A STUDY ON SECURITY ISSUES, VULNERABILITY AND THREATS CHALLENGES

Rishi Kumar Sharma[1] Vishal Vig[2]
[1,2]Department of Computer Science & Engineering and information Technology
Quantum Global Campus, Roorkee, India

Abstract
Cloud computing emerges as a new computing paradigm[1] which aims to provide most reliable and QoS guaranteed computing environments for the end-users. Cloud Computing enables us to access and share the subsequent services, resources, servers and application without eventually obtaining them. Cloud Computing is emerging exponentially all over the globe because of its adaptability, which in term is very efficient and effective. In other word cloud computing is a holistic approach to the success of the futuristic Computer Science and Engineering. Though many companies are providing the cloud based services for its client still there arose various issues which are related to the vulnerability and threats of Cloud Computing. These threats and vulnerability may be from the internal or the external sources and consists of factors such as Secure Data Transmission, Insecure API, Internet Dependency and Data Confidentiality. There are also some research confront in cloud computing which includes privacy, interoperability, reliability and service level agreement. This research paper includes study of cloud computing its services models, security and vulnerability issues and also suggests a best practice to cloud service proved to improve technology.

Keywords: **Cloud Computing, Clouds Vulnerability, Security Concerns, Cloud Solutions**.

I. INTRODUCTION

Cloud: as the name suggests is the wide open area which has no boundaries. It is emerging as the latest technology in the digital information technology world, which in terms providing the wide range of application and services to the clients. A cloud is virtual pool of Computer Resources, which can provide the various services to user facing applications and also providing support for the virtual and physical machines.

II. DEFINATION OF COLUD COMPUTING

According to the National Institute of Standards and Technology (NIST), Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction2.

When a Cloud is made available in a pay-as-you-go manner to the general public, we call it a Public Cloud; the service being sold is Utility Computing. As discussed in the later section about the Private Cloud, which refer to internal data centers of a business or other organization, is not made available for the general public. Cloud computing is empowered by virtualization technology; a technology that actually dates back to 1967, but for decades was available only on mainframe systems. In its quintessence, a host computer runs an application known as a hypervisor; this creates one or more virtual machines, which simulate physical computers so faithfully, that the simulations can run any software, from operating systems, to end-user applications.

DIFFERENCE BETWEEN CLOUD COMPUTING AND GRID COMPUTING

Cloud is basically an extension to the object-oriented programming concept of abstraction. Here cloud means the Internet. Cloud Computing provides the services in both the domains as the internet and the hardware and as the systems software in the datacenter that provide those services.

Grid systems as the name suggests is the collaborative sharing of resources. It can also be thought of as distributed and large-scale cluster computing. A Grid is basically the one that uses the processing capabilities of different computing units for processing a single task.3

III SERVICE MODELS OF CLOUD COMPUTING

We identify three categories of cloud computing services4: Infrastructure-as-a Service (IaaS), that is, raw infrastructure and associated middleware, Platform as-a-Service (PaaS), that is, APls for developing applications on an abstract platform, and Software-as-a-Service (SaaS), that is, support for running software services remotely.

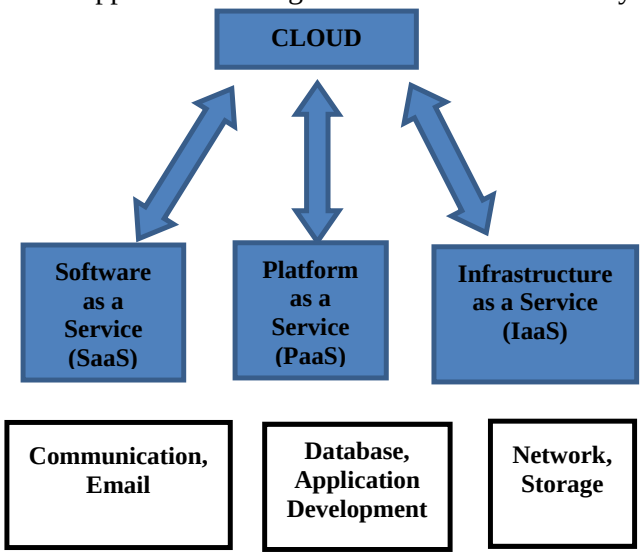

Fig1:Services of Cloud Computing [5]

Software-As-A-Service (Saas) [6]

It was found that SaaS could provide many benefits which are related to the outsourcing of the local control, installation and development of There are numerous SaaS vendors (formerly known as application service providers). They run a single application in a data center, and deliver the functionality via the Internet to the users. Enterprise SaaS vendors include salesforce.com, Oracle/Siebel, Workday, Citrix, and numerous others. SaaS desktop applications for end users include Google Apps, Zoho Office, Microsoft Windows Live, etc. Google Apps include Gmail, Google Talk, Google Calendar, Google Docs (documents, spreadsheets, presentations, and collaboration), etc. Microsoft Windows.

There are also many challenges that need to be addressed including ensuring the quality, privacy, security and business continuity which require the implementation of organizational changes and governance mechanisms for public sector organizations that are considering SaaS.

SaaS Benefits, No software expertise necessary Focus on core business, No need for human resource management of IT staff.

SaaS Disadvantages and Risks Need for contractual expertise, Reliability and long term sustainability of SaaS providers, Lack of technical expertise and experience, Difficulty to switch from provider, less customization opportunities, Integration of software from various SaaS

Providers, Lack of innovation and no grip on further

development and standardization.software which could result in potential cost-savings and better cost control.

Platform as a Service (PaaS)7

This is the idea that someone can provide the hardware (as in IaaS) plus a certain amount of application software - such as integration into a common set of programming functions or databases as a foundation upon which you can build your application. Platform as a Service (PaaS) is an application development and deployment platform delivered as a service to developers over the Web. It facilitates development and deployment of applications without the cost and complexity of buying and managing the underlying infrastructure, providing all of the facilities required to support the complete life cycle of building and delivering web applications and services entirely available from the Internet. This platform consists of infrastructure software, and typically includes a database, middleware and development tools.

Infrastructure-as-a-Service (IaaS)8

Infrastructure-as-a-Service is a delivery of a computer infrastructure as a service. The advantage of IaaS is that it is usage based

payment scheme. It uses the fastest delivery services as it uses the latest technology. The Infrastructure as a Service is a provision model in which an organization outsourcers the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.

Infrastructure-as-a-Service: like Amazon Web Services provides virtual server instances with unique IP addresses and blocks of storage on demand. Customers use the provider's application program interface (API) to start, stop, access and configure their virtual servers and storage. Infrastructure as a Service is sometimes referred to as Hardware as a Service (HaaS).

IV DEPLOYMENT MODELS OF CLOUD COMPUTING

There are also four6 different cloud deployment models namely Private cloud, Public cloud, Hybrid cloud and Community cloud. Details about the models are given below.

Private Cloud: Private cloud1 can be owned or leased and managed by the organization or a third party and exist at on-premises or off-premises. It is more expensive and secure when compared to public cloud. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security, since user's access and the networks used are restricted. One of the best examples of a private cloud is Eucalyptus Systems

Public Cloud: The cloud infrastructure is provided to many customers and is managed by third party. Multiple enterprises can work on the infrastructure provided, at the same time and users can dynamically provision resources. These clouds are fully hosted and managed by the cloud provider and fully responsibilities of installation, management, provisioning, and maintenance.

It is typically based on a pay-per-use model, which similar to a prepaid mobile pay–as-you-go system which is flexible enough to cater for spikes in demand for cloud optimization In this model, no access restrictions can be applied and no authorization and authentication techniques can be used.

Hybrid Cloud: Hybrid cloud is a private cloud linked to one or more external cloud services, which are centrally managed, provisioned as a single unit, and circumscribed by a secure network without affecting each other.

In this model, a company can outline the goals and needs of services. A well-constructed hybrid cloud can be useful for providing secure services such as receiving customer payments, as well as those that are secondary to the business, such as employee payroll processing. The major drawback to the hybrid cloud is the difficulty in effectively creating and governing such a solution. Services from different sources must be obtained and provisioned as if they originated from a single location, and interactions between private and public components can make the implementation even more complicated. These can be private, community or public clouds which are linked by a proprietary or standard technology that provides portability of data and applications among the composing clouds. An example of a Hybrid Cloud includes Amazon Web Services (AWS).

V BASIC PROBLEMS FOR CLOUD COMPUTING SET UP

Cloud computing contains lots of basic problems, which needs to be rectified in order to provide the efficient services for the same. Some of the main problems are 9

- Availability of Service
- Data Confidentiality
- Data Transfer Bottlenecks
- Removing Bugs
- Unpredictability in Performance
- Software Licensing

Availability of Service: Cloud data Can be very large (e.g. text-based or scientific applications), unstructured or semi-structured. To store such a huge data there is a need for the space where a very large data can be accumulated. Hence multiple cloud providers may be used to provide the support.

Data Confidentiality: While arranging space for such a large data, as there is a need for the multiple clouds then at the same time it is very

important to make sure confidentiality of the data and to make sure this will retain by deploying the encryption techniques and firewalls.

Data Transfer Bottlenecks: As mentions in the above two issues where we are using the multiple clouds and this in the transportation of data may leads to data lost, so it is indeed very essential to backup or achieve the data to sought out from any discrepancies.

Removing Bugs: To remove the bugs/errors from the system we need a debugger which can initiate the process to debug the errors from the systems.

Unpredictability in Performance: It is always uncertain to predict the performance but we can manage it by monitoring the above said factors viz space constraint, data confidentiality, data transfer bottleneck, removing bugs.

Software Licensing: There must be a pay-for-use licenses for all the concerned. For unauthorized users access must not be granted.

VI SECURITY ISSUES IN CLOUD COMPUTING

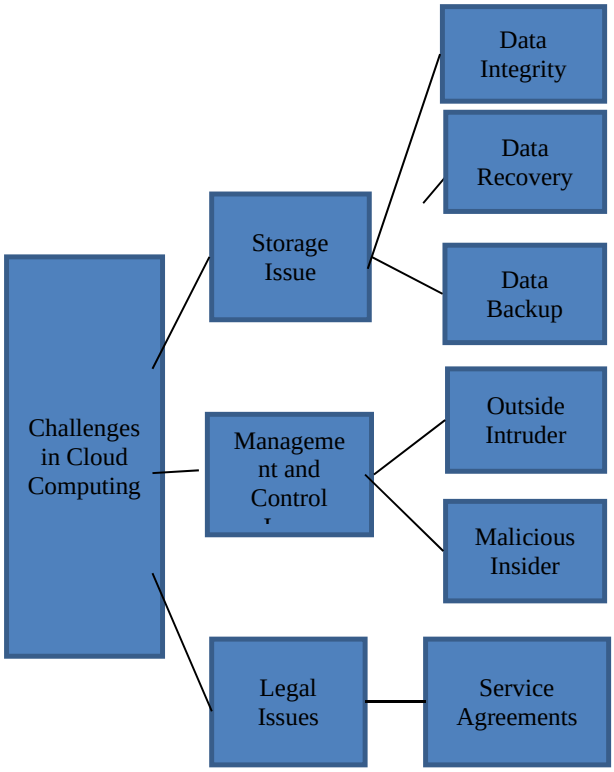

Fig 2. Challenges in Cloud Computing11

Data Issues:
Data Integrity: The main issues concerned to the data are the data integrity. Because of the nature of the simplicity of cloud computing there are increase in the number of users and thus the hosting of the data applications are very high. These situations lead to greater security threats to cloud clients. If any attack is successful on data entity will leads to data breach and takes an unauthorized access to data of all cloud users.

Data Recovery: As the number of cloud implemented in order to increase the data storage, hence we need a good data recovery system else the data recovery vulnerability can pose major threats to the sensitive user data

Data Backup: The data backup is an important when accidental and/or intentional disasters. The CSP has to perform regular backups of stored to ensure the data availability. In fact, the backup data should be keeping with security guidelines to prevent malicious activities such as tampering and unauthorized access.

Management and Control Issues: It is important to maintain track record for user identity for avoiding unauthorized access to the stored data. The identity and access controls are complex in cloud computing because of that data owner and stored data are at different executive platforms. The cloud resources are dynamic and are elastic for cloud user and IP addresses are continuously changed when services are started or restarted in pay per usage model. That allows the cloud users to join and leave feature to cloud resources when they required i.e., on-demand access policy. All these features need efficient and effective access control and identity management.

Outside Intruder: Attacks that come from external origins are called outsider attacks. Data security is one of the important issue in cloud computing. Since service providers does not have permission for access to the physical security system of data centers. But they must depend on the infrastructure provider to get full data security.

Malicious Inside: An insider threat can be posed by employees, contractors and /or third party business partners of an organization. In cloud environment i.e., at Cloud Service Provider (CSP) side attacks leads to loss of user's

information integrity, confidentiality, and security. This leads to information loss or breaches at both environments.

Legal Issues: There are many issues in geographic jurisdictions, regulatory law, performance assurance, contract enforcements, etc. The above mentioned issues are comes under the legalities, Service Level Agreements and data location in data centers.

Service Agreements: It specifies set of terms and conditions among user and Cloud service provider (CSP). The SLA should specify the following:

Actions that CSP will take when data breach happened, remedial actions and
Performance level at minimum level.

VII VULNERABILITIES IN CLOUD COMPUTING

As the cloud computing is a modern way to access and use computing resources over the Internet, so it inherits some security risks and vulnerability from the conventional Internet, such as data confidentiality, integrity, and availability, and etc. Moreover, cloud computing has brought new concerns have to be considered such as moving and storing in the cloud with probability to reside in other country, which has different regulations. This section highlights security-related issues that are believed to have long-term significance for cloud computing.

Vulnerabilities	Description
Insecure Interfaces and APIs	Improper and Insufficient input-data validation.
	Insufficient authorization checks.
Unlimited Allocation of Resources	Inaccurate modeling of resource usage can lead to overhead.
Data-related vulnerabilities	Data may be under the different jurisdictions which have different laws and thus is difficult to handle.
	Data cannot be completely removed leads to incomplete data deletion.
	Data backup done by untrusted third-party providers.
Vulnerabilities in Virtual Machines	Unrestricted allocation and de-allocation of resources with VMs.
	Uncontrolled Migration of VMs from one server to another due to fault tolerance, load balance, or hardware maintenance.
	Uncontrolled snapshots – VMs can be copied in order to provide flexibility but it may lead to data leakage.
	Uncontrolled rollback could lead to reset vulnerabilities - VMs can be backed up to a previous state for restoration, but patches applied after the previous state disappears.
Vulnerabilities in Virtual Networks	Sharing of virtual bridges by several virtual machines.

Table 1. Vulnerabilities in Cloud Computing10

VIII. CONCLUSION

Cloud computing cater the need of both academic and industry fields and therefore it is considered a backbone of future generations. Cloud computing is emerging as a new trend which has revolutionize the way we use the Internet. Cloud computing also helps us to reduce lots of cost and physical space by increasing economic efficiencies but at the same time it is causing a threat for which there is need be cautious about.

From the study, we came to know about cloud computing threats and vulnerability issues, which if not, be rectified or watched upon may lead to data lost so the a reliable access control system is a crucial requirement to secure clouds from unauthorized access. Access control systems in cloud computing can be more complex and sophisticated due to dynamic resources, heterogeneity and diversity of service.

IX REFERENCES

[1] F. Shahzad,"State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions" [online] available at http://www.sciencedirect.com/science/article /pii/S1877050914010187

[2] P Mall, T Grance,"The NIST definition of cloud computing,"

[3] M. Armbrust, A. Fox ,"A View of Cloud Computing."

[4] R. P Padhy, M.R. Patra,S. C. Satapathy, "Cloud Computing: Securities Issues and Research Challenges."

[5] Rinira Technologies, "Cloud Computing" [online] available http://www. rinira.com/ services/cloud _computing.

[6] Kuyoro S. O., Ibikunle F. and Awodele O., "Cloud Computing Security Issues and Challenges

[7] P. Arora, R. C. Wadhawan, S. P. Ahuja, "Cloud Computing Security Issues in Infrastructure as a Service" [online] available https://pdfs.Semanticscholar.org/413d/ 636ff409b268a1420bcab27d22e3969cb576.pdf.

[8] S. Bhardwaj, L. Jain, S. Jain," Cloud Computing: A Study of Infrastructure as a Service (IAAS)"

[9] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. K. G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, M Zaharia," Above the Clouds: A Berkeley View of Cloud Computing."

[10] D. Nagpal, Dr. D. Sharma, "Survey On Threats Attacks And Implementation Of Security In Cloud Infrastructure"

[11] N. Vurukonda, B.T. Rao," A Study on Data Storage Security Issues in Cloud Computing" [online] available http://www.sciencedirect.com/science/article/pii /S18770509 16315812".