Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 1, Number 2; November, 2014 pp. 13-17

http://www.krishisanskriti.org/acsit.html

Research Opportunities and Challenges in Cloud Security

Harshit Srivastava

Maharaja Agrasen Institute of Technology 603-Azure Height Supertech 34 Pavilion, Sector 34 Noida
E-mail: harshit.ndl@gmail.com

Abstract: *Cloud Computing is increasingly becoming more and more popular and is surely considered to bring a revolution to the Computer Industry. Many enterprise applications are moving to the Cloud platform and in the future, all the systems and machines will be connected to a cloud server. Cloud Computing has many advantages including availability, reduced cost, flexibility, ubiquitous access among others. However, the only barrier that remains with the Cloud Technology is of Security. Users put their valuable data on to a Cloud and they have to trust the Cloud Service Providers blindly about the safety and security of their data. In this paper, I discuss about the challenges and the issues that are prevalent in Cloud Computing as far as security and privacy is concerned. There are many areas in the current technique of deployment of the Cloud Technology, where security and reliability may prove to be a threat to the authenticity of the Cloud Service Provider. This creates a research opportunity to find the most efficient and secure technique to deploy a cloud. Much research has to be done in this field so as to assure the users that their data will be safe.*

Keywords: *Cloud Computing, Security, Privacy, Issues, Research*

1. INTRODUCTION

Cloud computing has been drawing much attention lately, and is known to be the next big thing in the computer world. Many visionaries vehemently say that Cloud computing will have a greater effect on our lives than the PC revolution and the dot-com revolution combined. The much talked about Cloud Computing, is the delivery of computing as a service and not as a product where shared resources, software and information is being provided as a utility over a network. Cloud computing is implemented with the help of distributed remote hosting servers over the internet, by logging into which we can access the service that the providers had promised to provide us with. The big players in the cloud computing industry are Amazon, Google and of late, IBM and Microsoft. Oracle/Sun and HP are also not far behind. Google has built the largest Cloud Computing infrastructure. Amazon, besides being a huge online shopping site, is also a big mover in cloud computing revolution. With recently gone live Microsoft Azure, Microsoft also entered the Cloud Computing industry. Oracle/Sun, IBM, RackSpace etc. have also tied their future to Cloud Computing.

The main reasons why Cloud Computing is drawing so much attention is because of low cost of services provided. The service is provided on a pay-what-you-use basis. This means that the user will pay only for the services he/she uses and will pay only for the specific time during which he/she used that service. It is very similar to the usage of electricity or heat. The companies that are new to the IT industry find it easy to start if they use a cloud service as there is no need to set up the infrastructure. They just have to login to the Cloud Service and by using any computing device such as laptops, desktops, tablets etc. they can use the services. Cloud providers provide the users with scalability which helps them provision one or more servers depending upon the current usage. This is done generally by Virtualization which will be discussed later in detail. The users get ubiquitous access of cloud services. They can access the services just by giving the login ID. By doing so, they get logged in and can use the services that they paid for. This can be done from anywhere in the world and by using any device that they own.

The only drawback that seems to be present in cloud computing is Security. Security has been a major concern for widespread adoption of cloud services. Users put their valuable data on to a remote server which are placed in unknown parts of the world. How can they be sure that their data is secured? The data they enter might be very confidential and by moving it to the cloud, they are diminishing its confidentiality. And what happens if the server of the Cloud Service Providers powers down due to some unnatural reason? All the data that the user put on the cloud feeling assured that it will be safe (as promised by the provider) will be lost. Another major concern is what happens if the cloud service provider goes out of business? The Users have no option but to trust the Cloud Service Providers totally and unconditionally with the security and reliability of their data.

There have been many instances where the Data Centers of the Cloud Service Providers have slowed down or have stopped working altogether. In June 2012, a big storm in North Virginia affected the Amazon's Data Center. As a result, websites like Netflix, Instagram, Pinterest, and Heroku were

down for few hours because they rely on Amazon's cloud service. A flawed storage software update over Google triggered an unexpected bug In March 2011. Around 150,000 Gmail accounts were affected and all their messages were deleted in the wake of that software bug. All these incidents have been reported to the media but what about unreported incidents? There must have been many such incidents that may have happened over the years but nobody came to know about it.

Cloud Service Providers usually try to cover all these security issues in the Service Level Agreement (SLA). In SLAs they mention that they will do their best effort in guaranteeing that user's data will be safe. They guarantee the users that 3 copies of their data is made and is kept in three different Data Centers. The location of these Data Centers is generally not disclosed. They assure that the Data Centers are secure from any natural calamity and that only a few trusted employees are permitted to enter the premises where the data is actually stored. They also vouch for the fact that they use very strong firewalls, antivirus and other software protection layers. Cloud Service Providers, in the end, tell the users that you are the one who is ultimately responsible to protect and create a backup of your data in case of such emergency.

This creates a big challenge for Cloud Computing Technology as far as security and reliability are concerned. It also creates an opportunity for researchers to find out the possible solutions to the security related issues and make the Cloud Computing Technology a great success.

2. CLOUD COMPUTING OUTLINE

2.1 Definition

Cloud Computing is a complex and evolving paradigm. There is no fixed definition for Cloud Computing. However, the definition of cloud computing as defined by the US National Institute of Standards and Technology (NIST) is "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".

2.2 Service Models

There are 3 basic service models by which Cloud Computing is promoted.

2.2.1 Software as a Service (Saas). The capability provided to the consumer in this highest level is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based e-mail). The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

2.2.2 Platform as a Service (Paas). The capability provided to the consumer in this intermediate level is to deploy onto the cloud infrastructure consumer-created or acquired applications developed using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

2.2.3 Infrastructure as a Service (Iaas). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

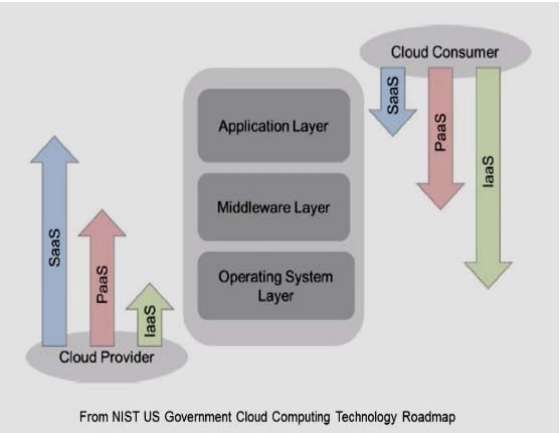

Fig. 1: NIST-Responsibilities between Cloud Consumer and Cloud Provider

2.3 Deployment Models

There are 4 deployment models through which Cloud Computing can be implemented.

2.3.1 Private cloud. The cloud infrastructure is provisioned for exclusive use within a single organization, managed and operated by the organization or a third party regardless whether it exists on or off premise. The owners can control the cloud infrastructure themselves.

2.3.2 Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

2.3.3 Public Cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

2.3.4 Hybrid Cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

2.4 Virtualization

Virtualization is considered as the core topic of Cloud Computing. Without Virtualization, Cloud Computing cannot be possible. With the help of Virtualization, servers are used dynamically depending on the number of users logged on at that very instant. Virtualization is a technology which allows sharing of servers and storage devices with the help of which, maximum utilization is achieved. Virtualization is the act of creating a virtual rather than actual version of something. IBM was a very early proponent of both virtualization and cloud computing. IBM Smart Business cloud solutions support clouds built behind the enterprise firewall, or the IBM cloud. IBM's public cloud offering is still new, while its private cloud offerings are, for the cloud, very mature. The IBM S/ 360-67, supporting up to four processors, was announced in 1965 which was the start of Virtualization.

Virtualization is achieved with the help of hypervisors such as VMware, XEN, KVM, QEMU etc. Hypervisor is the software that allows multiple virtual images to share a single physical machine. It is a layer of software running directly on computer hardware and replacing the operating system, thereby allowing the computer hardware to run multiple guest operating systems concurrently.

3. METHODS TO SECURE CLOUD

Cloud Service Providers usually execute Cloud Security by 3 methodologies.

3.1 Physical Layer

The physical layer of security encompasses many factors.

1. Data Center: This deals with the physical properties of the Data Center. The Walls of the Data Center is thick. There are cameras all around the place and alarms that go off in case of emergency. Employees and security guards are present in the Data Center 24 hours a day.
2. Biometric Scanning: There are methods such as finger-print scan or retina-scan which allows the employees to enter the Data Center. There are usually very few people that are allowed physical entry inside the area where the Data is actually stored.
3. Building: The buildings are generally designed to be a Data Center from the start. They are built in a way so that they can withstand hurricanes, tornado, earthquakes and other natural disasters.

3.2 Logical Layer

Logical Layer of security deals with the design of the network that is used for providing Cloud Services. The network is kept secure with the help of firewalls, anti-virus and intrusion detection systems. Big companies that provide Cloud Services do not compromise with the quality of the software used. The hypervisors are generally of high standards and the whole system works on Linux based operating system. These systems are centrally managed and protected.

3.3 Methodology Layer

This concerns with the security method used at local level in a Cloud Service Provider and it may differ from one organization to another. The main concept of this layer is to assure that various other aspects of security is taken care of. The password that every employee has is made to be very secure and difficult to crack as opposed to some preposterous passwords like "1234" which do not really help in making the system secure. The environment inside a Data Center is generally very secure and only a few trusted staff members are allowed to make significant changes in the system. Another very important aspect that helps in securing the Cloud is no outsourcing. The companies usually try to give the tasks to only a few trusted staff members who are full time employees at their company and the concept of outsourcing is not very prevalent in Cloud Computing Industry.

4. SECURITY ISSUES AND CHALLENGES

Cloud Service Providers assure that the data kept with them is secure. They also come up with schemes that if some data is lost, they will reimburse the amount that the data was worth. Usually it is 1$ for 1GB. All this however, does not guarantee that the data will remain safe with the Cloud Service Providers. There may be some issues that are out of their hand such as a natural calamity or a power outage. Software bugs, media attack and attack from outside or inside world is also possible and can ruin an organization. The servers generally cannot be hacked because of the high level firewalls used but there may be instances where the hackers might get a chance

to mess around with the system. Lack of administration is another aspect that can create security related issues. Generally Cloud Service Providers lack in providing transparency in their Infrastructure. As a result, the users do not trust the Cloud Providers very much and do not provide them with valuable and confidential data. There are basically 4 major issues related to Security and Reliability in Cloud Computing.

4.1 Legal Issues

Few security related concerns generally deal with the legal and compliance requirements. Users are not aware of where their data is being stored. This sort of puts them in a perturbing situation as they do not know the jurisdiction of the Data Centers where their data is being stored. Most Cloud Service Providers create replicas of the data and put them in 3 different Data Centers around the world. As the users do not know about the location of the Data Centers, they cannot be sure about the laws of that country and will always be concerned about whether the Data Center is built on legal grounds or not. If not, the Data Center will have to be demolished and the user's data might be lost. Another question that arises in this situation is about the regulations and whether or not the Cloud Service Providers are following that. For this, there are many certifications and standards but the cloud technology is evolving too fast and no one can be sure whether the legal and compliance requirements keep up with it and hence, the certifications cannot solely prove that a specific Cloud Service Provider complies with all the regulations.

4.2 Logical Issues

As the cloud technology depends upon various other technologies and all of them are put together to implement a Cloud, the surface area of an attack increases. The probability that one of them will fail is very high and this reduces the reliability of the Cloud Technology. The sharing of resources or co-residence with other users is unique to Cloud Computing and one may end up using the same machines as their competitors. Co-residence may lead to cross-Virtual Machine information leakage. The attacker may map the cloud infrastructure and identify where the target Virtual Machine is likely to reside. After several attempts they may be able to instantiate new Virtual Machines to be co-resident with the target and that can leak to all kinds of information leakage which is known as Side Channel attack. This is because the same resources will be used with the target and the attacker can find out the information that should remain secret from the competitor application such as memory, disk, network-interface, CPU Load, CPU cache usage etc.

4.3 Methodological Issues

Methodological issues generally deal with access of the employees. There should be proper levels of authentication and no unauthorized access must be given. Synchronizing enterprise and external cloud services access control lists in the context of prevention of unauthorized access to ensure right access roles is a very important challenging issue as PaaS and SaaS platforms have complex hierarchies and many fine-grained access capabilities (tenant org level, sub-tenant, and individual user levels). This assumes importance as users, who are no longer part of an enterprise, may still potentially exploit access provided in cloud; unless those credentials are revoked quickly. Cloud computing provides access to data, but the challenge is to ensure that only authorized entities can gain access to it. When we use cloud environments, we rely on third parties to make decisions about our data and platforms in ways never seen before in computing. It's critical to have appropriate mechanisms to prevent cloud providers from using customers' data in a way that hasn't been agreed upon. It seems unlikely that any technical means could completely prevent cloud providers from abusing customer data in all cases, so we need a combination of technical and nontechnical means to achieve this.

5. CLOUD AUDITOR

In addition to the entities such as Cloud Consumer, Cloud Provider and Cloud Broker, which have been discussed earlier, there is another entity call Cloud Auditor. This entity completes the Diagram involving all the actors involved in Cloud Technology. The Cloud Auditor entity is very important as far as the security and reliability of a Cloud is concerned. It is an independent and external entity which performs check on the security level of the cloud. It checks how the cloud operates and what sort of protection is used along with the redundancies it implies.

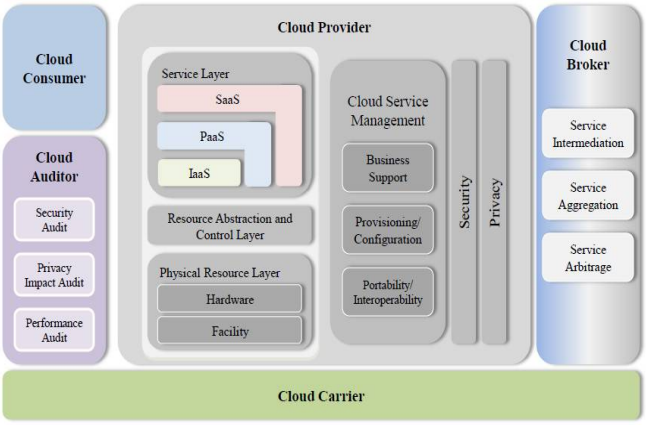

Fig. 2: NIST-View of Cloud Computing Actors

6. CONCLUSION

Cloud computing has potential to have far-reaching effects on the systems and networks of state agencies and other organizations. Many websites are connected to the Cloud

Servers and rely on them completely. With such reliability on one Technology, it is necessary to keep it completely secure and reliable. Also, due to its growing popularity and widespread acceptance, it has become a hotspot for attacks. Attackers are finding ways to find glitches in the technology and come up with a way to leak the information to other competitors. So, as the Cloud Computing Technology is growing, the system needs to be completely secure so that future users do not encounter any errors or setbacks. Even a small malfunction in the Cloud Environment can affect a million users.

This paper gives a brief idea of what Cloud Computing really is and why is it a hot-topic in today's computer world. The various deployment and service models are explained in detail. Then, the paper contains matter about the security issue that is prevalent in the Cloud Technology. Many methods are used by the Cloud Service Providers which ensure the users that their data is kept secured. This is usually done in 3 layers namely, Physical, Logical and Methodology layer. All these layers deal with a different aspect of security in the Cloud Technology. Then, the paper describes the numerous security issues that are present in Cloud Computing. These include Legal issues, which deal with the legal verification of the Data Centers. Then there are the Logical Issues which deals with the firewalls, anti-virus and most importantly, the Virtual Machines used to deploy a cloud. The Cloud Technology is dependent upon so many technologies that it becomes vulnerable and proves to be a large surface for attackers. And then there are the methodological issues which concern with the Authentication, Authorization and Access Control (AAA). Also, a short description of Cloud Auditor is given which plays a vital role in the Cloud Technology. It is an independent entity which performs checks on security and reliability of the Cloud.

With Cloud Computing moving towards being a major part of everyone's life and offering great opportunities to the small businesses, the only challenge that prevails is of Security. A user is asked to offer the Cloud Service Provider with confidential data which then resides with the Cloud Service Provider. This turns attention of the consumers on the Security and Reliability of the Cloud Technology. As seen in this paper, there are many concerns and issues with security deployed in the Cloud Technology and this creates an opportunity for researchers to find a perfect solution. Therefore, there is tremendous research opportunities to deploy a more fool-proof and less vulnerable system to minimize Security risks in Cloud Computing.

REFERENCES

[1] David E.Y. Sarna "Implementing and Developing Cloud Computing Applications", CRC Press, 2011

[2] Timothy Prickett Morgan "Amazon cloud knocked out by violent storms in Virginia", http://www.theregister.co.uk/2012/06/30/amazon_cloud_storm_outage/, 30th June 2012

[3] Paul Mah, "The big gmail crash and the lesson for email administrators", http://www.theemailadmin.com/2011/03/the-big-gmail-crash-and-the-lesson-for-email-administrators, March 4 2011

[4] Wikipedia Staff "Cloud Computing", http://en.wikipedia.org/wiki/Cloud_computing

[5] Saleem Ullah Lar, Xiaofeng Liao and Syed Ali Abbas, "Cloud Computing Privacy & Security", 2011 6th International ICST Conference on Communications and Networking in China

[6] Shubhashis Sengupta, Vikrant Kaulgud and Vibhu Saujanya Sharma, "Cloud Computing Security - Trends and Research Directions", 2011 IEEE World Congress on Services

[7] Wayne A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing", Proceedings of the 44th Hawaii International Conference on System Sciences – 2011

[8] Xiaoqi Ma, "Security Concerns in Cloud Computing", 2012 Fourth International Conference on Computational and Information Sciences

[9] Pengfei You, Yuxing Peng, Weidong Liu and Shoufu Xue, "Security Issues and Solutions in Cloud Computing", 2012 32nd International Conference on Distributed Computing Systems Workshops

[10] Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing", Special Publication 800-145, September 2011.