Cloud Computing Security Analysis

Virendra Agarwal
Student
Department of Computer Science and Engineering
SRM University, Chennai, India

***Abstract* - Cloud Computing is a buzzword in the market. Cloud Computing enables companies to consume computing resources as a utility rather than having to build and maintain computing infrastructure in-house. Cloud Computing provides elastic resources, metered services and self –service provisioning via internet. Cloud Computing promises to cut operational and capital costs and let the IT department focus on projects rather than keeping the datacenters running. But with growing trends to move the data from local computers to the cloud the concerns related to security and privacy of data also grow. The purpose of this paper is to examine various issues in cloud computing and measures which are being taken or measures which are to be taken to move towards a safer cloud.**

***Index Terms* - Cloud Computing, Denial of Service, Types of Cloud, Data Breaches.**

I. INTRODUCTION

Let's say you are an executive in a large corporation. Your job includes making sure that all your employees have the right hardware an software they need to do their jobs. Buying computers for everyone isn't enough. You also have to purchase software and software licenses to give employees the tools they require. Whenever you have a new hire you have to buy new software or make sure your current software allows new users. Doing all this would require spending huge amount of money depending on your company size.

Now consider an alternative. Instead of installing a suite of software for each computer you only have to load one application. That application would allow users to log into a web based service which hosts all the programs the user would need for his or her job. Remote machines owned by other companies would run everything from e-mail to word processing to other complex programs. This alternative is Cloud Computing. The only requirement for running a cloud application is a good internet connection. Cloud computing provides many features like elastic resources and pay per use services which make is so popular among its users. Clients need not worry about the maintenance and management of resources. This is why cloud computing allows consumption of computing resources as a utility.

But cloud computing has many security concerns which make it vulnerable to data breaches and theft of valuable information of its clients. This paper focuses on issues of security in cloud computing and examines various measures to improve cloud security.

II. CLOUD COMPUTING –SERVICES AND DEPLOYMENT MODELS

According to IBM Cloud Computing often referred to as simply "the cloud" is the delivery of on demand computing resources-everything from applications to datacenters-over the Internet for a pay-for-use basis.

There are three types of cloud computing services:

- Software as a service(SaaS)
- Platform as a service(PaaS)
- Infrastructure as a service(IaaS)

Software as a service(SaaS): Cloud based applications-or software as a service run on distant computers "in the cloud" that are owned and operated by others and that connect to user's computers via the Internet and, usually a web browser. Cloud providers manage the infrastructure and platforms that run the applications. SaaS is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis or using a subscription fee.

Platform as a service(PaaS): Platform as a service provides a cloud-based environment with everything required to support the complete life cycle of building and delivering web-based (cloud) applications—without the cost and complexity of buying and managing the underlying hardware, software, provisioning and hosting. For example IBM SmartCloud Application Services enable users to devlop and deploy applications to the cloud in minutes.

Infrastructure as a service(IaaS): Infrastructure as a service provides companies with computing resources including servers, networking, storage, and data centre space. In this model the cloud user maintains the operating systems and the application software. Cloud providers bill the IaaS services on a utility computing basis, cost reflects the amount of resources allocated and consumed.

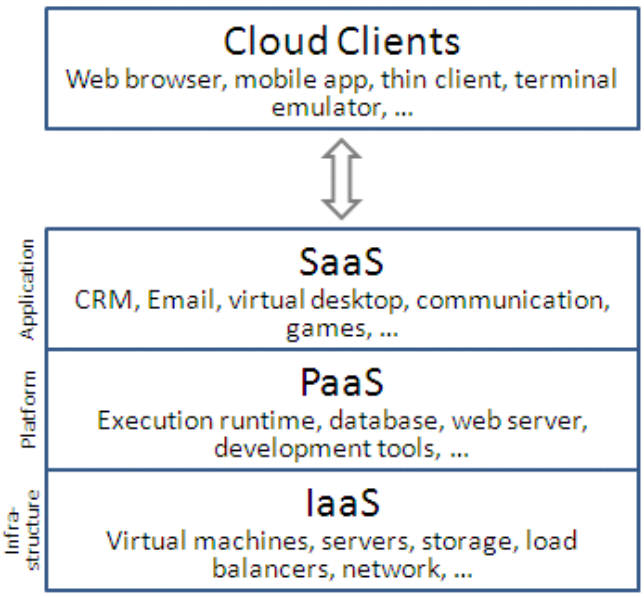

Fig 1: Cloud Computing Services

There are three deployment models in cloud computing:

- Public Cloud
- Private Cloud
- Hybrid Cloud

Public Cloud: Public clouds are owned and operated by companies that use them to offer rapid access to affordable computing resources to other organisations or individuals. With public cloud services, users don't need to purchase hardware, software or supporting infrastructure, which is owned and managed by providers.

Private Cloud: A private cloud is owned and operated by a single company that controls the way virtualised resources and automated services are customised and used by various lines of business and constituent groups. Private clouds exist to take advantage of many of cloud's efficiencies, while providing more control of resources and steering clear of multi-tenancy.

Hybrid Cloud: A hybrid cloud uses a private cloud foundation combined with the strategic use of public cloud services. The reality is a private cloud can't exist in isolation from the rest of a company's IT resources and the public cloud. Most companies with private clouds will evolve to manage workloads across data centre's, private clouds and public clouds—thereby creating hybrid clouds.

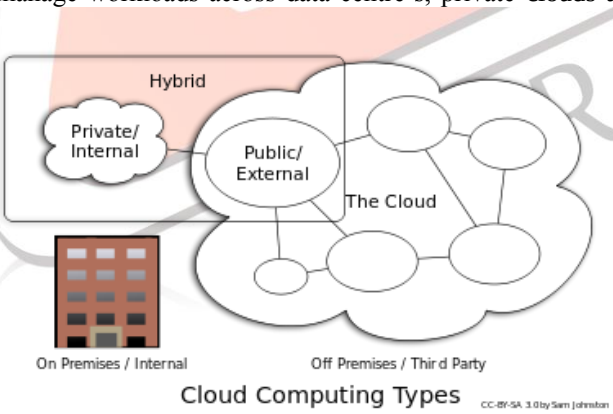

Fig 2: Cloud Computing Deployment Models

III. Cloud Computing Security Threats

Cloud Computing has some security threats which are discussed below:

- **Data Breaches and Data Loss:** Client's data is stored far from client's machine. Transmission of data to/from client's machine to the cloud, system upgrades, measures to mitigate a flaw, attacks by intruders etc can all lead to data breaches and data loss
- **Insecure Interfaces and API's:** IT administrators rely on interfaces for cloud provisioning, management, orchestration, and monitoring. APIs are integral to security and availability of general cloud services. From there, organizations and third parties are known to build on these interfaces, injecting add-on services. "This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third parties in order to enable their agency. Weak interfaces and API's can expose an organization to such security issues pertaining to confidentiality, integrity, availability and accountability.
- **Service Traffic Hijacking:** In this type of security breach , hackers seek to hijack your account by stealing your security credentials and then eavesdropping on your activities and transactions, manipulating data and inserting false

information. This type of attack is particularly scary because the attackers are able to use your reputation and the trust you have built up to manipulate your clients.

- **Distributed Denial of Service (DDoS):** In Distributed Denial of Service attack a large number of false requests are sent to the server. The server gets busy responding to the false requests and thus is not able to respond to an authentic request by the client leading to this attack.
- **Malicious Insiders:** Former or current employees of an organization providing cloud services can access to the stored information of a client and can misuse the information or sell it to another organization. All of this happens internally in an organization so the clients are left unaware.
- **Cloud Abuse:** Another security threat is cloud abuse such as a bad guy using a cloud service to break an encryption key too difficult to crack on a standard computer. Another example might be a malicious hacker using cloud servers to launch a Distributed Denial of Service attack, propagate malware, or share pirated software. The challenge here is for cloud providers to define what constitutes abuse and to determine the best processes for identify it.
- **Insufficient Due Diligence**: It means that organizations embrace the cloud without fully understanding the cloud environment and associated risks. For example, entering the cloud can generate contractual issues with providers over liability and transparency. What's more, operational and architectural issues can arise if a company's development team isn't sufficiently familiar with cloud technologies as it pushes an app to the cloud.
- **Shared Technology Vulnerabilities:** Cloud service providers shared infrastructure, platforms, and applications to deliver their services in a scalable way. "Whether it's the underlying components that make up this infrastructure (e.g. CPU caches, GPUs, etc.) that were not designed to offer strong isolation properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS), or multi-customer applications (SaaS), the threat of shared vulnerabilities exists in all delivery models," according to the CSA report. If an integral component gets compromised -- say, a hypervisor, a shared platform component, or an application -- it exposes the entire environment to a potential of compromise and breach.

IV. SECURITY: METHODS AND TECHNIQUES

- **Encryption-** Most widely used encryption techniques are RSA. For man in the middle attack network and message delays need to be monitored in sending and receiving data so that the attack can be recognized. To protect your data as it travels over the Internet during read and write operations, use Transport Layer Security (HTTPS).SSL is used to transmit data between user and server.
- **Security and Privacy Management-** Companies offering cloud computing services live and die by their reputations. It benefits these companies to have reliable security measures in place. Otherwise, the service would lose all its clients. It's in their interest to employ the most advanced techniques to protect their client's data. Privacy is another matter. If a client can log in from any location to access data and applications, it's possible the client's privacy could be compromised. Cloud computing companies will need to find ways to protect client privacy. One way is to use authentication techniques such as user names and passwords. Another is to employ an authorization format such that each user can access only the data and applications relevant to his or her job.
- **Inter Cloud-** The Intercloud is an interconnected global "cloud of clouds" and an extension of the Internet "network of networks" on which it is based**.** Storage services don't communicate directly with each other but instead go through the larger cloud for authentication. Data is encrypted as it leaves one station and decrypted before it reaches the next. If one cloud happens to fail, a back-up cloud responds immediately. The cloud-of-clouds is also intrinsically more secure: "If one provider gets hacked there is little chance they will penetrate other systems at the same time using the same vulnerability.
- **Security of Physical Infrastructure-** Physical infrastructure used for maintaining the cloud service should be secured and it is the responsibility of the cloud service provider to ensure the protection of physical infrastructure against external, internal and environmental threats including control of personnel working in secure area and providing necessary backups against any danger.
- **Detection and Prevention-** A cloud service provider must allow legitimate network traffic and drop malicious network traffic. Intrusion detection and prevention softwares must be up to date to prevent any illegitimate activities. Customer should receive login notifications. Policy changes and any updates must be regularly communicated.
- **Safe Exit-** The exit process or termination of the use of cloud service by a consumer requires careful considerations. It is important that once the customer has completed the exit process, the customer must be able to ensure a smooth transition without loss or breach of data.The provider must ensure that any copies of the data are wiped clean from the provider's environment, wherever they may have been stored (i.e. including backup locatio ns as well as online data stores) .

V. CONCLUSION

No doubt that cloud computing offers some exciting new opportunities for increased collaboration, working remotely and globally, and cost savings. There are risks associated with moving to the cloud but they are no more than when the services are hosted internally. If we take the time to understand the vulnerabilities that exist in the cloud and what we can do to prevent attackers from exploiting them, cloud-based services can be as secure as any service hosted within an organization's local or wide area network.

VI. REFERENCES

[1] Cloud Security Alliance,"Cloud Usage: Risks and Oppurtinities Report",Sept 2014.
[2] http://computer.howstuffworks.com/cloud-computing/cloud-computing3.htm
[3] http://www.infoworld.com/article/2613560/cloud-security/cloud-security-9-top-threats-to-cloud-computing-security.html
[4] https://cloudsecurityalliance.org/
[5] https://msdn.microsoft.com/en-us/magazine/ee291586.aspx
[6] https://cloud.google.com/storage/docs/concepts-techniques#bestpractices
[7] http://www.ciphercloud.com/products/ciphercloud-for-salesforce/
[8] http://www.cisco.com/c/en/us/products/cloud-systems-management/intercloud-fabric/index.html
[9] en.wikipedia.org/wiki/Intercloud
[10] http://www.cisco.com/c/en/us/products/cloud-systems-management/intercloud-fabric/index.html
[11] Jitender Grover,Shikha and Mohit Sharma,"Cloud Computing and Its Securiy Issues-A Review",5th ICCCNT-2014,Hefei,China
[12] Sherif El-etriby,Eman M.Mohamed and Hatem S.Abdul-Kader,"Modern Encryption Techniques For Cloud Computing".
[13] Aizmed Amin Soofi,M.Irfan Khan and Fazal-e-Amin,"Encryption Techniques for Cloud Data Confidentiality",International Journal of Grid Distribution Computing,Vol 7,No 4(2014),pp.11-20,http://dx.doi.org/10.14257/ijgdc.2014.7.4.02
[14] Venkata Sravan KumarMaddineni and Shivashanker Ragi,"Security Technique for Protecting Data in Cloud Computing",Master Thesis,Department of Computing,Blekinge Institute of Technology,SE-37179,Karlskrona,Sweden.
[15] V.Shobana and M.Shanmugasundaram,"Data Lekage Detection Using Cloud Computing",International Journal of Emerging Technology and Advanced Engineering