Cloud Computing: Security and Privacy Issues

[1]T. Deepa and [2]M.Kiran Mayee,
[1,2]Assistant Professor, CSE Department, Ravindra College of Engineering for Women, Kurnool, India

***Abstract*—** Cloud computing, a rapidly developing technology, has become the concern of the entire world. It aims in constructing a perfect system with powerful computing capabilities with a large number of relatively low-cost computing services. It uses many advanced models like SaaS, PaaS and IaaS for distributing powerful computing capabilities to end users. Cloud computing is internet based technology where the customer data is stored and managed by the service providers in the data centers this may create various serious security issues and threats. This paper outlines the different cloud models and privacy and security issues. We identified the most five important privacy and security attributes(i.e confidentiality, integrity, availability, accountability, and privacy-preservability) and discussed various threats based on these attributes.

***Index Terms*—**Cloud computing, cloud architecture, Data security, privacy

I. INTRODUCTION

Now a day's cloud computing is everywhere. Users are using the cloud without knowing that they are using it. It provides organization and individuals with a cost effective model by delivering the services over the Internet. Small and medium organizations are moving to cloud computing because it will support their business with fast access to their application and reduce the cost of infrastructure. The Cloud computing is not only a technical solution but also a business model that computing power can be sold and rented. Cloud computing is focused on delivering services. Organization data are being hosted in the cloud. The ownership of data is decreasing while agility and responsiveness are increasing. Organizations now are trying to avoid focusing on IT infrastructure. They need to focus on their business process to increase profitability. Therefore, the importance of cloud computing is increasing, becoming a huge market and receiving much attention from the academic and industrial communities.

Regarding definition of cloud computing model, the most widely used one is made by NIST as "Cloud computing is a model for enabling 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. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models."[1]

The cloud computing model NIST defined[7] has three service models, four deployment models and five characteristics as shown in figure1. The three service models, also called SPI model, are: Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS) and Cloud Infrastructure as a Service (IaaS). The four deployment models are: Private cloud, Community cloud, Public cloud and Hybrid cloud. Characteristic of cloud computing

On-demand self-service: A cloud customer may obtain computing capabilities, like the usage of various servers and network storage, on demand, without interacting with the cloud provider.

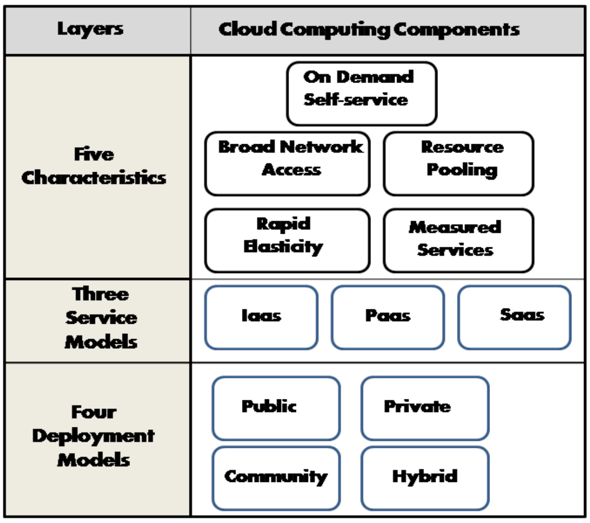
Broad network access: Services are delivered across the Internet via a standard mechanism that allows customers to access the services through heterogeneous tools e.g., PCs, mobile phones, and PDAs.

Resource pooling: The cloud provider employs a multitenant model to serve multiple customers by pooling computing resources, where different physical and virtual resources dynamically assigned or reassigned according to customer demand. Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

Rapid elasticity: Resources are dynamically increased when needed and decreased when there is no need. Cloud customer may obtain computing capabilities, like the usage of various servers and network storage, as on demand, without interacting with the cloud provider.

Measured service: The service purchased by customers can be quantified and measured. For both the provider and customers, resource usage will be monitored, controlled, metered, and reported.

Cloud computing appeared as a business necessity now a days, basing on the idea of just using the infrastructure without managing it. Initially this idea was present only in the academic area; recently, it was transposed into industry by companies like Microsoft, Amazon, Google, Yahoo! and Salesforce.com. This makes it possible for new startups to enter the market easier, since the cost of the infrastructure is greatly diminished. This allows developers to concentrate on the business value rather on the starting budget. The cloud providers rent computing power (virtual machines) or storage space (virtual space) dynamically, according to the requirements of their business.



Layers	Cloud Computing Components
Five Characteristics	On Demand Self-service Broad Network Access Resource Pooling Rapid Elasticity Measured Services
Three Service Models	Iaas Paas Saas
Four Deployment Models	Public Private Community Hybrid

Fig 1: Cloud environment Architecture

II. CLOUD COMPUTING SECURITY ISSUES

Compared with the traditional IT model, the cloud computing has many potential advantages. But from the consumers' perspective, cloud computing security concerns remain a major barrier for the adoption of cloud computing.

Cloud computing service providers touted the security and reliability of their services, actual deployment of cloud computing services is not as safe and reliable as they claim. In 2009, the major cloud computing vendors successively appeared several accidents. Amazon's Simple Storage Service was interrupted twice in February and July 2009. This accident resulted in some network sites relying on a single type of storage service were forced to a standstill. In March 2009, security vulnerabilities in Google Docs even led to serious leakage of user private information. Google Gmail also appeared a global failure up to 4 hours. It was exposed that there was serious security vulnerability in VMware virtualization software for Mac version in May 2009. People with ulterior motives can take advantage of the vulnerability in the Windows virtual machine on the host Mac to execute malicious code. Microsoft's Azure cloud computing platform also took place a serious outage accident for about 22 hours. Serious security incidents even lead to collapse of cloud computing vendors. As administrators' misuse leading to loss of 45% user data, cloud storage vendor Link-Up had been forced to close.

There are numerous security issues for cloud computing as it includes many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management[1]. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. As shown in Figure 2, there are six specific areas of the cloud computing environment where equipment and software require substantial security attention.

These six areas are: (1) security of data at rest, (2) security of data in transit, (3) authentication of users/applications/ processes, (4) robust separation between data belonging to different customers, (5) cloud legal and regulatory issues, and (6) incident response.

For securing data at rest, cryptographic encryption mechanisms are certainly the best options. The hard drive manufacturers are now shipping self-encrypting drives that implement trusted storage standards of the trusted computing group. These self-encrypting drives build encryption hardware into the drive, providing automated encryption with minimal cost or performance impact. Although software encryption can also be used for protecting data, it makes the process slower and less secure since it may be possible for an adversary to steal the encryption key from the machine without being detected.

Encryption[1] is the best option for securing data in transit as well. In addition, authentication and integrity protection mechanisms ensure that data only goes where the customer wants it to go and it is not modified in transit. Strong authentication is a mandatory requirement for any cloud deployment. User authentication is the primary basis for access control. In the cloud environment, authentication and access control are more important than ever since the cloud and all of its data are accessible to anyone over the Internet. The trusted computing group's (TCG's) IF-MAP standard allows for real-time communication between a cloud service provider and the customer about authorized users and other security issues. When a user's access privilege is revoked or reassigned, the customer's identity management system can notify the cloud provider in real-time so that the user's cloud access can be modified or revoked within a very short span of time.

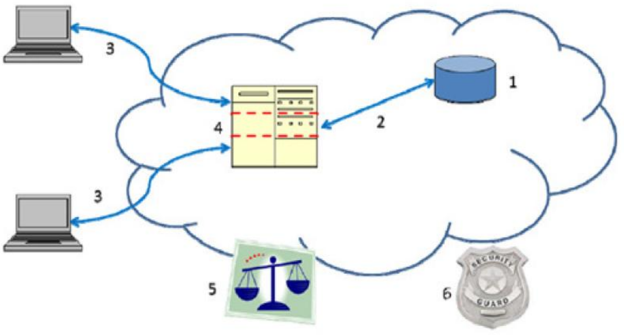


Figure 2: Areas for security concerns in cloud computing: (1) data at rest, (2) data in transit, (3) authentication, (4) separation between customers, (5) cloud legal and regulatory issues and (6) incident response.

One of the more obvious cloud concerns is separation between a cloud provider's users (who may be competing companies or even hackers) to avoid inadvertent or intentional access to sensitive information. Typically a cloud provider would use virtual machines (VMs) and a hypervisor to separate customers. Technologies are currently available that can provide significant security improvements for VMs and virtual network separation. In addition, the trusted platform module (TPM) can provide hardware-based verification of hypervisor and VM integrity and thereby ensure strong network separation and security.

III. CLOUD SECURITY THREATS

The threats to information assets residing in the cloud can vary according to the cloud delivery models used by cloud user organizations. There are several types of security threats to which cloud computing is vulnerable. The threats for cloud customers categorized according to the confidentiality, integrity and availability (CIA) security model and their relevance to each of the cloud service delivery model.

Threat to Confidentiality: The different threats that will affect the confidentiality of data are

a. ***Insider user threats:*** The threat of insiders accessing customer data held within the cloud is greater as each of the delivery models can introduce the need for multiple internal users:

   - SaaS – cloud customer and provider administrators
   - PaaS- application developers and test environment managers
   - IaaS- third party platform consultants

b. ***External attacker threats:*** The threat from external attackers may be perceived to apply more to public Internet facing clouds, however all types of cloud delivery models are affected by external attackers, particularly in private clouds where user endpoints can be targeted. Cloud providers with large data stores holding credit card details, personal information and sensitive government or intellectual property, will be subjected to attacks from groups, with significant resources, attempting to retrieve data.

This includes the threat of hardware attack, social engineering and supply chain attacks by dedicated attackers.

c. ***Data leakage:*** A threat from widespread data leakage amongst many, potentially competitor organizations, using the same cloud provider could be caused by human error or faulty hardware that will lead to information compromise.

Threat to Integrity: The different threats that will affect the integrity of data are

a. ***Data segregation:*** The integrity of data within complex cloud hosting environments such as SaaS configured to share computing resource amongst customers could provide a threat against data integrity if system resources are effectively segregated.
b. ***User access:*** Implementation of poor access control procedures creates many threat opportunities, for example that disgruntled ex-employees of cloud provider organizations maintain remote access to administer customer cloud services, and can cause intentional damage to their data sources
c. ***Data quality:*** The threat of impact of data quality is increased as cloud providers host many customers' data. The introduction of a faulty or misconfigured component required by another cloud user could potentially impact the integrity of data for other cloud users sharing infrastructure.

Threat to Availability: The different threats that will affect the availability of data are

a. ***Change management:*** As the cloud provider has increasing responsibility for change management within all cloud delivery models, there is a threat that changes could introduce negative effects. These could be caused by software or hardware changes to existing cloud services.
b. ***Denial of service threat:*** The threat of denial of service against available cloud. Computing resource is generally an external threat against public cloud services. However, the threat can impact all cloud service models as external and internal threat agents could introduce application or hardware components that cause a denial of service.
c. ***Physical disruption:*** The threat of disruption to cloud services caused by physical access is different between large cloud service providers and their customers. These providers should be experienced in securing large data center facilities and have considered resilience among other availability strategies. There is a threat that cloud user infrastructure can be physically disrupted more easily whether by insiders or externally where less secure office environments or remote working is standard practice.
d. ***Exploiting weak recovery procedures:*** The threat of inadequate recovery and incident management procedures being initiated is heightened when cloud users consider recovery of their own in house systems in parallel with those managed by third party cloud service providers. If these procedures are not tested then the impact upon recovery time may be significant.

Many of the security threats and challenges in cloud computing will be familiar to organizations managing in house infrastructure and those involved in traditional outsourcing models. Each of the cloud computing service delivery models' threats result from the attackers can be divided into two groups.

Internal attackers: The characteristics of an internal attacker are:

- He/ She is hired by the cloud service provider, other third party provider organization or customer supporting the operation of a cloud service.
- May have existing authorized access to cloud services, customer data or supporting infrastructure and applications, depending on their organizational role
- Uses existing privileges to gain further access or support third parties in executing attacks against the confidentiality integrity and availability of information within the cloud service.

External attackers: The characteristics of an external attacker are:

- Is not employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service
- Has no authorized access to cloud services, customer data or supporting infrastructure and applications
- Exploits technical, operational, process and social engineering vulnerabilities to attack a cloud service provider, customer or third party supporting organization to gain further access to propagate attacks against the confidentiality, integrity and availability of information within the cloud service.

CONCLUSION

Although cloud computing has many advantages, there are still many actual problems that need to be solved. The major issue for cloud computing model is providing Data security as it uses the idea of sharing of resources. According to service delivery models, deployment models and essential features of the cloud computing, data security and privacy protection issues are the primary problems that need to be solved as soon as possible. Cloud service providers need to inform their customers on the level of security that they provide on their cloud. In this paper, we first discussed various models of cloud computing, security issues. There are several other security challenges including security aspects of network and virtualization. This paper has highlighted all these issues of cloud computing. We believe that due to the complexity of the cloud, it will be difficult to achieve end-to-end security. New security techniques need to be developed and older security techniques needed to be radically improved to be able to work with the clouds architecture.

References

[1] Security and Privacy Issues in Cloud Computing, Jaydip Sen Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA

[2] *Security and Privacy in Cloud Computing*, Zhifeng Xiao and Yang Xiao, Senior Member, IEEE, IEEE Communications Surveys & Tutorials, Vol. 15, No. 2, Second Quarter 2013

[3] *Security and Privacy in Cloud Computing: Vision, Trends, and Challenges*, Zahir Tari, Xun Yi, Uthpala S.

Premarathne, Peter Bertok, and Ibrahim Khalil, RMIT University

[4] *Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions*, Sultan Aldossary*, William Allen, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016 485 | P a g e www.ijacsa.

[5] *Data Security and Privacy Protection Issues in Cloud Computing*, Deyan Chen1, Hong Zhao1,2 2012 International Conference on Computer Science and Electronics Engineering

[6] *Cloud Security Issues*, B. R. Kandukuri, R. Paturi V, A. Rakshit, In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[7] *The NIST Definition of Cloud Computing*, Peter Mell, and Tim Grance, Version 15, 10-7-09, http://www.wheresmyserver.co.nz/ storage/media/faq-files/cloud-def-v15.pdf.

[8] *Cloud computing security*, http://en.wikipedia.org/wiki/Cloud_computing_security.