ijergs
Open Access
International Journal of Engineering Research and Generic Science (IJERGS)
Available Online at www.ijergs.in
Volume 1; Issue 1; Page No. 36-39

A Survey of major Threats in Privacy and Security on Cloud Computing along with some possible solutions

Bhagyashree Shukla[1], Monika Prajapat[2], Susmita Banerjee[3], Vibha Swami[4], Deepti Singh[5], Sunita Rao[6]
monika.prajapat077@gmail.com, banerjeesona58@gmail.com, veena.swami13@gmail.com
MCA Scholar
Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan

Abstract
Cloud computing promises to increase the velocity with which applications are deployed, increase innovation, and lower costs, all while increasing business agility. Sun takes an inclusive view of cloud computing that allows it to support every facet, including the server, storage, network, and visualization technology that drive cloud computing environments to the software that runs in virtual appliances that can be used to assemble applications in minimal time. This survey paper discusses how cloud computing works and what are the major threats to cloud security and privacy. We have also mentioned about some possible solutions to those issue related to cloud.
Key Words: Security, Privacy, Cloud, Computing, Network, Server, Velocity.

1. Introduction

In this modernizing and Technophile world as we know that each and every thing is to made shorthand and easy by applying latest technologies. Day by day new researches are going on in order to increase the pace of development .A very emerging need of IT sector now a day's is *"Cloud"* .Daily life simple hacks to big technology coo pups can easily be accessed as well as managed by this. Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital intensive set up to a variable priced environment. Cloud computing is receiving a great deal of attention, both in publications and among users, from individuals at home to organizations. Cloud computing is a subscription based service where you can obtain networked storage space and computer resources. The cloud makes it possible for you to access your information from anywhere at any time. While a traditional computer setup requires you to be in the same location as your data storage device, the cloud takes away that step. The cloud removes the need for you to be in the same physical location as the hardware that stores your data. Your cloud provider can both own and house the hardware and software necessary to run your home or business applications. One requirement is that you need to have an internet connection in order to access the cloud. This means that if you want to look at a specific document you have housed in the cloud, you must first establish an internet connection either through a wireless or wired internet or a mobile broadband connection. The benefit is that you can access that same document from wherever you are with any device that can access the internet. These devices could be a desktop, laptop, tablet, or phone. This can also help your business to function more smoothly because anyone who can connect to the internet and your cloud can work on documents, access software, and store data.

2. Types of Cloud

There are different types of clouds that you can subscribe to depending on your needs as a home user or small business owner will most likely use public cloud services.

A. Public Cloud: A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space.

B. Private Cloud: A private cloud is established for a specific group or organization and limits access to just that group.

C. Community Cloud: A community cloud is shared among two or more organizations that have similar cloud requirements.

D. Hybrid Cloud: A hybrid cloud is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community.

3. Cloud Service Provider

In order to access online cloud services we must firstly connect ourselves to the internet. There is a person named as CSP or cloud service provider, he is the one who is responsible for services. He provides us services on cloud as per our demand and also charge money for that. When we choose a provider, compare our needs to the cloud services available. Keep in mind that our cloud provider will be pay as we go, meaning that if our technological needs change at any point

Corresponding Author: Vibha Swami

we can purchase more storage space (or less for that matter) from our cloud provider. Cloud Providers offer services that can be grouped into three categories.

A. Software as a Service (SaaS): In this model, a complete application is offered to the customer, as a service on demand. A single instance of the service runs on the cloud & multiple end users are serviced. On the customers side there is no need for upfront investment in servers or software licenses, while for the provider the costs are lowered, since only a single application needs to be hosted & maintained Today SaaS is offered by companies such as Google, Sales force, Microsoft, Zoho, etc.

B. Platform as a Service (Paas):Here, a layer of software, or development environment is encapsulated & offered as a service, upon which other higher levels of service can be built. The customer has the freedom to build his own applications, which run on the provider's infrastructure. To meet manageability and scalability requirements of the applications, PaaS providers offer a predefined combination of OS and application servers, such as LAMP platform (Linux, Apache, MySql and PHP), restricted J2EE,Ruby etc. Google's App Engine, Force.com, etc are some of the popular PaaS examples.

C. Infrastructure as a Service (Iaas): IaaS provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data centre space etc. are pooled and made available to handle workloads. The customer would typically deploy his own software on the infrastructure ,Some common examples are Amazon, Go Grid, 3 Tera, etc.

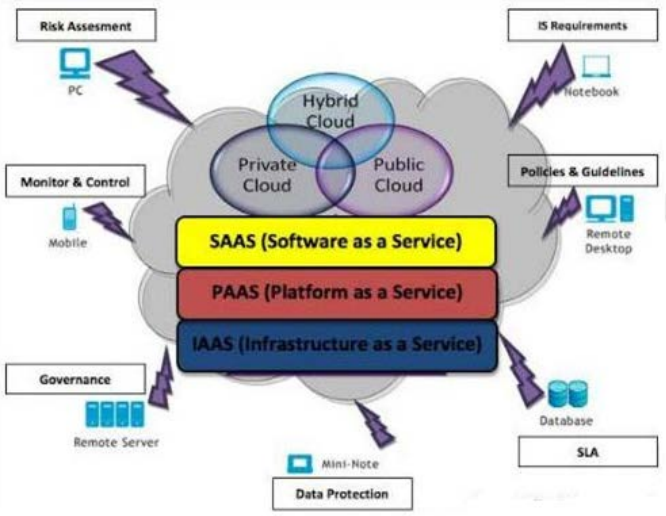

Figure 1: Cloud Computing Map

4. Characteristics of cloud computing:

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 the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

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). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Terms and conditions: Terms between user and company cannot alone protect the privacy and security of the user's information. Security can be breached, infrastructure can be damaged, and a company can become bankrupt, often leaving users without recourse. Furthermore, terms and conditions or service level agreements, may be unfair, as well as illegal in some countries, and can of course easily be broken.

Latency: It is another element that contributes to network speed. The term latency refers to any of several kinds of delays typically incurred in processing of network data. A so-called low latency network connection is one that generally experiences small delay times, while a high latency connection generally suffers from long delays. Although the theoretical peak bandwidth of a network connection is fixed according to the technology used, the actual bandwidth you will obtain varies over time and is affected by high latencies. Excessive latency creates bottlenecks that prevent data from filling the network pipe, thus decreasing effective bandwidth.

Data Segregation and Ownership: The use of shared infrastructure can create data commingling and segregation issues. For this reason, an organization may choose not to move sensitive or confidential information into the cloud. Further, depending on the nature of the information that is being stored or processed, the organization may need to ensure that its data can be segregated from all other third-party data as part of the cloud-service. The ownership of the data by the organization should be confirmed in the contract and the cloud provider should be required to return or destroy the data in its possession at the end of the relationship.

Location of Data: A cloud provider's infrastructure may be located in different jurisdictions which can result in a number of legal issues for the organization. Among other things, if data is transferred to another country it may become subject to the privacy laws of that country. Therefore, the physical location of the servers where the organization's data will be stored should be specified in the agreement with the cloud provider. The contract should also restrict the locations where the data may be held (for example, if the cloud-service is provided from a location in Canada, the contract should prohibit transmission of data outside of Canada without the organization's specific consent).

Data Leakage: A threat from widespread data leakage among at many, potentially competitor organizations, using the same cloud provider could be caused by human error or faulty hardware that will lead to information compromise. **Outside Attacks**: The threat from external attackers may be perceived to apply more to public Internet facing clouds, however all types of cloud delivery models are affected by external attackers, particularly in private clouds where user endpoints can be targeted. Cloud providers with large data stores holding credit card details, personal information and sensitive government or intellectual property, will be subjected to attacks from groups, with significant resources, attempting to retrieve data.

Data Quality: The threat of impact of data quality is increased as cloud providers host many customers' data. The introduction of a faulty or misconfigured component required by another cloud user could potentially impact the integrity of data for other cloud users sharing infrastructure.

Possible solutions available:

In to overcome these issues there are many solutions available as well as many different researches are going on day by day .Some of the popular solution available are as follows:

Cloud watcher is used to provide monitoring services for large and dynamic clouds. The Cloud Watcher automatically detects the network packets which needs be inspected by using the pre-installed network security devices. A simple policy script is used for these operations and thus a cloud network administrator is able to protect his cloud network easily. A cloud operator can monitor the cloud easily and efficiently with Cloud watcher and it provides security monitoring as a service to all its tenants. Cloud watcher provides practical and feasible network security monitoring in a cloud network.

The **FBCrypt** encrypts the inputs and outputs between a VNC client and a user VM using the VMM (Virtual Machine Monitor). The VMM decrypts the inputs encrypted by a VNC client when a user VM reads them. Whenever a user VM updates a frame buffer, the VMM encrypts the updated pixel data, which are decrypted by a VNC client. Thus the sensitive information is located in the middle which is protected against the management VM.

IDM (Identity management) approach is proposed which has the ability to use identity data on untrusted hosts. This approach uses the predicates over encrypted data and multi-party computing for the use of a cloud service. It uses active middle-ware agent that includes privacy policies, a virtual machine that enforces the policies, and has a set of protection mechanisms to protect it. An active agent interacts in the place of a user to authenticate to cloud services using user's privacy policies

A protocol called "***Trust Token***" is proposed which guarantees that the user VM can only be migrated to a cloud platform which is trustable. In the proposed protocol, the cloud user can define the migration policy and the user can later audit the VM migration process which is performed by the cloud provider. The Trust Token used for the migration ensures that the user VM is never migrated to an untrusted platform.

A method called **SVA** (Security Vulnerability Assessment) process is used which is a risk-based and performance-based method which involves five steps such as Apply SVA Tools, Assessment Report, Vulnerability Analysis, Risk Assessment, Counter measures Analysis.

Host Identity Protocol (HIP) is a proposed solution which provides a way to authenticate and protect data flows between tenants belonging to the same security domain. HIP is experimented under different conditions to address the multi-tenancy challenges for public and hybrid IaaS clouds. In this solution, developers and administrators can access cloud services directly over HIP, whereas consumers access the cloud without HIP using a reverse HTTP proxy which also acts as a load balancer for a distributed test service. HIP was used to secure internal connectivity in the clouds and a load balancer terminated HIP tunnels towards end-users.

Live migration defense framework (LMDF) is developed in, which can be used for incorporating security policy within a VM. It is shown that with the LMDF two times more integrity checks can be performed, nearly three times more data can be encrypted and the VM is relocated. The LMDF can estimate the distance between the old and the new location and perform internal adaptations and corresponding actions based on the location fingerprint training.

5. Conclusion

This paper discusses about the emerging issues in cloud as well as provides knowledge about the possible popular solutions to them available. This paper basically focus about the general issues as this paper is just a part of a survey which we have gone through in order to made information available to people. Awareness is the only measure to avoid any type of inconsistency of services. Until and unless we are not alert about the consequences of the the actions we are not able to rectify our own security.

6. References

[1]. Nir Kshetri,Privacy and Security issues in Cloud Computing,PTC'11 Proceedings.

[2]. Jaydip Sen, Security and Privacy issue in Cloud Computing, Innovations Labs TCS Kolkata (India).

[3]. Osama Harfoushi (2013),Data Security issues and challenges in cloud computing:A conceptual analysis ans review,www.scirp.org/journal/cn.

[4]. Vic(J.R.)Winkler (2013),Cloud Computing:Privacy,Confidentiality and the cloud, TechNet magazine

[5]. Kevin Hamle(2010),Security Issues for Cloud Computing, International Journal of Information Security and Privacy 4(2)39-51.

[6].Siddharth Jain, Rakesh Kumar, Saurabh Kumavat, Sunil Kumar(2014),An analysis of security and privacy issues,challenges with possible solutions on Cloud Computing, National Conference on Computational and mathematical Sciences(COMPUTATIA-IV).

[7].S.C.Rachana, Dr.H.S. Guruprasad (2014),Emerging security issues and challenges in Cloud Computing, International Journal of Engineering Science and Innovative Technologies (IJESIT)Vol.3,Issue 2