater Noida
talwar.anish@yahoo.in

Abstract
Cloud services will eliminate the need to install and manage client rich applications and further its scope in all the private sector would increase thus it would help the company to reduce high cost infrastructure and maintenance cost. . In this paper we are surveying the security related issues in the field of cloud computing. We will discuss the different techniques regarding the data privacy and also the advancement in these techniques .This paper evaluates different data privacy techniques involved in Cloud computing and then proposing the most optimized technique. This paper focuses on the usage of Cloud services and security issues to build these cross-domain Internet-connected collaborations
.

Index terms -Cloud computing, cloud security, data security, SaaS, Private cloud.

1. INTRODUCTION
The word cloud is used as a metaphor for the Internet, based on the standardized use of a cloud-like shape to denote a network on telephony schematics and later to depict the Internet in computer network diagram as an abstraction of the underlying infrastructure it represents

As we know that Cloud-Computing is the latest trend and it refers to both the application delivered as services over the internet and the hardware. The services themselves have long been referred to as Software as a Service (SaaS).When a Cloud is made available as pay-as-you-go manner to the generic public, we call it Public Cloud , the services being sold is Utility Computing . On the other hand, the term Private Cloud refers to internal data centers of a business or other organization, thus not made available for general public. Cloud computing is emerging technology through which we can store and maintain the data but there are some security related issues regarding the data privacy and its content.

Conventionally the security of cloud computing has several loop holes which leads to loss of content and even the private data can be leaked through an external person or they can easily hack the server and can view our content. Sometimes even the cloud service provider can access our data and can get our personal information. The demand for improvement in performance, scalability, stability and security we will provide the technical foundation for future cloud computing security features.

The underlying concept of cloud computing dates back to the 1950s, when large-scale mainframe became available in academia and corporations, accessible via thin clients/terminal computers. Because it was costly to buy a mainframe, it became important to find ways to get the greatest return on the investment in them, allowing multiple users to share both the physical access to the computer from multiple terminals as well as to share the CPU time, eliminating periods of inactivity, which became known in the industry as time-sharing. In early 2008, Eucalyptus became the first open-source, AWS API-compatible platform for deploying private clouds. Then by mid-2008, Gartner saw an opportunity for cloud computing “to shape the relationship among consumers of IT services and those who sell them “and then most of the projects shifted towards Cloud-Computing hence leading to a dramatic growth of this new technology. .Finally on March 1, 2011 IBM announced the Smarter Computing framework to support support Smarter Planet. Among the various components of the Smarter Computing foundations, cloud computing is a critical piece.

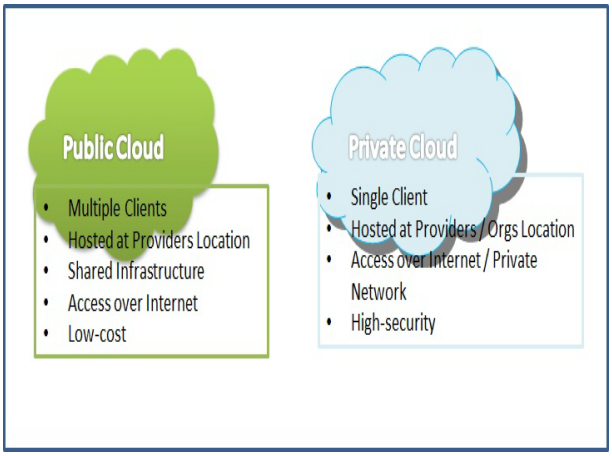

Fig 1: Types of Clouds

2. Related work

V. Krishna R et.al[1] proposed the main security issues at various levels existing in Cloud computing and categorized them into various distinguishing categories based on Cloud computing architecture. He suggested that there should be a balance between the risk identified at various levels of cloud computing architecture against the protection and privacy controls and expected limits from there utilization. He finally concluded that too several controls may be ineffective and inefficient, if the advantages overweigh the prices and associated risks. Also the security issues are to be addresses in all the levels of cloud environment with essential protocols, specifications and tools.

Deyan C et.al [2] describes all-round analysis on data security and privacy protection issues associated with cloud computing across all stages of data life cycle. He mentions some current solutions and proposed future research work about data security and privacy protection issues in cloud. He analyzed that according to service delivery models, deployment models and essential features of cloud computing, data security and privacy protection issues are the primary problems that need to be solved as soon as possible. Conclusion of his paper was that it is necessary to have integrated and comprehensive security solutions to meet the needs of defense in depth and the entire primary task such as privacy protection, privacy data identification and isolation should be considered during the design of cloud-based applications.

Kevin H. et.al[3] discussed about issues related to security for cloud computing environment and presented a layered framework for securing data stored in the cloud and then focused on both layers i.e. storage layer and the data layer. Also a scheme for the third party applications of the documents in the cloud. Author also discussed about XACML implementation for Hadoop and their benefits with the help of which building trusted applications from untrusted components will be a major aspect of secured cloud computing.

F.A. Alvi et al [4] reviewed the security and trust issues of cloud computing. His paper included some surveys which were conducted by IDC that show the motivation for the adoption of cloud computing. Also he discussed the issues and the solution to over-come these problems. Comparison of system performance is done with SACS model and without SACS model. He proposed the security model which is has more stable performance when facing the attacks threats. Finally his paper addresses the various issues that arise during the deployment of the cloud services after identifying these challenges some steps are explained to mitigate these challenges and solutions to solve these problems.

P. Shanthi B et.al [5] exposes the various security crisis related to data management also it includes the various tools for developing cloud computing and services provided by cloud computing with their key components. He further states that cloud is a virtualization of resources that maintains and manages itself; it deals with how the user can securely access data, resources and services to fulfill their dynamically changing needs. Also designing the cloud for educational purposes is provided. This paper investigated the infrastructure of cloud computing their services, security issues and virtual cloud computing are discussed.

3. Cloud computing

In today's world most companies want to store and retrieve data and cloud computing helps to make their job more flexible and easy to complete also the cost of storing huge amount of data will be minimal compared to storing the data physically or in an external device. Besides the benefits of cloud computing there are certain disadvantage which cloud faces and all these are regarding the security issues in order to separate one cloud user from another, in order to maintain data privacy, confidentiality and integrity. Moreover as cloud service provider has a complete control on the infrastructure, so security risk like manipulating or stealing of code by service provider exist (Cloud Security Alliance, 2010).
Cloud computing provides different services and these services are available into 3 models:
1) Software as a Service (SaaS)–it is mostly run by cloud service providers to the organizations and users can access this from the internet.
2) Network as a Service (NaaS)-it is a tool for developing the websites without installing any software on the system and without the administrator rights.
3) Internet as a Service (IaaS)-it is controlled and maintained through various cloud services providers and can perform task such as storage, hardware, networking and servers..

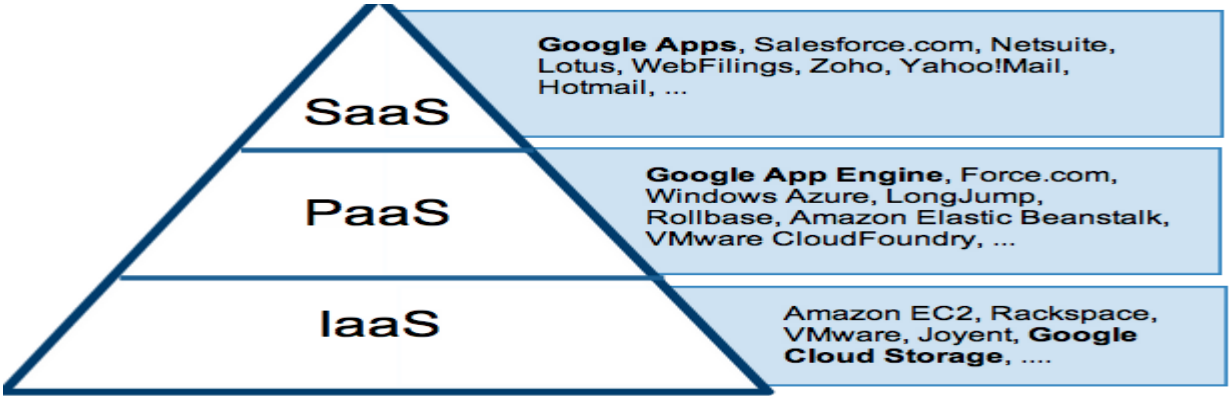

Fig2. Models of services in cloud computing

There are different types of clouds which can be categorized as follows:-

- Public cloud- this cloud infrastructure is available only for public or a large industry group and it is provided by single service provider selling cloud services like Google App engine or Amazon elastic cloud compute offer its users highly flexible cloud environment. They enable users to share and store data as per their personal capacities.
- Private cloud - it is generally operated by an organization and its main benefit is security and integrity of data.
- Hybrid cloud - this architecture is a mixture of two or more clouds. It helps in load balancing between the clouds.

Some characteristics of cloud computing are as follows:-

- Cloud-Computing is location independent which means that one can access the cloud from any location and retrieve data.
- The cloud services are provided on laptops, mobile phones and personal digital assistants which means that it uses ubiquitous network access
- It provides platform visualization environment rather than purchasing servers and software.
- Cloud services have an easy interfacing with technology and even a common person can understand the services of cloud and can operate it easily.

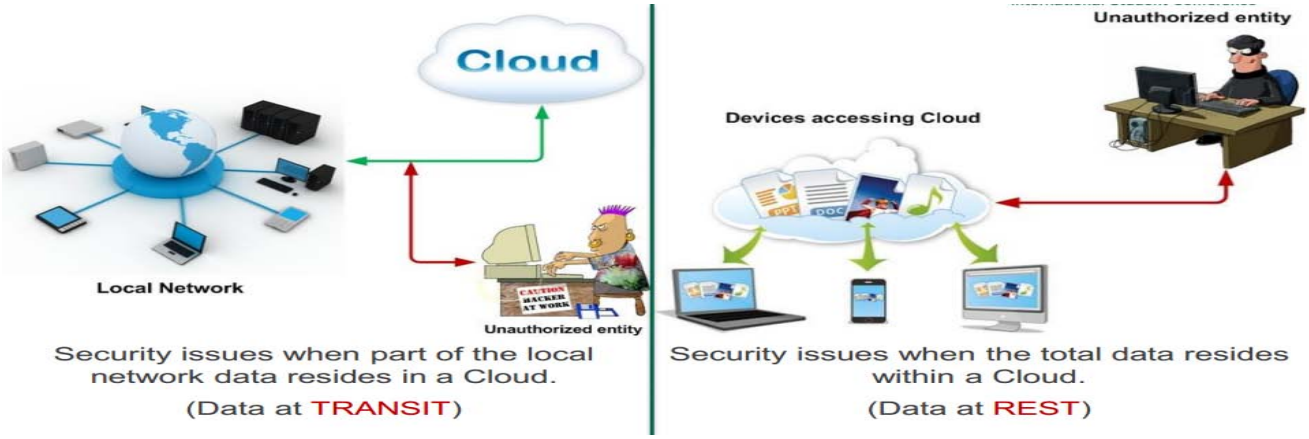

Fig3: Security Breach in Cloud Computing

This figure explain us how data is accessed from the cloud and how an unauthorized entity can access our private content.

4. Security measures in cloud computing

As the growth of cloud services are increasing, on the other hand the security of cloud computing services is a contentious issue that may be delaying its adoption. Cloud computing offers many benefits, but it is also vulnerable to threats. There are many challenges and risk in cloud computing that increases the threat of data being compromised. Security is becoming a major concern in order to establish trust in cloud computing technology.

Some of the major problems faced by cloud computing technology are as follows:-

- Lack of user control, in SAAS environment service provider is responsible to control data.
- Availability and backup is also a major drawback of this important consideration.
- Intrusion detection and prevention , we should have knowledge of our network and also we should examine the virtual network traffic.

- As our system gets complex the chances of misconfiguration takes place, because lack of expertise coupled with insufficient communication.
- Threat to access important information is also a major concern which can lead to huge loss of data and can even lead to hacking.
- Investigative support, investigating inappropriate or illegal activity may be impossible in cloud computing.

5. New Research fields in cloud computing security

The "black hat" community has also discovered cloud computing exploits that affect extensions of existing vulnerabilities, with dedicated cloud security track emerging at Black Hat USA 2009.

For example, username brute forcers and Debian Open SSL exploit tools run in the cloud as they do in botnets. Social engineering attacks remain effective—one exploit tries to convince Amazon Elastic Compute Cloud (EC2) users to run malicious virtual machine images simply by giving the image an official sounding name such as "fedora-core" . Virtual machine vulnerabilities also remain an issue, as does weak random number generation due to lack of sufficient entropy.

6. Security techniques used in Cloud Computing

Various security techniques used by Cloud computing providers to secure the transmission of data between Cloud and LAN are:

1. Service Level Agreement (SLA):

The SLA records a common understanding about services, priorities, responsibilities, guarantees, and warranties. Each area of service scope should have the "level of service" defined. The SLA may specify the levels of availability, serviceability, performance, operation, or other attributes of the service, such as billing. The "level of service" can also be specified as "expected" and "minimum," which allows customers to be informed what to expect (the minimum), while providing a measurable (average) target value that shows the level of organization performance. In some contracts, penalties may be agreed upon in the case of non-compliance of the SLA (but see "internal" customers below). It is important to note that the "agreement" relates to the services the customer receives, and not how the service provider delivers that service.

SLAs commonly include segments to address: a definition of services, performance measurement, problem management, customer duties, warranties, disaster recovery, termination of agreement.[1] In order to ensure that SLAs are consistently met, these agreements are often designed with specific lines of demarcation and the parties involved are required to meet regularly to create an open forum for communication. Contract enforcement (rewards and penalties) should be rigidly enforced, but most SLAs also leave room for annual revalidation so that it is possible to make changes based on new information.

2. Secure Socket Layer (SSL)

SSL (Secure Sockets Layer) is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser; or a mail server and a mail client (e.g., Outlook).SSL allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely. Normally, data sent between browsers and web servers is sent in plain text—leaving you vulnerable to eavesdropping. If an attacker is able to intercept all data being sent between a browser and a web server they can see and use that information.

More specifically, SSL is a security protocol. Protocols describe how algorithms should be used; in this case, the SSL protocol determines variables of the encryption for both the link and the data being transmitted.SSL secures millions of peoples' data on the Internet every day, especially during online transactions or when transmitting confidential information. Internet users have come to associate their online security with the lock icon that comes with an SSL-secured website or green address bar that comes with an extended validation SSL-secured website. SSL-secured websites also begin with https rather than http.

3. Role Based Access Control:

Role-based access control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise. In this context, access is the ability of an individual user to perform a specific task, such as view, create, or modify a file. Roles are defined according to job competency, authority, and responsibility within the enterprise.

When properly implemented, RBAC enables users to carry out a wide range of authorized tasks by dynamically regulating their actions according to flexible functions, relationships, and constraints. This is in contrast to conventional methods of access control, which grant or revoke user access on a rigid, object-by-object basis. In RBAC, roles can be easily created, changed, or discontinued as the needs of the enterprise evolve, without having to individually update the privileges for every user.

4. Third party Auditor (TPA)

TPA is the third party auditor who will audit the data of data owner or client so that it will let off the burden of management of data of data owner. TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The released audit report would not only help owners to evaluate the risk of their subscribed cloud data services, but also be beneficial for the cloud service provider to improve their cloud based service platform .This public auditor will help the data owner that his data are safe in cloud.

5. Proof of Retrievability:

A specific problem encountered in the context of cloud storage, where clients outsource their data (files) to untrusted cloud storage servers, is to convince the clients that their data are kept intact at the storage servers. An important approach to achieve this goal is called Proof of Retrievability (POR), by which a storage server can convince a client --- via a concise proof --- that its data can be recovered. However, existing POR solutions can only deal with static data (i.e., data items must be fixed), and actually are not secure when used to deal with dynamic data (i.e., data items need be inserted, deleted, and modified).Various techniques used to secure the data on cloud from unauthorized access are:

6. Multi tenancy based access control

When the roles, relationships, privileges, static and dynamic data scopes are user definable by the end customer, and when the sample application serves multiple customers / tenants (from a single instance of the application), then we need to store all these access control configurations - tenant wise. So during run time, we should not only resolve the data scopes-privileges-roles-users, but also apply the tenant context and look up the appropriate tenant specific access control settings, before deciding to allow or disallow a particular action in the application.

Privilege mapping should be possible at the field Level, entity Level, form Level and page Level, so that the end customer / tenant has absolute control and flexibility in defining and modifying "Who sees what" and "Who can do what" in the system.

7. Intrusion Detection system

There are various Intrusion Detection Systems having various specifications to each. Cloud computing have two approaches i. e. Knowledge-based IDS and Behavior-Based IDS to detect intrusions in cloud computing. Behavior-Based IDS assumes that an intrusion can be detected by observing a deviation from normal to expected behavior of the system or users. Knowledge-based IDS techniques apply knowledge accumulated about specific attack . Knowledge-based IDS can't detect unknown attacks, but it uses rules and monitors a stream of event s to find malicious characteristics and set the new rules for unknown attacks.

8. Virtual private network

VPN (Virtual private network) is a secure private network enabled over a public infrastructure like Internet. On getting the cloud VPN services, your system is connected to remote server located in another country through an encrypted tunnel. Besides, all information routed through the tunnel is encrypted before being allowed inside. Decidedly, it keeps your data beyond the reach of hackers, scammers, etc, because users need validation before being authorized to access the tunnel. On top of it, both the ends of the VPN tunnel are secured by tunneling protocols like PPTP, L2TP, IPSec, etc. Moreover, you will also be assigned a new IP address generated from a remote server based in another country. On browsing with the server generated IP, your privacy and data will remain protected as nobody would know your real online identity.

9. A Novel Cloud dependability model

A novel cloud dependability model CDSV is established to enhance the security of heterogeneous cloud environments. System-level virtualization techniques are used to enhance the dependability of cloud environments. Systematic analysis shows that this model can enhance the system dependability and security. Experimental results show that the dependability model CDSV can efficiently and safely construct dependability relationship in heterogeneous cloud environments.

7. Conclusion & Future scope

Cloud computing technology is facing many challenges regarding the security of data but also on the other hand modification of this technology helps to secure the data and also many research on this technology are taking place which would eventually help this technology to expand its scope in future leading to more secure data and more advance clouds structure and architectures , thus it will help to grow the IT industry as well as advancement of this technology would help in big organizations as well as full-fill the requirement of public industry as well. As the advancement of cloud computing is taking place from day-to-day, this technology will eventually expand and its scope would certainly increase, leading to expansion of cloud development industry and the research is not stop here much work can be done in future. Our objective is to design a set of unified identity management and privacy protection frameworks across applications or cloud computing services.

8. REFERENCES

[1] F. A. Alvi1; B.S Choudary; N. Jaferry; E.Pathan, “A review on cloud computing security issues & challenges.

[2] Kevin Hamlen; Murat Kantarcioglu; Latifur Khan; Bhavani Thuraisingham,” Security Issues for Cloud Computing”, Volume 4, Issue 2,International Journal of information security and privacy.

[3] V.KRISHNA REDDY1; Dr. L.S.S.REDDY,” Security Architecture of Cloud Computing”, International Journal of EngineeringScienceandTechnology(IJEST).

[4] Deyan Chen; Hong Zhao,” Data Security and Privacy Protection Issues in Cloud Computing” International conference on computer science and engineering, Vol 3 March 2012.

[5] P.Shanthi Bala, ”Intensification of Educational Cloud Computing and Crisis of Data Security In Public Clouds”, International Journal on Computer Science and EngineeringVol.02,No.03,2010,741-745