www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 11 Nov. 2016, Page No. 18843-18847

A Review on Security Challenges and Considerations in Cloud Computing

Riten Shah[1], *Karan Pittie*[2], *Priya G.*[3]

[1]VIT University, School of Computer Science and Engineering,
Vellore, Tamil Nadu – 632014, India
riten.shah2013@vit.ac.in

[2] VIT University, School of Computer Science and Engineering,
Vellore, Tamil Nadu – 632014, India
karan.pittie2013@vit.ac.in

[3] VIT University, School of Computer Science and Engineering,
Vellore, Tamil Nadu – 632014, India
gpriya@vit.ac.in

Abstract: ***This paper focusses on the current security challengers in cloud computing analyzing and providing solutions to the given challenges.***

Keywords: Security, IaaS, PaaS, SaaS

1. Introduction

Cloud Computing is an on demand practice of using servers or network resources as the resources for computation and data processing. It provides access to a pool of resources that can be shared among the computers and the systems in the same network and this requires very little or no management efforts. Cloud computing enables organizations and individuals to process and store their data in cloud thereby enabling them to unlimited access to resources for both storage and computation purposes. Cloud computing majorly works on the principle of sharing of a pool of resources among various systems in a network thereby achieving coherence and economies of scale. Cloud computing enables organizations and companies to spend less time and resources in buying servers and data warehouses and enables them to concentrate more on things like business logic and implementation and the technologies to be used for development. Cloud computing also offers the way to spend less time in managing the resources and helps them in adjusting quickly to the growing demands and needs of the users. It also provides the flexibility to the users as per the usage that is the user will pay only for the amount of the resources that he will be using for his organization which will save a lot of resources which can be utilized elsewhere. There are many kinds of clouds that are available. There is a Public cloud, a Private cloud and a Hybrid cloud. Public clouds are generally available to the public for usage and can be used to enable services like Software as a Service and Data storage available to the public. There are many public clouds that are quite popular, some of them being, Amazon Elastic Compute Cloud (EC2), Sun Cloud, IBM's Blue Cloud, Google App Engine and Windows Azure Platform. These kind of clouds are cheap and inexpensive and are easy to set up and maintain as the major maintenance part is handled by the company whose cloud space you are going to purchase. All the maintenance and management related work with respect to the cloud storage and computation resources will be set up and handled by the third party company and the user will only need to bother about the business logic that needs to be implemented as the part of the computational logic. It's mostly designed as a pay per usage model where the user will pay only for the storage or the computational resources that his company individually will require for to implement the business logic and hence he will be able to save a lot of resources in the process which can be utilized on some other component. The only drawback that can be seen in the public cloud is the part where security comes into the picture. Although, there are many reliable and secure cloud providers available today it is still a concern as the cloud itself is not owned by you hence there is always a chance that the data and the logic implemented in the cloud may be leaked. Private Clouds are clouds that are owned privately by the company / organization and these clouds provide the option of greater flexibility, maintainability, scalability, automation, monitoring and automation. The main motive behind the private cloud is not to provide the customers with a service but to enable the customers to gain the benefits of cloud architecture without having to give up the part of having your own cloud based data center. Private clouds are expensive and typically should not be used by small or medium sized firms. They are generally being implemented or used by companies for whom security is at the top most priority due the data they deal with or due to the logic that is been implemented in the cloud. They are mainly used to have the companies have their own infrastructure that is totally under their own control and they have the sole right to make nay amends to any logic or data that is being there on the cloud. It is used mainly to keep assets within a firewall. The third type of Cloud is the Hybrid Cloud; this is a type of cloud that is mainly used by companies today. It is a mixture of the services offered by the public and the private clouds. In this type of service, the companies maintain an internal private cloud and also own a public cloud space for business logic and data storage that they feel doesn't need to be limited to the people that are a part of the organization. Typically, for an example, a company that is offering Service A, Service B and Service C will initially be hosted on the private cloud and eventually when the need arises for the company to host the service on the public cloud the company will then deploy the service on to the public cloud.

There are many services offered on cloud. A few of the service models include SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service). SaaS or Software as a service model is basically a service that is hosted on cloud is licensed on a subscription basis and is generally located and available centrally. SaaS services are generally accessed by the users using web based platforms or Web Browsers. It is mainly based on a multitenant architecture where in the same services, hardware, version of the software is deployed or given to all the customers based on a particular pricing model. This is used on all the systems in order to support scalability of the software being deployed on the cloud. In some of the cases of SaaS, virtualization is used in place of the multitenancy in order to support scalability of the software, but the exact contribution of multitenancy of the fact that multitenancy is a necessary component in the service model is still a topic of discussion. SaaS services generally offer the customers the independency and the flexibility to personalize and customize the service that the customer is user. This gives the user the independency to change the look and feel of the application as per his requirement which will enhance the user experience overall. There is a common setting initially set by the service provider which is the default setting for all the users initially after which the user has an option of changing the look and feel of the application as per his requirement. SaaS applications also generally the characteristic of being updated regularly typically on a monthly basis. This major characteristic of SaaS is enabled by the factors that support this, a few of them being the fact that the service is centrally located and hence every update on the coed in one machine will automatically reflect on the systems using the application after deployment. In order to have the service being hosted be used widely SaaS application usually provide API's so that other applications can also make use of these API's and integrate the services into their own platform or a service. Due the success if online social networks SaaS provides users the opportunity to work in a group and collaborate on projects and SaaS applications in order to develop something on a larger scale and a more scalable and a better application. PaaS or Platform as a Service is typically a service model that allows the customers to develop code and run the applications on a platform without having to worry about the infrastructure that is indeed underneath required to be implemented and built in order for the code to run. This makes the job of the developers easy as the developers now only have to worry about the business logic without having to case about the underlying logic that defines the infrastructure on which the code is currently being run on. PaaS can be delivered to the customers or the users in two ways, one via the public cloud where in the user can have minimal or no control over the configuration of the service and the other is the private cloud in which the user has full control over the system and the configuration of the service and change the details as per his requirement. There are many types of PaaS schemes that are offered, some of them being, PaaS, which provides deployment capabilities to mobile app designers and developers. Open PaaS allows the users to users and the customers to run the applications and code in an open source environment. There are many technology giants that offer PaaS services, some of them being, heroku, cloudera, oracle etc. IaaS or Infrastructure as a Service is a kind of service that offers the users with a virtual runtime environment like virtual machine or other resources to the subscribers. IaaS offers these resources with the help of the pool of resources that are located centrally on large data centers and these services and resources are allocated on the basis of their demand and the resource is allocated only if the user has demanded for that particular resource to be assigned to that particular subscriber. Due to the current growth of internet and networking technologies, the spread of multimedia and its data is massive via the use of internet. Even though there is a number of digital documents available and there is large availability of the disk processing tools and the international way in which the use of internet has been easier has created a very appropriate medium through which the content that is being delivered in the form of multimedia gets accessed with the unauthorized people and the use and distribution of such data illegally is on the rise. A major issue in this area is to protect the interest and work of scholars in the form of multimedia content and the security and the protection of such information is a pressing matter and is of prime importance. There are a number of information sorts that can be described as media sorts. They are mainly of the following kind, text is one kind of media in which the information can be coded in the form of ASCII values and the other ways of having data in such a sort in by the use of spreadsheets, databases and annotations. Images are the blocks of data containing information in the form of pixel intensity values. Each image is nothing but a composition of pixels and each pixel is identified with the help of its pixel intensity value which identifies how dark or bright a particular point or pixel in an image would appear like. Audio is also a form of multimedia which can take 2Mb of storage space even for a moment of it. Sound is mainly stored in the form of waves which can then be interpreted. Audio, Video and Text are the main ways in which information can be expressed or stored as. There are many disadvantages of representing data as multimedia. A few of them being, the data that is stored in the form of multimedia would be more expensive in real and would occupy more space and the net time or the computational power that will be required to process that amount of data is generally larger than what is required to process a normal data in the form of text.

2. Security Considerations and Mechanisms for the Cloud Service Model

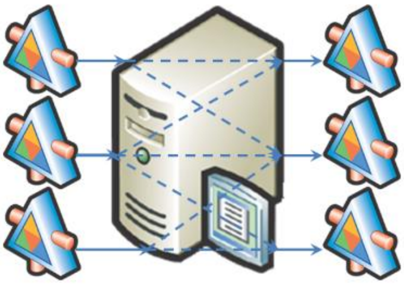
Addressing the three service models in Cloud Computing:
SaaS, PaaS and IaaS.

1. **SaaS (Software as a Service)**
   - SaaS solutions only provides control at the application layer. Where as in the case of a Public Cloud, the vendor has undisputed control on the infrastructure and the platform and thus requires the customer to have trust. Considering the history, one should consider the established processes for security. While evaluating one should check if there is a provision for network security along with data security.
   - Network Security may not be considered as SaaS, but it can be implemented along with application controls. One should realize the security responsibilities. Service Level Agreements define the responsibilities of the vender and customer of cloud.
   - When Cloud vendors offer solutions via app store, there are possibilities of malware intrusion via third party apps,

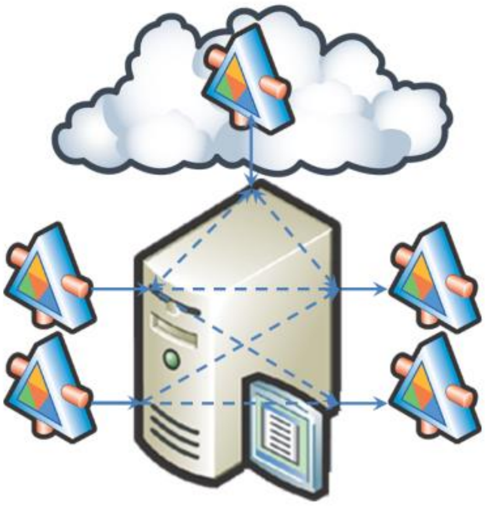
- If one deploys their own SaaS application, they should be aware of the hackers checking their system for vulnerabilities. Common threats like SQL injection are easy to exploit but can also be easily blocked if the security specifications are met.
- A Private Cloud system is less vulnerable to outside threats however the damage maybe caused due to poorly written code and if not properly scrutinized like the internet for data security and network the system can be damaged.
- Even though SaaS is not related to storage, one should ensure the safe transmission of data across the internet. The data should be encrypted to avoid risks on storing sensitive data.
- On the Client side one should take into account browser vulnerabilities, versions and compatibilities to issue required updates quickly. Every version needs to be tested and evaluated before deploying.
- For an example of Architectural Design, Contosa when developing SaaS solutions decided to give every network with equivalent security measures, not without sending any data without encryption. The data is stored on their private servers. When additional usage is required the cloud solutions can handle them. With the cost savings involved and increasing levels of trust, they plan to shift other systems onto a public cloud.

2. **PaaS (Platform as a Service)**

- PaaS model provides a complete environment for developers to run code via deploying it through their service. This method helps in creating a dev environment on the server, enabling the customer to easily connect to PaaS vendor and simple start developing applications and publishing them globally without delay.
- Accessing and authorising users, Distributed Computing, managing data and securing it are some of the important issues for PaaS.
- PaaS must ensure a level of abstraction among its users by enabling authentication and authorization.
- An effective authenticating framework is required for users for proper identification without opening up to possible attacks. Type of attacks found here are like those faced in non-cloud systems, these are Impersonation, Phishing, Password Attacks and Dictionary attacks.
- Two Level of authentication can provide the required security by use of smart cards and biometric techniques but these come at a greater cost of expense and complexity.
- For Distributed Applications,
  - Enterprise Service Bus (ESB) acts as a bridge for the services without the need to program each application individually to other services. Additionally, ESB helps with transformation and providing workflow capabilities.



  - ESB is popular in connecting any Enterprise system to the Private Cloud.
  - Hybrid Models with help of ESB extend the service to Public Clouds.
  - For In House developers creating web applications ESB helps with validating and encrypting the data.
  - This also helps in handling connectivity and security of it to the PaaS allowing message transformation.



- N-Tier Applications having distributed architecture provides a challenge for cloud environment. Considering the example where an n-tier distributed application needs to be migrated to the cloud. Due to Security concerns, the data is kept in Private Cloud and rest of the system is shifted to Public Cloud.
- The Challenges faced in this situation are, Security in terms of authenticating and proving access control with firewalls and cryptography; Synchronicity might be exchanged in favour of asynchronous operations; Managing Performance and Exceptions; Reporting Errors.

3. **IaaS (Infrastructure as a Service)**

- Commonly called Utility Computing, acts as an on demand virtual machine, that can be remotely accessed and in variable capacity, meaning all the required components like infrastructure, networks, storage, hardware and memory are made available by this model.

- Majority of the concerns related to security of IaaS arise as a result of virtualization of its data centres, networks, hardware and pooling of resources.
- Irrespective of deployment model, the security requirements have to get implemented at host level for concerns of memory, storage and network.
- Based on the services offered, the security state of the client system can be controlled by enforcing tools of malware protection like anti-virus and updated security patches.
- Issues of DNS Misdirection, DDOS and prefix hijacking deteriorate the quality of network. Thus continuous monitoring needs to be implemented for mitigating attacks on network availability.
- A System for Cloud storage needs to be designed to create a resource pool, detail abstraction like location and type of storage and its persistence. This allows the data across various tenants stay on same disk with any breach of the system leading to sensitive data exposure to hackers and unintended tenants.
- Access Controls and authentication mechanisms like XACML and SAML help in user identification which leads to mitigating the issue. Implementation of access control mechanism with authentication mechanisms rely on the cloud based platform’s deployment models.
- When a Public cloud offers a delivery model in IaaS, it might use web services via the web portals providing access control along with authentication mechanism.
- Eventing and Reporting is required in private clouds to significantly improve the complexity in the infrastructure to overall computing. For this one needs to have an awareness of the devices, collecting information, determinacies of intelligence data and integrate it.
- With the use of Private cloud, almost everyone works in virtualized setup, and for the development of the hypervisor one should consider if the application should be based out of relative security by various hypervisors.

3. Challenges in Multimedia Cloud Computing

Multimedia and service heterogeneity

We know that there are many services that are offered as multimedia services in the cloud such as Voice over IP (VoIP), sharing of photos and editing them, multimedia streaming, video conferencing, searching for images, video transcending and adaptation, image based rendering and multimedia content delivery, the cloud will be able to support all the different sets of multimedia services that shall be offered to millions of users simultaneously and hence it is important that the services that are being offered should be of scalable in nature and hence it should be easy to deploy the services and make it available to millions of users simultaneously.

Quality of Service Heterogeneity

There are many forms and types of media that need to be deployed on the cloud for the storage and processing and since there are so many types of multimedia it is essential to note that the requirement of the quality of the services being offered will be different for different types of media. We can say that the quality of service that is offered for the display of visual images should be different from the quality of service being offered for the audio content. The cloud should be able to handle all the different requirement and edge cases for each of the specific type of multimedia and make change according to the type of the multimedia that is being stored in the cloud.

Network Heterogeneity

There is no perfect network and all the networks are unique in the sense that each and every network has its own properties and characteristics such as time, jitter bandwidth, delay, speed etc. Hence the cloud should be able to adapt to all these varying demands and should be able to provide content that is tailor made and is suitable for the systems that are connected in that particular network and are able to view to content that is made specifically for them in order for them to have an enhanced user experience.

Device Heterogeneity

As there are different types of devices that are available in the market the applications that are deployed to the cloud or the content that is being stored and viewed in the cloud should be able to adapt the device specific characteristic and should be able to adjust itself in terms of aspect ratio and quality in order for the user to have an enhanced user experience.

Security

As the cloud is usually accessible to anyone and everyone who is a subscriber of the particular service of the cloud it is essential to understand that the data being stored in the cloud is at risk since the data would be accessible to anyone who is viewing the cloud and hence the data needs to store in a way that it is safe and only the people who are authorized to view the data should be able to view or make any changes to it.

Power Consumption

The increase in the number of data centers and the amount of computation power that is required has e dot an increase in the amount computation power that is required in order to process the data and hence the amount of power consumption has increased drastically and hence it’s an important issue that needs to be addressed.

4. Conclusion

According to recent surveys 2.4 billion users are currently using cloud based services and several companies are now migrating from their traditional services to cloud based services. Even big companies like google provide cloud based services like Google App Engine. Other big shots like Microsoft, Google, Apple provide various cloud based storage technologies with different names all using the same base technology of having cloud based storage service. Continuous research and analysis is being carried out by companies today to increase the battery life of handheld devices, their resource availability, their computation power and their displays. Since, CC is so widely being used in today's world it is essential that the various faults, bugs and defects related to CC be addressed with utmost skill so as to solve the problems and have the technology be available globally as a standard. CC will revolutionize the future of handheld devices and will completely change the way in which the handheld devices are currently being used or will typically broaden their usage. In this paper further, we will discuss the various issues that Cloud Computing faces as challenges and we will look at a few ways as suggested by researchers in order to deal with these issues. Securing data and information in CC is more important as CC is being used by many finance based institutions and the data that is typically stored in a financial institution is meant to be kept private and if leaked, may lead to huge losses, be it on an individual level or an organizational level. In this review paper the various issues faced by CC, as analyzed by researchers is going to be presented and analyzed. Since, CC is a trending technology, many companies and services are migrating from their traditional service models to cloud based service models in order to improve their client base. Trending technology often attracts crowd and with crowd, come hackers and exploiters that continue to find bugs in the system and try to exploit them in order to expose the systems vulnerabilities. Hence in this paper we will be looking at a few issues and their solutions as faced by Cloud Computing.

References

[1] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions On Parallel and Distributed Systems, Vol. 22, No. 5, 2011.

[2] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Privacy Preserving Public Auditing for Data Storage Security in, cloud Computing", 2010.

[3] M. Sudha, Dr. Bandaru Rama Krishna Rao, M.Monica, A comprehensive approach to ensure secure data communication in cloud environment‟ International Journal of Computer Application (0975-8887), Volume 12- No 8, Dec 2010.

[4] Palivela Hemant, Nitin.P.Chawande, Avinash Sonule, Hemant Wani,‟ Development of Server in cloud Computing to solve issues related to security and backup‟, in IEEE CCIS 2011.

[5] John Harauz, Lori M. Kaufman and Bruce Potter,"Data security in the world of cloud computing" published by the IEEE computer and reliability societies in July/August 2009.

[6] J.Srinivas, K.Venkata Subba Reddy, Dr.A.Moiz Qyser(2012 july)"Cloud Computing Basics"International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 1, Issue

[7] Jagjit Singh, Er. Gurjit Singh Bhathal "A Review on Storage Security Challenges in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering.

[8] Swati Paliwal, Ravindra Gupta (2013 February)," A Review of Some Popular Encryption Techniques",International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 2, ISSN: 2277 128X.