Security as a Challenge in Cloud Computing: A Survey

P.Selvigrija, Assistant Professor, Department of Computer Science & Engineering., Christ College of Engineering &Tech., Pondicherry

D.Sumithra , M.Tech. II Year,Department of Computer Science & Engineering., Christ College of Engineering &Tech., Pondicherry

ABSTRACT

Could computing is defined as management and provision of resources, applications, software and information as the services over internet on cloud. However, cloud computing is raised from the IT technicians desire to add another layer of separation in processing information. The ability to provide users dynamically shared resources, scalable over the Internet and avoid large upfront fixed costs, cloud computing has recently emerged. Cloud computing is one of the most significant shifts in information technology many of us are likely to see in our lifetimes. Reaching the point where computing functions as a utility has great promising innovations we cannot yet imagine. On the other hand the security risks and issues are growing more now-a-days. In this paper we explain the cloud computing along with its advantages in brief and emphasize on various security threats in cloud computing also the methods to control them along with their pros and cons.

I. INTRODUCTION

Cloud computing is the collection of virtualized and scalable resources and IT services that use advanced computational power and improved storage capabilities. Services are provided to the users with the" pay only for use" strategy where the users pay only for the number of service units they consume. The business software solutions and data are stored on servers at a remote location. Cloud computing eliminates the costs and complexity of buying, configuring and managing the hardware and software's which is needed to build and deploy applications these applications are delivered as a service over the cloud. To perform the computing needs of users, the cloud computing uses the web services as third party service. The cloud services are broadly categorized into three stages: In the Application layer, the Software as a Service (SaaS) delivers software's over the Internet which avoids the problem of software installation by the customers. This model provides the complete service and application to the customers. The Platform layer provides cloud Platform as a Services (PaaS)

consumes cloud infrastructure by retaining cloud applications.

II. CLOUD COMPUTING OVERVIEW

1. Definitions

What is Cloud Computing?

Cloud computing is a way of leveraging the Internet to consume software or other IT services on demand. Users share processing power, storage space, bandwidth, memory, and software. With cloud computing, the resources are shared and so are the costs. Users can pay as they go and only use what they need at any given time, keeping cost to the user down. Cloud computing is very much a business model as well. Providers of cloud computing solutions, whether they are software, hardware, platform, or storage providers, deliver their offerings over the Internet. There are no shrink wrapped boxes containing discs or hardware for you to buy and set up yourself.

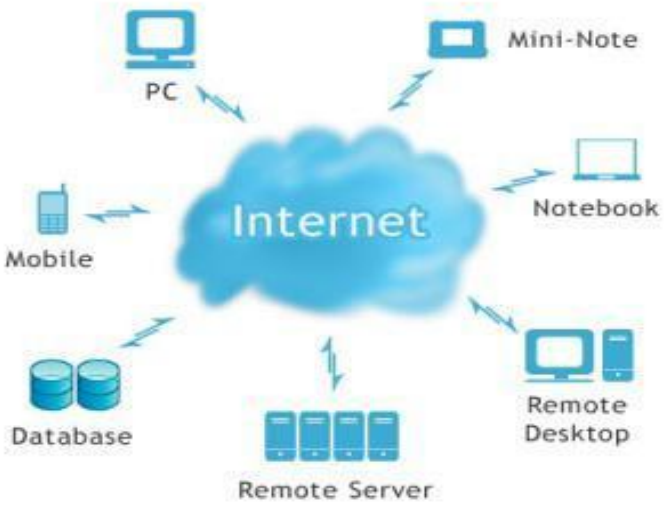

Figure 1: Cloud Computing

2. Cloud Service Models

a) Software-as-a-Service (SaaS). The SaaS service model offers the services as applications to the consumer, using standardized interfaces. The services run on top of a cloud infrastructure, which is invisible for the consumer. The cloud provider is responsible for the management the application, operating systems and underlying infrastructure. The consumer can only control some of the user-specific application configuration settings. Example:

Yahoo!, Gmail, Google Diocs, etc.

b) Platform-as-a-Service (PaaS). The PaaS service model offers the services as operation and development platforms to the consumer. The consumer can use the platform to develop and run his own applications, supported by a cloud-based infrastructure. "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". Example: Google Aps, SQL Azure, etc.

c) Infrastructure-as-a-Service (IaaS). The IaaS service model is the lowest service model in the technology stack, offering infrastructure resources as a service, such as raw data storage, processing power and network capacity. The consumer can the use IaaS based service offerings to deploy his own operating systems and applications, offering a wider variety of deployment possibilities for a consumer than the PaaS and SaaS models. "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)". Example: Amazon (S3, EC2), Windows Azure, etc.

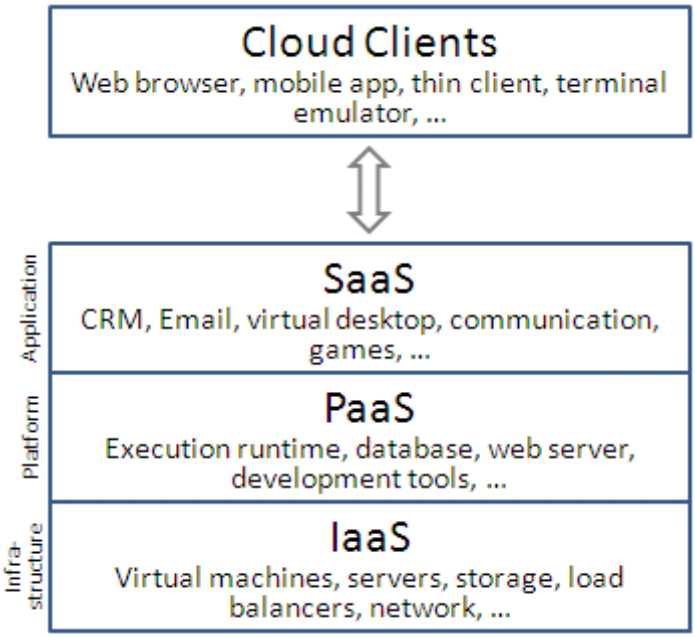

Figure2: Layers of cloud computing

3. Cloud Deployment Models

Regardless of which delivery model is utilized, cloud offerings can be deployed in four primary ways, each with their own characteristics. The characteristics to describe the deployment models are; (i) who owns the infrastructure; (ii) who manages the infrastructure; (iii) where is the infrastructure located; (iv) and who accesses the cloud services.

a. Public Clouds

Public cloud computing is based on massive scale offerings to the general public. The infrastructure is located on the premises of the provider, who also owns and manages the cloud infrastructure. Public cloud users are considered to be Untrusted, which means they are not tied to the organization as employees and that the user has no contractual agreements with the provider.

b. Private clouds

Private clouds run in service of a single organization, where resources are not shared by other entities. "The physical infrastructure may be owned by and/or physically located in the organization's data centers (on-premise) or that of a designated service provider (off-premise) with an extension of management and security control planes controlled by the organization or designated service provider respectively". Private cloud users are considered as trusted by the organization, in which they are either employees, or have contractual agreements with the organization.

c. Community clouds

Community clouds run in service of a community of organizations, having the same deployment characteristics as private clouds. Community users are also considered as trusted by the organizations that are part of the community.

d. Hybrid clouds

Hybrid clouds are a combination of public, private, and community clouds. Hybrid clouds leverage the capabilities of each cloud deployment model. Each part of a hybrid cloud is connected to the other by a gateway, controlling the applications and data that flow from each part to the other. Where private and community clouds are managed, owned, and located on either organization or third party provider side per characteristic, hybrid clouds have these characteristics on both organization and third party provider side. The users of hybrid clouds can be considered as trusted and untrusted. Untrusted users are prevented to access the resources of the private and community parts of the hybrid cloud.

III. FEASIBILITY OF CLOUD COMPUTING

1. Advantages of Cloud Computing [4]:

The following are some of the major advantages of cloud computing:

1. **Virtualization.** Virtualization is defined as decoupling and separation of the business service from the infrastructure needed to run it.

2. **Flexibility to choose vendor.**
3. **Elasticity.** Elastic nature of the infrastructure allows rapidly allocating and de-allocating massively scalable resources to business services on a demand basis.
4. **Cost Reduction.** Reduced costs due to operational efficiencies, and more rapid deployment of new business services.

2. Obstacles and opportunities of cloud computing

3.2. The following table shows the top ten obstacles and opportunities of cloud computing.

NO	Obstacles	Opportunities
1	Availability/Business Continuity	Use Multiple Cloud Providers
2	Data Lock-In	Standardize APIs, Compatible SW to enable Surge or Hybrid Cloud Computing
3	Data Confidentiality and Auditability	Deploy Encryption, VLANs, Firewalls
4	Data Transfer Bottlenecks	FedExing Disks, Higher BW switches
5	Performance Unpredictability	Improved VM support, Flash Memory, Gang Schedule VMs.
6	Scalable Storage	Invent Scalable Store
7	Bugs in Large Distributed Systems	Invent Debugger that relies on distributed VMs
8	Scaling Quickly	Invent Auto-Scalar that relies on ML, Snapshots for Conservation
9	Reputation Fate Sharing	Offer reputation-guarding services like those for email
10	Software Licensing	Pay-for-use licenses

3. Cloud Computing Security Threats

3.1. Top Seven Security Threats

Top seven security threats to cloud computing discovered by “Cloud Security Alliance” (CSA) are [6]:

1. **Abuse and Nefarious Use of Cloud Computing.** Abuse and nefarious use of cloud computing is the top threat identified by the CSA. A simple example of this is the use of botnets to spread spam and malware. Attackers can infiltrate a public cloud, for example, and find a way to upload malware to thousands of computers and use the power of the cloud infrastructure to attack other machines.
2. **Insecure Application Programming Interfaces.** As software interfaces or APIs are what customers use to interact with cloud services, those must have extremely secure authentication, access control, encryption and activity monitoring mechanisms - especially when third parties start to build on them.
3. **Malicious Insiders.** The malicious insider threat is one that gains in importance as many providers still don't reveal how they hire people, how they grant them access to assets or how they monitor them. Transparency is, in this case, vital to a secure cloud offering, along with compliance reporting and breach notification.
4. **Shared Technology Vulnerabilities.** Sharing infrastructure is a way of life for IaaS providers. Unfortunately, the components on which this infrastructure is based were not designed for that. To ensure that customers don't thread on each other's "territory", monitoring and strong compartmentalization is required.
5. **Data Loss/Leakage.** Be it by deletion without a backup, by loss of the encoding key or by unauthorized access, data is always in danger of being lost or stolen. This is one of the top concerns for businesses, because they not only stand to lose their reputation, but are also obligated by law to keep it safe.
6. **Account, Service & Traffic Hijacking.** Account service and traffic hijacking is another issue that cloud users need to be aware of. These threats range from man-in-the-middle attacks, to phishing and spam campaigns, to denial-of-service attacks.

IV. CLOUD SECURITY

Cloud computing and web services run on a network structure so they are open to network type attacks. One of these attacks is the distributed denial of service attacks. If a user could hijack a server then the hacker could stop the web services from functioning and demand a ransom to put the services back online. To stop these attacks the use of syn cookies and limiting users connected to a server all help stop a DDOS attack. Another such attack is the man in the middle attack. If the secure sockets layer (SSL) is incorrectly configured then client and server authentication may not

behave as expected therefore leading to man in the middle attacks. It is clear that the security issue has played the most important role in hindering Cloud computing. Without doubt, putting your data, running your software at someone else's hard disk using someone else's CPU appears daunting to many. Well-known security issues such as data loss, phishing, and botnet (running remotely on a collection of machines) pose serious threats to organization's data and software. Moreover, the multi-tenancy model and the pooled computing resources in cloud computing has introduced new security challenges that require novel techniques to tackle with.

A. User Identity

In Organizations, only authorized users across their enterprise and access to the data and tools that they require, when they require them, and all unauthorized users are blocked for access. In Cloud environments support a large enterprise and various communities of users, so these controls are more critical. Clouds begin a new level of privileged users working for the cloud provider is administrators. And an important requirement is privileged user monitoring, including logging activities. This monitoring should include background checking and physical monitoring.

B. Audit and Compliance

An organization implements the Audit and compliance to the internal and external processes that may fallow the requirements classification with which it must stand and the requirements are customer contracts, laws and regulations, driven by business objectives, internal corporate policies and check or monitor all such policies, procedures, and processes are without fail. In traditional Out sourcing relationships plays an important role for Audit and compliance. In Cloud dynamic nature, increase the importance of these functions in platform as-a service (PaaS), infrastructure-as-a-service (laaS), and software- as-a-service (SaaS) environments.

C. End User Security Issues

End Users need to access resources within the cloud and may bear in mind of access agreements like acceptable use or conflict of interest. The client organization have some mechanism to find vulnerable code or protocols at entry points like servers, firewalls, or mobile devices and upload patches on the native systems as soon as they are found.

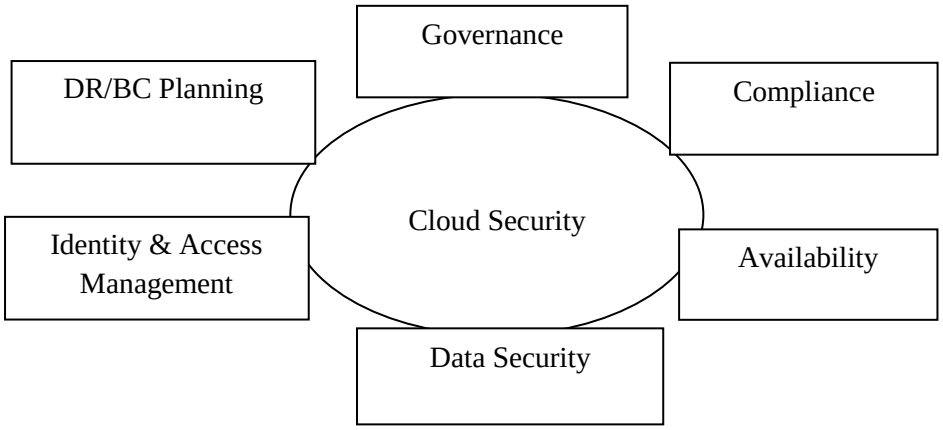

Figure3: Various Types of Cloud Security

D. Limitations of Cloud Computing

1. Data losses / leakage: Cloud computing efforts to control the security of the data is not very better; accordingly API access control and key generation, storage and management deficiencies may result in data leakage, and also may lack the important data destruction policy. Leakage, and causes lack the vital- data destruction policy.

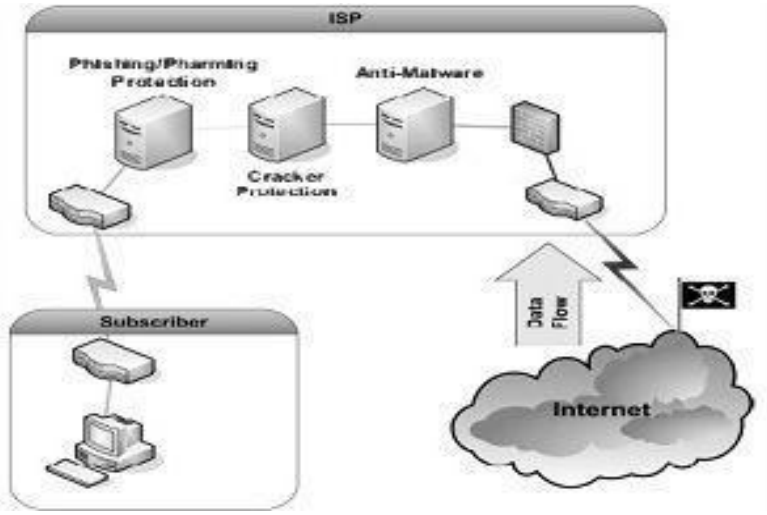

Figure 4: Security aspect of cloud

2. Difficult to assess the reliability of suppliers: Cloud computing service provider of background checks on staff strength may be related to corporate efforts which is then actually used to control data access which is different from many suppliers in this

circumstances, but not enough, companies need to Evaluation of suppliers and propose to prove that how to filter the program staff.

3. Authentication mechanisms are not so strong: In cloud, huge data, applications and resources are collected and cloud computing is very weak authentication mechanism, then the attacker can easily obtain the client user account and log in the virtual machine.

V. CONCLUSION

Cloud computing is a kind of computing paradigm that can access conveniently a dynamic and configurable public set of computing resources (e.g. server, storage, network, application and related service), provided and published rapidly and on-demand with least management and intervention. However, it provides a large array of benefits, but many challenges in this domain, including automatic resource positioning, energy management, information security are only attracted the research community. There are still so many issues to be explored. Opportunities are enough in this arena for some groundbreaking contribution and bring significant development in the industry.

REFERENCES

[1] "Security Architecture of Cloud Computing", V.KRISHNA REDDY 1, Dr. L.S.S.REDDY, International Journal of Engineering Science and Technology (!JEST).

[2]. “Peter Mell, and Tim Grance, "Draft NIST Working Definition of Cloud Computing," 2009.

[3] The NIST Definition of Cloud Computing, version 15, by Peter Mell and Tim Grance, October 7, 2009, National Institute of Standards and Technology (NIST), Information Technology Laboratory (www.csrc.nist.gov)

[4] Wang, Lizhe; von Laszewski, Gregor; Kunze, Marcel; Tao, Jie. Cloud computing: A Perspective study, *Proceedings of the Grid Computing Environments (GCE) workshop. Held at the Austin Civic Center: Austin, Texas*: 16 November 2008.

[5] Wikipedia, http:// en.wikipedia.org/ wiki/ Cloud Computing.

[6] Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing (v2.1). Decemeber,2009

[7]Cloud Security Alliance. Top Threats to Cloud Computing, 2010.http://www.cloudsecurityalliance.org [accessed on: March, 2010].