CLOUD COMPUTING: SECURITY ISSUES AND SECURITY MEASURES

Disha Bhatnagar[1], Rajkumar Singh Rathore[2]

[1]PG Scholar, Masters of Technology ,
Galgotias College of Engineering and Technology, Greater Noida (India)
[2] Assistant Professor, Department of Computer Science & Engineering
Galgotias College of Engineering & Technology, Greater Noida (India)

ABSTRACT

Cloud based services and service providers are being evolved which has resulted in a new business trend based on cloud technology. With the introduction of numerous cloud based services and geographically dispersed cloud service providers, sensitive information of different entities are normally stored in remote servers and locations with the possibilities of being exposed to unwanted parties in situations where the cloud servers storing those information are compromised. If security is not robust and consistent, the flexibility and advantages that cloud computing has to offer will have little credibility. This paper presents a review on the cloud computing concepts as well as security issues inherent within the context of cloud computing and cloud infrastructure. Cloud computing is a fast growing information technology, has aroused the concern of the whole world. This is a favorable situation to study and application of cloud computing related technologies. However, most existing Cloud Computing platforms have not formally adopted the service-oriented architecture (SOA) that would make them more flexible, extensible, and reusable. The security aspects in a cloud based computing environment remains at the core of interest. We have categorized these threats according to different viewpoints, providing a useful and little-known list of threats. After that some effective countermeasures are listed and explained.

Keywords : ***Cloud Architecture , Security Concerns, Security Measures and Counter Attacks in Cloud Computing ,CCOA, Iaas, OSI Model, Paas, SaaS , SOA,***

I INTRODUCTION

Cloud computing is a term used to describe both a platform and type of application. A cloud computing platform dynamically provisions, configures, reconfigures, and deprovisions servers as needed. Servers in the cloud can be physical machines or virtual machines. Advanced clouds typically include other computing resources such as storage area networks (SANs), network equipment, firewall and other security devices. Cloud computing also describes applications that are extended to be accessible through the Internet. These cloud applications use large data

centers and powerful servers that host Web applications and Web services. Anyone with a suitable Internet Recent developments in the field of could computing have immensely changed the way of computing as well as the concept of computing resources. In a cloud based computing infrastructure, the resources are normally in someone else's premise or network and accessed remotely by the cloud users. Processing is done remotely implying the fact that the data and other elements from a person need to be transmitted to the cloud infrastructure or server for processing; and the output is returned upon completion of required processing. In some cases, it might be required or at least possible for a person to store data on remote cloud servers. These gives the following three sensitive states or scenarios that are of particular concern within the operational context of cloud computing:

1. The transmission of personal sensitive data to the cloud server,
2. The transmission of data from the cloud server to clients' computers and
3. The storage of clients' personal data in cloud servers which are remote server not owned by the clients.

Cloud computing has several distinct characteristics that distinguish it from a traditionally-hosted computing environment:

- Users often have on-demand access to scalable information technology capabilities and services that are provided through internet-based technologies.
- These resources run on an external or third-party service provider's system. This is in contrast to traditional systems, which run on locally-hosted servers. Unlike traditional systems which are under the user's personal control or institutional control, cloud computing services are fully managed by the provider.
- Typically, many unaffiliated and unconnected users share the service provider's infrastructure.
- Using cloud services reduces the need to carry data on removable media because of network access anywhere, anytime.

Cloud services, sometimes called "software as a service" (SaaS) ,"infrastructure as a service" (IaaS), or "platform as a service" (PaaS), facilitate rapid deployment of applications and infrastructure without the cost and complexity of purchasing, managing, and maintaining the underlying hardware and software.

II. SERVICES IN CLOUD

In recent years, the cloud has evolved in two broad perspectives – to rent the infrastructure in cloud, or to rent any specific service in the cloud. Where the former one deals with the hardware and software usage on the cloud, the later one is confined only with the 'soft' products or services from the cloud service and infrastructure providers. The computing world has been introduced with a number of terminologies like SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) with the evolution of cloud computing. As discussed earlier, the term 'cloud computing' is rather a concept, so are the terminologies to define different blends of cloud computing. At its core essence, cloud computing is nothing but a specialized form of grid International Journal of

Network Security & Its Applications and distributed computing which varies in terms of infrastructure, services, deployment and geographic dispersion .

The services provided by cloud providers can be divided into following three main layered categories. Each layer consumes services provided by the layer below it.

1. Software as a service (SAAS)

SaaS clients rent usage of applications running within the Cloud‟s provider infrastructure, for example SalesForce . The applications are typically offered to the clients via the Internet and are managed completely by the Cloud provider. That means that the administration of these services such as updating and patching are in the provider's responsibility. One big benefit of SaaS is that all clients are running the same software version and new functionality can be easily integrated by the provider and is therefore available to all clients.

2. Platform as a service (PAAS)

PaaS Cloud providers offer an application platform as a service, for example Google App Engine. This enables clients to deploy custom software using the tools and programming languages offered by the provider. Clients have control over the deployed applications and environment-related settings. As with SaaS, the management of the underlying infrastructure lies within the responsibility of the provider.

3. Infrastructure as a service (IAAS)

IaaS delivers hardware resources such as CPU, disk space or network components as a service. These resources are usually delivered as a virtualization platform by the Cloud provider and can be accessed across the Internet by the client. The client has full control of the virtualized platform and is not responsible for managing the underlying infrastructure.

4. Storage as a service

Storage as a service (STaaS) is a business model in which a large service provider rents space in their storage infrastructure on a subscription basis. The economy of scale in the service provider's infrastructure allows them to provide storage much more cost effectively than most individuals or corporations can provide their own storage, when total cost of ownership is considered. Storage as a Service is often used to solve offsite backup challenges**.** Critics of storage as a service point to the large amount of network bandwidth required to conduct their storage utilizing an internet-based service.

5. Security as a service

Security as a service (SCaaS) is a business model in which a large service provider integrates their security services into a corporate infrastructure on a subscription basis more cost effectively than most individuals or corporations can

provide on their own, when total cost of ownership is considered. These security services often include authentication, anti-virus, anti-malware/spyware, intrusion detection, and security event management, among others.

6. Data as a service

Data as a service, or DaaS, is a cousin of software as a service. Like all members of the "as a Service" (aaS) family, DaaS is based on the concept that the product, data in this case, can be provided on demand to the user regardless of geographic or organizational separation of provider and consumer. Additionally, the emergence of service-oriented architecture (SOA) has rendered the actual platform on which the data resides also irrelevant.

III. CLOUD COMPUTING SECURITY

When talking about a cloud computing system , it's helpful to divide it into two sections: the front end and the back end. They connect to each other through a network, usually the Internet. The front end is the side the computer user, or client, sees. The back end is the "cloud" section of the system. The front end includes the client's computer (or computer network) and the application required to access the cloud computing system. Not all cloud computing systems have the same user interface. Services like Web-based e-mail programs leverage existing Web browsers like Internet Explorer or Firefox. Other systems have unique applications that provide network access to clients. On the back end of the system are the various computers, servers and data storage systems that create the "cloud" of computing services. In theory, a cloud computing system could include practically any computer program you can imagine, from data processing to video games. Usually, each application will have its own dedicated server.

However, it is important to distinguish between risk and security concerns in this regard. For example, vendor lock-in might be considered as one of the possible risks in cloud based services which do not essentially have to be related to security aspects. On the contrary, using specific type of operating system (e.g. opensource vs. proprietary) might pose security threat and concerns which, of course, is a security risk. Other examples of business risks of cloud computing could be licensing issues, service unavailability, provider's business discontinuity that do not fall within the security concerns from a technical viewpoint. Thus, in cloud computing context, a security concern is always some type of risk but any risk cannot be blindly judged to be a security concern. Allocation of responsibilities among the parties involved in a cloud computing infrastructure might result in experiencing inconsistency which might eventually lead to a situation with security vulnerabilities. Like any other network scenario, the provision of insider-attack remains as a valid threat for cloud computing Any security tools or other kinds of software. used in a cloud environment might have security loopholes which in turn would pose security risks to the cloud infrastructure itself. The problem with third party APIs as well as spammers are threats to the cloud environment. As cloud computing normally means using public networks and subsequently putting the transmitting data exposed to the world, cyber attacks in any form are anticipated for cloud computing. The existing contemporary cloud based services have been found to suffer from vulnerability issues with the existence of possible security loopholes that could be exploited by an attacker. Security and privacy both are concerns in cloud computing due to the nature of such computing approach . The approach by which cloud computing is done has made it prone to both information security and network security issues .

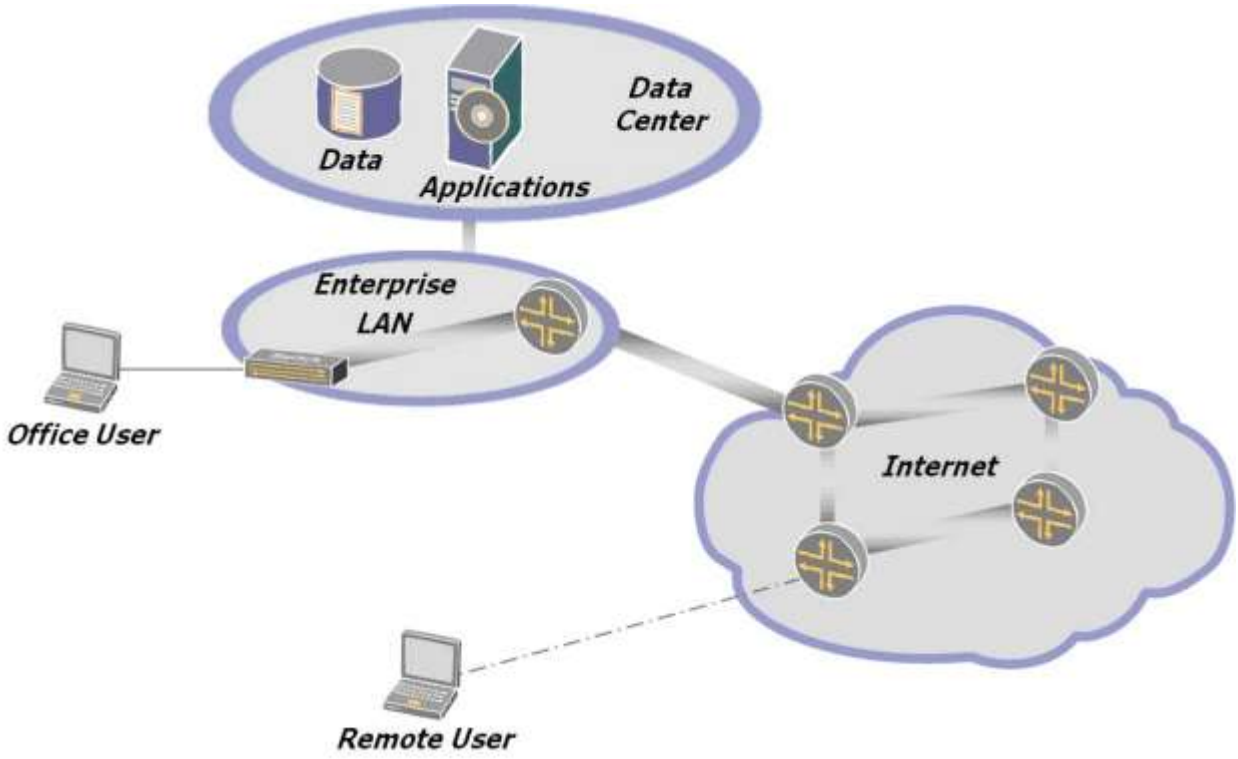

Fig 1: Cloud Computing Model

A central server administers the system, monitoring traffic and client demands to ensure everything runs smoothly. It follows a set of rules called protocols and uses a special kind of software called middleware. Middleware allows networked computers to communicate with each other. Most of the time, servers don't run at full capacity. That means there's unused processing power going to waste. It's possible to fool a physical server into thinking it's actually multiple servers, each running with its own independent operating system. The technique is called server virtualization. By maximizing the output of individual servers, server virtualization reduces the need for more physical machines. If a cloud computing company has a lot of clients, there's likely to be a high demand for a lot of storage space. Some companies require hundreds of digital storage devices. Cloud computing systems need at least twice the number of storage devices it requires to keep all its clients' information stored. That's because these devices, like all computers, occasionally break down. A cloud computing system must make a copy of all its clients' information and store it on other devices. The copies enable the central server to access backup machines to retrieve data that otherwise would be unreachable. Making copies of data as a backup is called redundancy.

3.1 Security Concerns of Cloud Computing Architecture

Principle 1: Overall Security Concerns

[1] Gracefully lose control while maintaining accountability even if operational responsibility falls upon 3rd parties.

[2] Provider, user security duties differ greatly between cloud models 22 Governance.

[3] Identify, implement process, controls to maintain effective governance, risk mgt, compliance

[4] Provider security governance should be assessed for sufficiency, maturity, consistency with user ITSEC process 3 rd Party Governance

[5] Request clear docs on how facility & services are assessed

[6] Require definition of what provider considers critical services, information.

[7] Perform full contract, terms of use due diligence to determine roles, accountability 24 Legal, e-Discovery

[8] Functional: which functions & services in the Cloud have legal implications for both parties.

[9] Jurisdictional: which governments administer laws and registrations impacting services, stakeholders, data assets .

[10] Both parties must understand each other's roles – Litigation hold, Discovery searches – Expert testimony • Provider must save primary and secondary (logs) data.

PRINCIPLE 2: Bigger Security Concerns For Cloud Computing

There are two basic approaches for enabling virtualization in the Cloud Computing environment.

a. Hardware virtualization that is to manage hardware equipment in plug-and-play mode.

b. Software virtualization, i.e., to use software image management or software code virtualization technology to enable software sharing.

• **Management interface vulnerability**. Consumer management interfaces of a public cloud provider are usually accessible through the Internet and mediate access to larger sets of resources than traditional hosting providers and therefore pose an increased risk, especially when combined with remote access and web browser vulnerabilities.

• **Data protection**. Cloud computing poses several data protection risks for cloud consumers and providers. The major concerns are exposure or release of sensitive data but also include loss or unavailability of data. In some cases, it may be difficult for the cloud consumer (in the role of data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g., between federated cloud services.

• **Malicious behavior of insiders**. Damage caused by the malicious actions of insiders working within an organization can be substantial, given the access and authorizations they may have. This is compounded in the cloud computing environment since such activity might occur within either or both the consumer organization and the provider organization.

• **Business failure of the provider**. Such failures could render data and applications essential to the consumer's business unavailable.

• **Service unavailability**. This could be caused by a host of factors, from equipment or software failures in the provider's data center, through failures of the communications between the consumer systems and the provider services.

• **Insecure or incomplete data deletion**. Requests to delete cloud resources, for example,when a consumer terminates service with a provider, may not result in true wiping of the data. Adequate or timely data deletion may also be impossible (or undesirable from a consumer perspective), either because extra copies of data are stored but are not available, or because the disk to be deleted also stores data from other clients. In the case of multi-tenancy and the reuse of hardware resources, this represents a higher risk to the consumer than is the case with dedicated hardware.

PRINCIPLE 3: MANAGING SECURITY IN CLOUD

Since cloud computing typically involves two organizations - the service consumer and the service provider, security responsibilities of each party must be made clear. This is typically done by means of a service level agreement (SLA) which applies to the services provided, and the terms of the contract between the consumer and the provider. The SLA should specify security responsibilities and should include aspects such as the reporting of security breaches. SLAs for cloud computing are discussed in more detail in the CSCC document "Practical Guide to Cloud Service Level Agreements. One feature of an SLA relating to security is that any requirements that are placed on the cloud provider by the SLA must also pass on to any peer cloud service providers that the provider may use in order to supply any part of their service(s). It should be explicitly documented in the cloud SLA that providers must notify consumers about the occurrence of any breach of their system, regardless of the parties or data directly impacted. The provider should include specific pertinent information in the notification, stop the data breach as quickly as possible, restore secure access to the service as soon as possible, apply best-practice forensics in investigating the circumstances and causes of the breach, and make long-term infrastructure changes to correct the root causes of the breach to ensure that it does not recur

IV. EXAMINING SECURITY REQUIREMENTS OF EXIT PROCESS

The exit process or termination of the use of a cloud service by a consumer requires careful consideration from a security perspective. From a security perspective, it is important that once the consumer has completed the termination process, "reversibility" or "the right to be forgotten" is achieved - i.e. none of the consumer's data should remain with the provider. 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 locations as well as online data stores). Note that other data held by the provider may need "cleansing" of information relating to the consumer (e.g. logs and audit trails), although some jurisdictions may require retention of records of this type for specified periods by law. Clearly, there is the opposite problem during the exit process itself - the consumer must be able to ensure a smooth transition, without loss or breach of data. Thus the exit process must allow the consumer to retrieve their data in a suitably secure form, backups must be retained for agreed periods before being eliminated and associated event logs and reporting data must also be retained until the exit process is complete.

.

V. CONCLUSION

Cloud computing has enormous prospects, but the security threats embedded in cloud computing approach are directly proportional to its offered advantages. Cloud computing is a great opportunity and lucrative option both to the businesses and the attackers – either parties can have their own advantages from cloud computing. The vast possibilities of cloud computing cannot be ignored solely for the security issues reason – the ongoing investigation and research for robust, consistent and integrated security models for cloud computing could be the only path of motivation. The security issues could severely affect could infrastructures and software. The vastness and potentiality of cloud computing cannot be overlooked, subsequently robust security models for cloud computing scenarios is the most prioritized factor for a successful cloud based infrastructure development and deployment. With the goal of secured exploitation of a Service Oriented Architecture, the security aspects and issues of cloud computing are inherent not only with the elements that from the cloud infrastructure but also with all associated services as well as the ways computing is done both at the users' and the cloud service providers' ends. The security issues in cloud computing are somewhat sensitive and crucial on the basis of sociological and technological viewpoints – the technological inconsistency that results in security breach in cloud computing might lead to significant sociological impact. Cloud computing brings us the approximately infinite computing capability, good scalability, service on-demand and so on, also challenges at security, privacy, legal issues and so on. To welcome the coming cloud computing era, solving the existing issues becomes utmost importunity.

REFERENCES

[1] Web-Resource http://en.wikipedia.org/wiki/Cloud_computing

[2] Mircea, M. (2012). Addressing Data Security in the Cloud. World Academy of Science, Engineering and Technology, 66, 539-546.

[3] Cloud Computing and Grid Computing 360-Degree Compared by Ian Foster, Yong Zhao, Ioan Raicu, Shiyong Lu. (IEEE Conference, **Date of Conference:** 12-16 Nov. 2008)

[4] Cloud Computing: a Perspective Study Lizhe WANG, Gregor VON LASZEWSKI

[5] http://computer.howstuffworks.com/cloud-computing/cloud-computing1.htm

[6] Ryan, P. and Falvey, S. (2012). Trust in the clouds. Computer Law and Security Reviews, 28, 513- 521. http://dx.doi.org/10.1016/j.clsr.2012.07.002

[7] Liang-Jie Zhang and Qun Zhou, CCOA: Cloud Computing Open Architecture 2009 IEEE International Conference on Web Services, 2009.

[8] http://en.wikipedia.org/wiki/Virtualization

[9] http://www.dummies.com/how-to/content/how-to-use-virtualization-with-cloud-computing.html