International Journal of Scientific Research in Computer Science and Engineering

Review Paper
Volume-1, Issue-1, Jan- Feb-2013
Available online at www.isroset.org

Study of Threats, Risk and Challenges in Cloud Computing

Rajesh Piplode[#1], Pradeep Sharma[#2] and Umesh Kumar Singh[#3]
[#1]Department of Computer Science, Govt. Holkar Science College Indore, India
[#3]Institute of Computer Science, Vikram University, Ujjain, India

***Abstract*—Cloud computing security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. In this paper we present security issues that fetch by cloud computing technology and also analysis the threats, risk and challenges in cloud environment.**

***Keywords*- Cloud Computing, Security Risk, Service Models, Deployment Models**

I. INTRODUCTION AND BACKGROUND

The National Institute of Standards and Technology (NIST) Information Technology Laboratory, cloud computing is defined as follows:

"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, 2, 3].

Essential Characteristics

- On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- Measured Service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

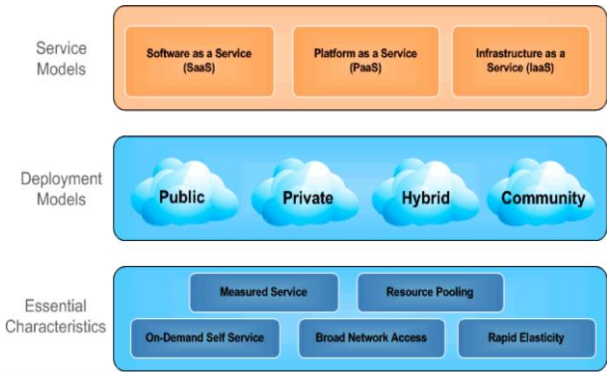

Fig. 1 Cloud Computing Framework

Service Models:

- Cloud 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). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported

Corresponding Author: P Sharma,psharma29762@gmail.com

by the provider. 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.

- Cloud 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. 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).

Deployment Models:

- Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

II. RELATED WORK

Cloud computing is a current technology. There are many researchers they are doing research in the field of cloud computing. This section present the related work of this research work.

In [4], K.Mukherjee and G.Sahoo, have discuss about cloud computing is computing over a cloud; where cloud consists of grids of commodity machine and software layer(Called Hadoop). Hadoop is a new framework for secured use of cloud computing, which is responsible for distributing applications data across the machines, parallelizing and managing application execution across the machines, and detecting and recovering from machine failures. they purpose that Hadoop which consisting of for component each of the component have specific job(see figure 2).

Figure 2 Components of Hadoop

Where

- U.I is User Interface.
- A.C is Authentication Check.
- W.S.M is Computational Web Service Mapping
- J.S is Job Scheduler.

Whenever the user requests for a web service to Hadoop, the latter checks the authenticity of the user after interfacing with "Authentic Server" then Hadoop refers to "Web Service Mapping" and maps to web services existing at different locations and fetches the required webservice from it and submits it to "Job scheduler" of Hadoop which schedules the jobs to the Grid of volunteer commodity hardware.

Kresimir Popovic, Zeljko Hocenski, "Cloud computing security issues and challenges", In [5], they discussed about the security issues, requirements and challenge that cloud service provider (CSP) face during cloud engineering and also recommended security standard and management model to address these are suggested for technical business community. Security management models section describes twenty recommended security management models and their requirements for cloud computing that cloud service providers should definitely consider as they develop or refine their compliance programs.

In [6], that discussed about the cloud computing security (some time that refers to cloud security). It is a sub-domain of computer security, network security or information security and it refers to a broad set of polices, technologies and the associate infrastructure of cloud computing.

In [7], research paper "On Technical Security Issues in Cloud Computing" that focus on technical security issues arising from the usage of cloud services. Here they also discuss about Web Service Security (WS Security) and Transport Layer Security (TLS).

In [8] Rituik Dubey, Muhammad Asim Jamshed, Xiaohui Wang, Rama Krishna Batalla, "Addressing Security Issues in Cloud Computing" that discussed several security issues in the cloud computing that includes the metering problems (The metering problem arises when a cloud computing service is being used as a huge search database. A client making a search query may hold reservations whether the server performed a complete search, scanning the table(s) in entirety before returning the results to the client) and the problem of data backup.

In [9], Shilpashree Srinivasamurthy, David Q. Liu, " Survey on Cloud Computing Security" this research paper discussed about cloud computing open secure architecture advantages in brief and emphasize on various security threats in cloud computing which includes seven security threads given by CSA (Cloud Security alliance) and other security threads given in [10,11].

III. CLOUD COMPUTING SECURITY THREATS

Top seven security threats to cloud computing discovered by Cloud Security Alliance (CSA) are [12]:

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.

Suggested remedies by the CSA to lessen this threat:

- Stricter initial registration and validation processes.
- Enhanced credit card fraud monitoring and coordination.
- Comprehensive introspection of customer network traffic.
- Monitoring public blacklists for one's own network blocks.

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.

Suggested remedies by CSA to lessen this threat:

- Analyze the security model of cloud provider interfaces.
- Ensure strong authentication and access controls are implemented in concert with encrypted transmission.
- Understand the dependency chain associated with the API.

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.

Suggested remedies by CSA to lessen this threat:

- Enforce strict supply chain management and conduct a comprehensive supplier assessment.
- Specify human resource requirements as part of legal contracts.
- Require transparency into overall information security and management practices, as well as compliance reporting.
- Determine security breach notification processes.

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.

Suggested remedies by CSA to lessen this threat:

- Implement security best practices for installation.
- Monitor environment for unauthorized changes/activity.
- Promote strong authentication and access control for administrative access and operations.
- Enforce service level agreements for patching and vulnerability remediation.
- Conduct vulnerability scanning and configuration audits.

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.

Suggested remedies by CSA to lessen this threat:

- Implement strong API access control.
- Encrypt and protect integrity of data in transit.
- Analyze data protection at both design and run time.
- Implement strong key generation, storage and management, and destruction practices.
- Contractually demand providers to wipe persistent media before it is released into the pool.
- Contractually specify provider backup and retention strategies.

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.

Suggested remedies by CSA to lessen this threat:

- Prohibit the sharing of account credentials between users and services.
- Leverage strong two-factor authentication techniques where possible.
- Employ proactive monitoring to detect unauthorized activity.
- Understand cloud provider security policies and SLAs.

Unknown Risk Profile:

Security should always in the upper portion of the priority list. Code updates, security practices, vulnerability profiles, intrusion attempts – all things that should always be kept in mind.

Suggested remedies by CSA to lessen this threat:

- Disclosure of applicable logs and data.
- Partial/full disclosure of infrastructure details (e.g., patch levels, firewalls, etc.).
- Monitoring and alerting on necessary information.

IV. SOME OTHER SECURITY THREATS

Failures in Providers Security: Cloud providers control the hardware and the hypervisors on which data is stored and applications are run and hence their security is very important while designing cloud [13].

Attacks by other customer: If the barriers between customers break down, one customer can access another customer's data or interfere with their applications [14].

Availability and reliability issues: The cloud is only usable through the Internet so Internet reliability and availability is essential [14].

Legal and Regulatory issues: The virtual, international nature of cloud computing raises many legal and regulatory issues regarding the data exported outside the jurisdiction [13][14].

Perimeter security model broken: Many organizations use a perimeter security model with strong security at the perimeter of the enterprise network. The cloud is certainly outside the perimeter of enterprise control but it will now store critical data and applications [14].

Integrating Provider and Customer Security Systems: Cloud providers must integrate with existing systems or the bad old days of manual provisioning and uncoordinated response will return [13] [14].

V. VULNERABILITIES IN CLOUD COMPUTING

Security is the most important issue in vulnerabilities cloud Cloud computing shares in common with other network-based

application, storage and communication platforms certain vulnerabilities in several broad areas:

- *Web application vulnerabilities*, such as cross-site scripting and sql injection (which are symptomatic of poor field input validation, buffer overflow; as well as default configurations or mis-configured applications.
- *Accessibility vulnerabilities*, which are vulnerabilities inherent to the TCP/IP stack and the operating systems, such as denial of service and distributed denial of services [15]
- *Authentication of the respondent device or devices*. IP spoofing, RIP attacks, ARP poisoning (spoofing), and DNS poisoning are all too common on the Internet. TCP/IP has some unfixable flaws such as trusted machine status of machines that have been in contact with each other, and tacit assumption that routing tables on routers will not be maliciously altered.
- *Data Verification*, tampering, loss and theft, while on a local machine, while in transit, while at rest at the unknown third-party device, or devices, and during remote back-ups.
- *Physical access issues*, both the issue of an organization's staff not having physical access to the machines storing and processing a data, and the issue of unknown third parties having physical access to the machines
- *Privacy and control issues* stemming from third parties having physical control of a data is an issue for all outsourced networked applications and storage, but cloud architectures have some specific issues that are distinct from the usual issues. Christodorescu, et al. show a significant gap between what is assumed and what is reality, i.e., all virtual machines are brought into existence clean, when in reality a compromised hypervisor can spawn compromised VMs, or all VM operating systems are known and available for audit, when in reality the Windows source-code, among others, is not available for audit [16].

VI. TOP SECURITY RISK IN CLOUD

The most important classes of cloud-specific risks identified in this section are:

Loss of governance: In using cloud infrastructures, the client necessarily cedes control to the Cloud Provider (CP) on a number of issues which may affect security. At the same time, SLAs may not offer a commitment to provide such services on the part of the cloud provider, thus leaving a gap in security defenses.

Lock -in: There is currently little on offer in the way of tools, procedures or standard data formats or services interfaces that could guarantee data, application and service portability. This can make it difficult for the customer to migrate from one provider to another or migrate data and services back to an in-house IT environment. This introduces a dependency on a particular CP for service provision, especially if data portability, as the most fundamental aspect, is not enabled.

Isolation failure: Multi-tenancy and shared resources are defining characteristics of cloud computing. This risk category covers the failure of mechanisms separating storage, memory, routing and even reputation between different tenants (e.g., so-called guest-hopping attacks). However it should be considered that attacks on resource isolation mechanisms (e.g.,. against hypervisors) are still less numerous and much more difficult for an attacker to put in practice compared to attacks on traditional Oss[17]. Compliance risk: Investment in achieving certification (e.g., industry standard or regulatory requirements) may be put at risk by migration to the cloud:

- If the CP cannot provide evidence of their own compliance with the relevant requirements
- If the CP does not permit audit by the cloud customer (CC).

In certain cases, it also means that using a public cloud infrastructure implies that certain kinds of compliance cannot be achieved (e.g., PCI DSS (4)).

Management interface compromise: Customer management interfaces of a public cloud provider are 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 customers and providers. In some cases, it may be difficult for the cloud customer (in its role as 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 clouds. On the other hand, some cloud providers do provide information on their data handling practices. Some also offer certification summaries on their data processing and data security activities and the data controls they have in place, e.g., SAS70 certification.

Insecure or incomplete data deletion: When a request to delete a cloud resource is made, as with most operating systems, this may not result in true wiping of the data. Adequate or timely data deletion may also be impossible (or undesirable from a customer perspective), either because extra copies of data are stored but are not available, or because the disk to be destroyed also stores data from other clients. In the case of multiple tenancies and the reuse of hardware resources, this represents a higher risk to the customer than with dedicated hardware.

Malicious insider: While usually less likely, the damage which may be caused by malicious insiders is often far greater. Cloud architectures necessitate certain roles which are extremely high-risk. Examples include CP system administrators and managed security service providers [17].

VII. CONCLUSION

Cloud computing introduces new security threats and vulnerabilities that are not present in traditional IT environments. Current IaaS technologies lack adequate security mechanisms to handle these new threats and risks, potentially exposing information stored in the cloud to the service providers, attackers with Internet access, and all the other users of the cloud. In this research work we totally analyze security threats, risk and challenges in cloud computing technology.

REFERENCES

[1] National Institute Of Standard and technology **(2009).** www.csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc,

[2] Open Security Architecture http://www.opensecurityarchitecture.org/

[3] Tim Mather, Subra Kumaraswamy, Shahed Latif Cloud Security and Privacy : An Enterprise perspective of Risks

[4] K.Mukherjee , G.Sahoo, "A Secure Cloud Computing", Proc. **2010** International Conference on Recent Trends in Information, Telecommunication and Computing

[5] Krešimir Popović, Željko Hocenski, "Cloud computing security issues and challenges" Proc. MIPRO 2010, May **24-28, 2010**, Opatija, Croatia

[6] Cloud computing security retrived from http://en.wikipedia.org/wiki/Cloud_computing_security

[7] Meiko Jensen, J¨org Schwenk, Nils Gruschka, Luigi Lo Iacono " On Technical Security Issues in Cloud Computing" **2009** IEEE International Conference on Cloud Computing.

[8] Rituik Dubey, Muhammad Asim Jamshed, Xiaohui Wang, Rama Krishna Batalla "Addressing Security Issues in Cloud Computing".

[9] Shilpashree Srinivasamurthy, David Q. Liu, " Survey on Cloud Computing Security".

[10] Salesforce, Salesforce.com, **2010**

[11] Windows Azure, www.microsoft.com/azure, **2010**

[12] Security Guidance for Critical Areas of Focus in Cloud Computing, April **2009**. www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[13] Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, Ryusuke Masuoka, Jesus Molina. Controlling Data in the Cloud Outsourcing Computation without Outsourcing Control. CCSW '09: Proceedings of the **2009** ACM workshop on Cloud computing security, pages **85-90**. November **2009**.

[14] Steve Hanna. A security analysis of Cloud Computing. Cloud Computing Journal. www.cloudcomputing.sys-con.com/node/1203943 .

[15] Matthew Glotzbach, Product Management Director, Google Enterprise, "What We Learned from 1 Million Businesses in the Cloud," www.googleblog.blogspot.com/2008/10/whatwe-learned-from-1-illion.html, 30 Oct **2008.**

[16] KrÃ¼gel, C., Toth, T., & Kirda, E. (**2002**). Service specific anomaly detection for network intrusion detection. In Proceedings of the 2002 ACM symposium on Applied computing (pp. **201-208**). Madrid, Spain: ACM. Retrieved from www.portal.acm.org.library.capella.edu/citation.cfm?id=508835&dl=GUIDE&coll=GUIDE&CFID=80867670&CFTOKEN=24312614

[17] Shivlal Mewada, Umesh Kumar Singh, Pradeep Sharma,"Security Based Model for Cloud Computing", IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol. 1, No. 1, pp(**13-19**), December **2011**. http://www.iracst.org/ijcnwc/vol1no1.htm)

AUTHORS PROFILE

Rajesh Piplode has received his Master of Philosophy in Computer Science (M.Phil.-CS) from Institute of Computer Science, Vikram University. He is presently working as Guest lecturer in Department of Computer Science, Govt. Holkar (Autonomous) Science Collage, Indore - India. His research interest includes Security in-Cloud computing, Wireless Mesh Network and Information Technology based education.

Dr. Pradeep Sharma obtained his Ph.D. in Physics from Vikram University, Ujjain -INDIA. He is currently Professor and Head of department, (HOD) in Department of Computer Science, Govt. Holkar (Autonomous) Science College-INDIA. He has 28 year teaching exceprience in college level. His various research papers are published in national and international journals of repute. His various paper published in national and international conferences His researh interest includes X-ray spectroscopy, Networking.

Dr. Umesh Kumar Singh obtained his Ph.D. in Computer Science from Devi Ahilya University, Indore-INDIA. He is currently Reader (Director) in Institute of Computer Science, Vikram University, Ujjain-INDIA. He served as professor in Computer Science and Principal in Mahakal Institute of Computer Sciences (MICS-MIT), Ujjain. He is formally Director I/C of Institute of Computer Science, Vikram University Ujjain. He has served as Engineer (E&T) in education and training division of CMC Ltd., New Delhi in initial years of his career. He has authored a book on "Internet and Web technology "and his various research papers are published in national and international journals of repute. Dr. Singh is reviewer of International Journal of Network Security (IJNS), IJCSIS, ECKM Conferences and various Journals of Computer Science. His research interest includes network security, secure electronic commerce, client-server computing and IT based education.