www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 1, Jan 2014 Page No. 3643-3651

Network Security: Security in Cloud Computing

Mr. Vikas Malik, Srishti Gupta, Jyoti Kaushik
Computer Science and Engineering
(Network Security)
India

Abstract— This paper presents a survey on Security in Cloud Computing. This discussion is centered on overview of Cloud Computing threats, issues, security in cloud communication, infrastructure security, management in cloud. Cloud computing as we know is envisioned of the next-generation technology of IT industry. Cloud computing can be used by a prospective Cloud service for analyzing the data security risk before putting the confidential data into a cloud computing environment.

Keywords— SaaS, PaaS, IaaS

Introduction

Cloud Computing is a natural evolution of the widespread adoption of the Virtualization. It promises not just cheaper IT, but also faster, easier, more flexible, and more effective IT. Broadly we can define cloud as- A 'cloud' is an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple aspects for a specified level of Quality of Service (QoS) [1].

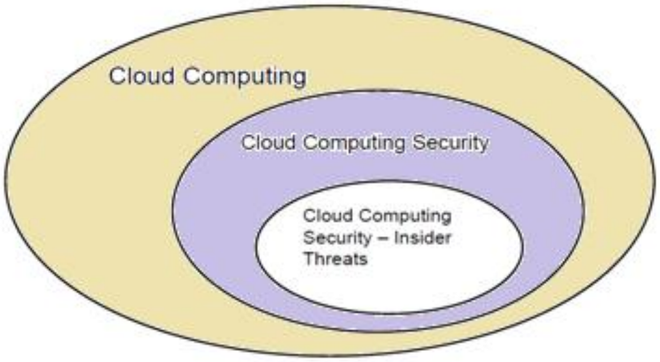

Fig 1: Scope of Cloud Computing Security

There is a critical need to store, manage, share and analyze huge amounts of complex (e.g., semi-structured and unstructured) data in a secure fashion in order to determine patterns and trends in order to improve the quality of healthcare, better safeguard the nation and explore alternative energy. Because of the critical nature of the applications, it is important that clouds be secure. The major security challenge with clouds is that the owner of the data may not have control of where the data is placed. This is because if one wants to exploit the benefits of using cloud computing, one must also utilize the resource allocation and scheduling provided by clouds. We need to protect our data from the un trusted users.

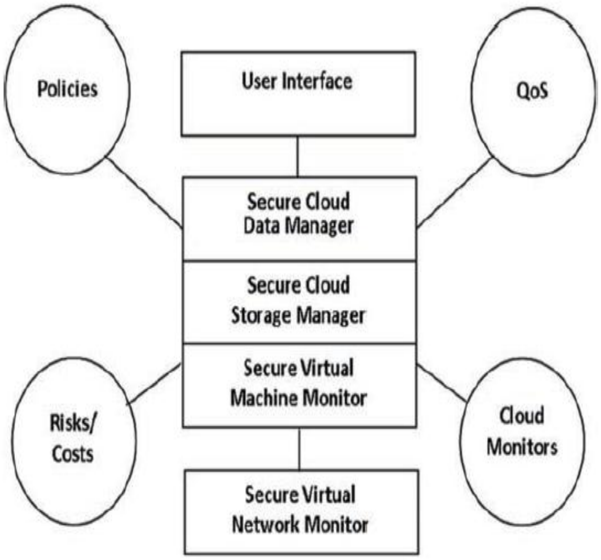
Policies
User Interface
QoS
Secure Cloud Data Manager
Secure Cloud Storage Manager
Secure Virtual Machine Monitor
Risks/ Costs
Cloud Monitors
Secure Virtual Network Monitor

Fig 2: Layered framework for assured cloud.

I. Security In Cloud

If we wish to enable cloud-driven growth and innovation through security, we must have a clear framing on what is meant by security. Security has been hard to define in the general. The canonical goals of information security are Confidentiality, Integrity, and Availability.

Let us discuss the few examples of how they can be supported by both technical and non-technical mechanisms.

1. **Confidentiality** refers to keeping data private. Confidentiality is supported by technical tools such as encryption and access control, as well as legal protections.
2. **Integrity** is a degree confidence that the data in the cloud is what is supposed to be there, and is protected against accidental or intentional alteration without authorization. Integrity is supported by well audited code, well-designed distributed systems, and robust access control mechanisms.
3. **Availability** means being able to use the system as anticipated. Availability is supported by capacity building and good architecture as well as well-defined contracts and terms of agreement.
4. **Accountability** maps actions in the system to responsible parties. Accountability is supported by robust identity, authentication and access control, as well as the ability to log transactions and then, critically, audit these logs.
5. **Assurance** refers to the need for a system to behave as expected. Assurance is supported by a trusted computing architecture in the cloud, and a by careful processes mapping from business case to technical details to legal agreements.
6. **Resilience** in a system allows it to cope with security threats, rather than failing critically. Resilience is supported by redundancy, diversification and real-time forensic capacity.

II. Cloud Service Threats

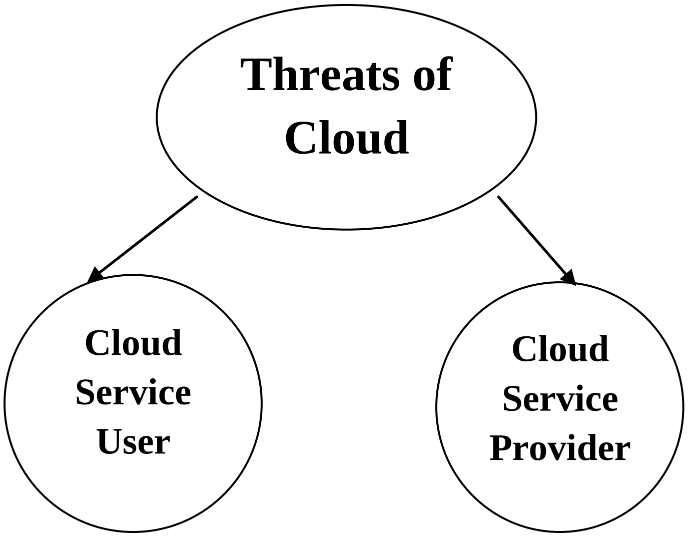

Fig 3: Classification of Cloud Service Threats

A.) Cloud Service User:

- Responsibility Ambiguity
- Loss of Governance
- Loss of Trust
- Service Provider Lock-in
- Unsecure Cloud Service User Access
- Lack of Information/Asset Management
- Data loss and leakage

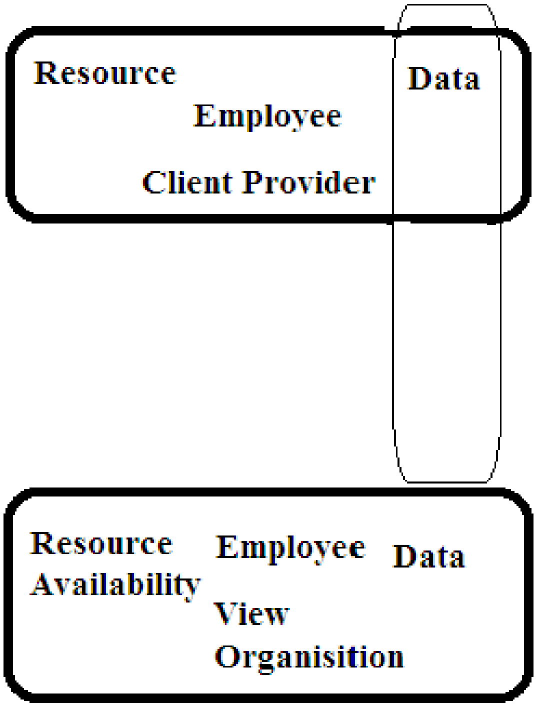

Fig 4: Provider /User Relationship

B.)Cloud Service Provider:

- Protection Inconsistency
- Responsibility Ambiguity
- Evolutional Risks
- Business Discontinuity
- Supplier Lock-in
- License Risks
- Bylaw Conflict
- Bad Integration

III. Security Issues Of Cloud

Security issues come under both technical and socio-technical in origin. The Cloud Security Alliance1 is a non-profit organization that seeks to promote the best practices for providing security assurance within the cloud computing landscape.

Various issues are:

1. Abuse and Nefarious Use of Cloud Computing
2. Insecure Application Programming Interfaces
3. Malicious Insiders
4. Shared Technology Vulnerabilities
5. Data Loss/Leakage
6. Account, Service and Traffic Hijacking
7. Unknown Risk Profile

Categorize the Security Concerns as:

1. Traditional security
2. Third-party data control

1. Traditional Security:

These concerns involve computer and network intrusions or attacks that will be made possible or at least easier by moving to the cloud. Cloud providers respond to these concerns by arguing that their security measures and processes are more mature and tested than those of the average company. Another argument, made by the Jericho Forum [2], is: "It could be easier to lock down information if it's administered by a third party rather than in-house, if companies are worried about insider threats… In addition, it may be easier to enforce security via contracts with online services providers than via internal controls."

2. Third-party data control:

The legal implications of data and applications being held by a third party are complex and not well understood. There is also a potential lack of control and transparency when a third party holds the data. Part of the hype of cloud computing is that the cloud can be implementation independent, but in reality regulatory compliance requires transparency into the cloud.

In order to increase the resource utilization, the cloud computing stores the data at remote site. Then it is need to secure our data and available to only authorized users. It needs to secure third party publication of data that is necessary for outsourcing as well as external publication.

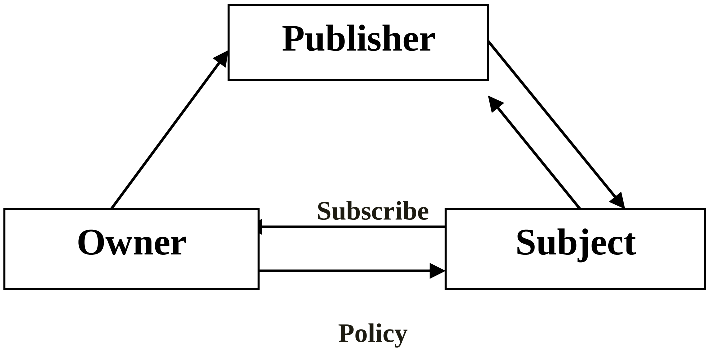

Fig 5: Secure Third Party Publication

IV. Security In Cloud Communication

Security can be classified into two ways: Intra cloud communication and Inter cloud Communication.

A.) Intra Cloud Communication

Intra-cloud communication is secured from outside threats, there are still prevailing security risks due to the following:

- The transferred business data between two services could potentially be 'visible' to the cloud provider.

• It is possible for a malicious neighbor instance within the same physical machine or LAN to snip the transferred business data. [3]

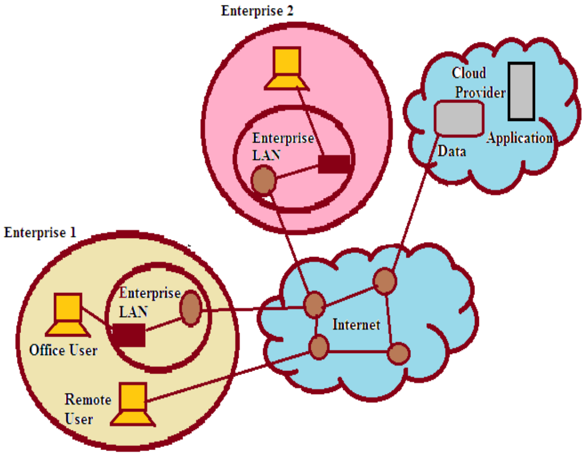

Fig 6: Security Model In Cloud Computing

B.) Inter Cloud Communication

Inter cloud – "the cloud of clouds". Name derived from the Internet (network of networks). It does not dictate the internal organization or structure used inside of a cloud (intra cloud), but rather only the connection between clouds. It coordinates the delivery of ubiquitous and interoperable services for content, storage, computation, etc It relies on the generation, maintenance and usage of gathered information about the federated clouds. It create among federated clouds common: naming, addressing, Identity, trust, presence, messaging, multicast, time domain and application messaging.[4]

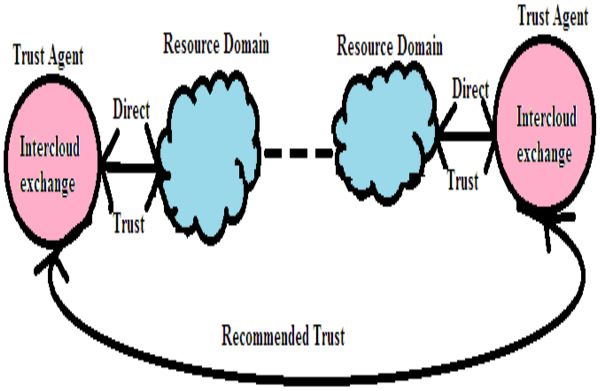

Fig7: Inter Cloud Communication

V. Security In SPI Model

1. **Software as a Service (SaaS):** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).

2. **Platform as a Service (PaaS):** The capability provided to the consumer is to deploy onto the cloud infrastructure his own applications without installing any platform or tools on their local machines. PaaS refers to providing platform layer resources, including operating system support and software development frameworks that can be used to build higher-level services.

3. **Infrastructure as a Service (IaaS):** The capability provided to the consumer is to provision processing, storage, networks, and

other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

VI. Cloud Computing Infrastructure Security

1. Infrastructure Security at the Network Level
2. Infrastructure Security at the Host Level
3. Infrastructure Security at the Application Level
4. Note: We will examine IaaS, PaaS and SaaS Security issues at Network, Host and Application Levels.

Security in Network Level:

1. Ensuring data confidentiality and integrity of the organizations data in transit to and from the public cloud provider.
2. Ensuring proper access control (Authentication, Authorization, Auditing) to resources in the public cloud.
3. Ensuring availability of the Internet facing resources of the public cloud used by the organization.
4. Replacing the established network zones and tiers with domains.[5]

Security in Host Level:

1. Host security at PaaS and SaaS Level
   - Both the PaaS and SaaS hide the host operating system from end users
   - Host security responsibilities in SaaS and PaaS are transferred to CSP
2. Host security at IaaS Level
   - Virtualization software security
     1. Hypervisor security
     2. Threats: Blue Pill attack on the hypervisor
   - Customer guest OS or virtual server security
     1. Attacks to the guest OS: e.g., stealing keys used to access and manage the hosts.

Security in Application Level:

1. Usually it’s the responsibility of both the CSP and the customer.
2. Application security at the SaaS level.
   - SaaS Providers are responsible for providing application security.
3. Application security at the PaaS level.
   - Security of the PaaS Platform.
   - Security of the customer applications deployed on a PaaS platform.
4. Application security at the IaaS Level.
   - Customer applications treated a black box.
   - IaaS is not responsible for application level security.[5]

VII. Cloud Storage And Data Security

1. **Aspect of Data Security**
   - Security for

   a. Data in transit

   b. Data at rest

c. Processing of data including multi tenancy

d. Data Lineage

e. Data Provenance

f. Data remnance

- Solutions include encryption, identity management, sanitation.

2. Data Security Mitigation

- Even through data in transit is encrypted, use of the data in the cloud will require decryption.i.e., cloud will have unencrypted data
- Mitigation
  -Sensitive data cannot be stored in a public cloud
  -Homomorphic encryption may be a solution in the future.

3. **Provider Data and its Security**

1. Provider collects the data in the form of meta data.

2. Data security issues includes the : Access control, Key management are used for encrypting the data.

3.Confidentiality, Integrity and Availability are objectives of data security in the cloud.

VIII. Security Management In Clouds

1. **Security Management Standards**: Security of information is becoming a serious matter over the internet. There are number of security standards developed which are used in conventional computing.

a. ISO 27001 (BS ISO/IEC 27001:2005, BS 7799-2:2005)

This standard which was formerly was known as BS 7799-2, is intended to “provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system (ISMS)” (BSI, 2005 a).[6]

b. ISO 27002 (BS ISO/IEC 27002:2005, BS 7799-1:2005, BS ISO/IEC 17799:2005)

This standard is an auxiliary standard to ISO 27001. It establishes the “guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organization” (BSI, 2005 b). It purpose is stated as “provide general guidance on the commonly accepted goals of in format ion security management” (BSI, 2005 b). The objectives and controls in this standard are expected to meet the requirements identified during risk assessment when implemented.[6]

c. ITIL (Information Technology Infrastructure Library) and ISO 27001/27002

2. Management of security in cloud:

1. Availability Management (ITIL)

2. Access Control (ISIO, ITIL)
3. Vulnerability Management (ISO, IEC)
4. Patch Management (ITIL)
5. Configuration Management (ITIL)
6. Incident Response (ISO/IEC)
7. System use and Access Monitoring

3. **Access Control Management in Cloud:** The access is control in the cloud by considering certain question in our mind. These question are:

1. Who should have access and why?
2. How is a resources accessed?
3. How is the access monitored?
4. Impact of access control of SaaS, PaaS and IaaS?

IX. Future Aspects For Security In Cloud

Future Threats

- Encryption
- Supply chain
- Targeted attacks – corporate espionage Provider collusion

Future Research

- Measurement/metrics
- Forensics
- Incident Response
- SLA enforcement
- Isolation
- Attack vectors
- CSA Reference Architecture

X. Conclusion

Cloud computing has a dynamic nature that is flexible, scalable and multi-shared with high capacity that gives an innovative shape of carrying out business Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down its use.. Cloud fears largely stem from the perceived loss of control of sensitive data. Current control measures do not adequately address cloud computing’s third-party data storage and processing needs. In our vision, we propose to extend control measures from the enterprise into the cloud through the use of Trusted Computing and applied cryptographic techniques. These measures should alleviate much of today’s fear of cloud computing, and, we believe, have the potential to provide demonstrable business intelligence advantages to cloud participation. A secure cloud computing environment depends on identifying security solutions. A deeper study on current security approaches to deal with different security issues related to the cloud should be the focused of future work.

References:

[1] By “The Future Of Cloud Computing Opportunity For European Cloud Computing2010”,Expert Group report Publisher version 1.0,Rapporteur: Lutz Schubert.

[2] Don’t cloud your vision. http://www.ft.com/cms/s/0/303680a6-bf51-11dd-ae63-0000779fd18c.html?nclick_check=1.

[3] By “ Secure Connectivity for Intra-Cloud and Inter-Cloud Communication**”** Shiping Chen and Surya Nepal, Information Laboratory, CSIRO ICT Centre, Sydney, Australia.

[4] “Inter Cloud Security” By William Strickland, COP 6938 Fall 2012, University of Central Florida, 10/08/2012.

[5] “A Comprehensive Overview of Secure Cloud Computing” By Dr. Bhavani Thuraisingham , November, 2012.

[6] “Cloud Computing: Strategies for Cloud Computing Adoption” By Faith ShimbaDublin Institute of Technology, faith.shimba@gmail.com