**Challenges in Migration to Cloud**

Amar Kumar Choudhary

GM- Sales

IWG Group, Pune, India

amarchoudhary97@gmail.com

MIT UNIVERSITY, School Of Management

**Abstract**

**Cloud computing is an Internet-accessible business model with flexible and multiple resource allocation on demand and it works on pay-per-use model. The most important issue is related to security and privacy subjects in cloud-based environments. This paper presents a review on the challenges and issues of Cloud computing. We will identify numerous challenges from the Cloud computing implementation perspective and we will highlight the Cloud interoperability issue that deserves significant further research and development.**

***Keywords: Cloud computing, Issues in cloud, Service-Oriented Computing,******Security challenges, Virtualization, Web Service Security.***

1. **INTRODUCTION**

Cloud computing is a continuously developing and Delivering excellent promising technology. It has awakened the concern of the computer society of whole world. It is Internet-based computing, whereby shared information, resources, and software, are provided to terminals and portable devices on-demand, like the energy grid and using the advanced deployment models like SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service), HaaS (Hardware as a Service) to distribute the powerful computing capacity to end-users. While it is important to take advantages of could base computing by means of deploying it in diversified sectors, the security aspects in a cloud based computing environment remains at the core of interest. Cloud based services and service providers are being evolved which has resulted in a new business trend based on cloud technology. What are those general challenges and issues for both cloud providers and consumers? While answering these questions, we will aim to define key research issues and articulate future research challenges for cloud computing.

1. **Cloud computing framework**

**2.1 Service models**

The NIST (National Institute of Standards and Technology) divides the services provided by the cloud computing in below three categories,

(a) Software as a service (SaaS)

 (b) Platform as a service (PaaS)

 (c) Infrastructure as a service (IaaS).

The cloud service model is referred to as SPI (software, platform, and infrastructure).

**Software as a service (SaaS)**

The SaaS enables the customers to use CSP’s applications, which runs on the cloud infrastructure, through the Internet. The thin client interface can be used to access the applications such as web browser. Though SaaS one cannot create an application or software. The SaaS only provides software through Internet building it a model to allocate the software through Web. The customers pay for the usage and do not own the software.

**Platform as a service (PaaS)**

Applications that are owned by the customer need a groundwork where it can be executed and managed. It includes integrated development environments (IDE), operating systems, and platform layer resources, etc. The above-mentioned services are provided as PaaS. The PaaS does not provide customers with the control over the fundamental cloud infrastructure but only on the applications that are moved to the cloud.

**Infrastructure as a service (IaaS)**

The IaaS refers to the hardware infrastructure provided by the CSP including the network, storage, memory, processor, and various other computing resources. These resources are provided in the form of virtualized systems and accessible through Internet. The CSP has a control over the primary resources.

**2.2 Deployment models**

There are four models that can be used to deploy a cloud computing infrastructure,

(a) Private cloud

(b) Public cloud

(c) Community cloud

(d) Hybrid cloud.

**Private cloud:**

Cloud that is run and managed only for a single organization is the private cloud. Organization may or may not own the physical infrastructure and can be managed by the organization itself or by a third party. Also, private cloud may or may not be located at organization’s geographical site. Though, private cloud is for the use of only single organization and mentioned resources are not utilized by any other customer.

**Public cloud:**

The cloud’s physical infrastructure is owned by the Cloud provider and is open to all organizations. The mentioned resources are shared among all the customers. Customers pay the cloud owner as per the services and resources they use. The physical infrastructure is located off-site to the customers and is managed by the Cloud provider.

**Community cloud:**

Community cloud is shared by set of organizations forming a community. Normally, Community shares common interests, such as the mission, security requirements, policy, and compliance.

Community cloud could be managed by any of the organizations in the community. Also, it may be located on premise or off-premise.

**Hybrid cloud:**

Hybrid cloud is the mix of two or more clouds (public, private, or community). All of the contributing clouds retain their status of a unique entity, but share standardized or exclusive technology.

1. **Cloud security challenges**

Besides legal security desires, it is necessary to address some basic security desires like authentication, integrity, transparency, confidentiality, availability, audits, etc.

The Four levels of security namely are communication, computation, Data and service level agreement. Security issues in each level are also clearly described with further grouping.

The security risks in cloud may differ from the risks of orthodox IT infrastructure either in nature. Resource pooling permits the use of same pool by multiple users through multi-tenancy and virtualization technologies. Even though, these technologies present rapid elasticity and optimal management of resources, they also introduce certain risks in the system. Multi-tenancy leads to the risks of data visibility to other users and suggestion of processes.

On-demand self-service specific is provided to the customers by means of Web based management interfaces that causes the probability of unauthorized access to the management interface higher than the traditional systems. Likewise, virtualized environment introduces its own set of risks and vulnerabilities that includes malicious cooperation between virtual machines (VM) and VM escape. Also, from the cloud service model view point, the service models are dependent on each other. The SaaS applications are built and deployed over the PaaS and the PaaS is dependent primarily on IaaS.

Operational dependency of the service models on each other brings in the security dependency as well (e.g. if an attacker succeeds to take control of IaaS, the result will be a compromised PaaS that is utilizing IaaS. A compromised PaaS can lead to compromised SaaS). So the understanding is any compromised service model gives access to other layer of the service model. The private cloud deployment model inherits the same set of vulnerabilities as controlled by the orthodox IT infrastructure.

This is the reason private cloud is meant for the use of a single organization. The public, community, and hybrid clouds own more cloud specific vulnerabilities and risks due to presence of users from different origins and Management control of a third party. In the subsequent discussion we present the security challenges being faced by the cloud computing. There are numerous works that look upon the cloud security challenges from service model viewpoint.

In this paper we will go through the detail challenges on the cloud based on four abstract domains, namely:

 **(a) Communication issues**

 **(b) Computational issues**

 **(c) Data level issue**

 **(d) Contractual and legal issues**

Some of the technologies in cloud computing do not affect any specific service model. In its place more than one models become affected, such as, virtualization that can affect both the IaaS and PaaS. Therefore, we look at the challenges at abstract level regardless of the service model.

**3.1 Challenges at communication level**

The cloud infrastructure services are normally available to the customers through the Internet. Standard Internet protocols and mechanisms are used to communicate between the customers and the cloud. The communication process results in transmission of either data or information or applications between the customer and the cloud. Besides, there exists communication within cloud between VMs. We divide the cloud communication into two categories, mention as below:

1. Communication external to the cloud (between customers and cloud)
2. Communication internal to the cloud (communication occurring within cloud infrastructure).

The external communication of cloud is similar as any other communication over the Internet. Therefore the challenges faced by the cloud due to Internet characteristic are same as the challenges of traditional IT communication. These challenges include denial-of-service, man-in-the-middle, eavesdropping, IP-spoofing based flooding, masquerading, etc. The solutions to these challenges are also the same as employed traditionally, such as, Secure Socket Layer (SSL), Internet Security Protocol (IPSec), DDos, intrusion detection and prevention systems, traffic cleaning, etc. All these challenges and resolutions are integral from traditional IT infrastructure, we do not detail them in this study. We will focus on internal cloud communication that generates cloud specific challenges because of its specific characteristics and technologies.

**3.2 Challenges at Computational level**

Application of this concept of virtualization in the cloud is one of the biggest computational level challenges.

**3.2.1 Virtualization challenges**

1. VM cloning
2. VM isolation
3. VM migration

 4. VM Escape

 5. VM rollback

 6. VM sprawl

 7. VM Hopping/VM Hyper jumps

**3.2.2 Hypervisor level (Virtualization layer)**

1. Basic information security
2. Threats in virtual networking

 3. VM-to-VM attack

 4. Security issue with VM introspection

 5. Issues due to virtualized trusted computing (VTC)

 6. Hyperjacking / hypervisor subversion

 7. Issue due to resource sharing

**3.3 Challenges at Data level**

Data is the heart and the source of the entities of any cloud. Data breach was identified as the most serious threat. Prior to moving on to the new computing technology, there is an imperative need to have knowledge of the levels of security that the technology provides to the data predicted.

Storage of the data in some remote place and achieving multi-tenancy gives rise to an issue called Data Leakage.

The notable issues in cloud data security include data privacy, data protection, data availability, data location, and secure transmission. The security challenges in the cloud include threats, data loss, service disruption, outside malicious attacks, and multi tenancy issues. Privacy and data security issues in the cloud are on privacy protection, data segregation, and cloud security. Data security issues are primarily at SPI (SaaS, PaaS, and IaaS) level and the major encounter in cloud computing is data sharing.

Data security can be classified as data-in-transit and data-in-rest. Data-in-transit does not lead to additional security risks compared to data-in-rest, because, the transmission of data is done by default through TLS which provides a secured way of data transfer.

**3.4 Challenges at contractual and legal levels**

Implementing the cloud computing, results in moving the organizations data and applications to the Management control of CSP. It brings many issues such as performance assurance, regulatory laws compliance, geographic jurisdictions, monitoring of contract enforcement, etc. The abovementioned problems are related to the service level agreement (SLA), legalities, and physical locations of the data.

**3.4.1 Service Level Agreement**

Even though cloud consumers do not have control over the primary computing resources, they do need to ensure the quality, availability, reliability, and performance of these resources when consumers have migrate their core business functions onto their trusted cloud.

Typically, these are provided through SLA negotiated between the providers and consumers. The very first issue is the definition of SLA specifications in such a way that has an suitable level of granularity, namely the transactions between articulacy and complexity, so that they can cover most of the consumer expectations and is relatively simple to be weighted, verified, evaluated, and enforced on the cloud. In addition, different cloud offerings (IaaS, PaaS, SaaS, and DaaS) will need to define different SLA met specifications.

The resource managers need to work fast and effective decision models and optimization algorithms to do this. It possibly will need to reject certain resource requests when SLAs cannot be met. All these need to be carried out in a nearly systematic and automatic mode due to the promise of "self-service" in the cloud computing. Additionally, advanced SLA instruments need to constantly integrate user feedback and customization features into the SLA assessment frame.

1. **CLOUD INTEROPERABIOLITY ISSUE**

Presently, each cloud offering has its own way on how cloud clients, applications and users interact with the cloud. This harshly delays the development of cloud ecosystems by forcing vendor lock in, which prohibits the ability of users to choose from alternative vendors and offering simultaneously in order to optimize resources at different levels within an organization.

Moreover, registered cloud APIs makes it very difficult to integrate cloud services with an organization's own existing legacy systems. The scope of interoperability here states both to the links amongst different clouds and the connection between a cloud and an organization's local systems. The primary goal of interoperability is to realize the seamless fluid data across clouds and between cloud and local applications.

1. **Conclusion**

The several security issues in communication, computational and Service Level Agreement are explored. Both virtualization and data related security issues are considered to be the most vulnerable entity. Data related security issues are categorized as issues on data at rest and issues on data in transmission.

Currently, security challenges are numerous thus providing several opportunities for hackers. Cloud computing need to gain more trust specially in Banking segment, where several private or SBU are still not sure of moving to cloud because of security concern on data, privacy, etc.

**References**

[1] Mell P, Grance T. Version 15 The NIST definition of cloud computing October 7. National Institute of Standards and Technology; 2009http://csrc.nist.gov/groups/SNS/cloud-computing.

[2] Walker K. Cloud security alliance(CSA). The treacherous 12: cloud computing top threats in 2016. 2016. Feb. 29 <https://cloudsecurityalliance.org/media/news/cloud-security-alliance-releases-the-treacherous-twelve-cloud-computing-top-threats-in-2016/>.

[3] Kamara S, Lauter K. Cryptographic cloud storage. Microsoft Research Cryptography Group; January 2010http://research.microsoft.com/pubs/112576/cryptocloud.pdf.

[4] Rebollo O, Mellado D, Fernandez-Medina E, Mouratidis H. Empirical evaluation of a cloud computing information security governance framework. Inf Software Technol 2015;58:44–57www.elsevier.com/locate/infsof.

[5] Bhadauria R, Sanyal S. Survey on security issues in Cloud Computing and Associated Mitigation Techniques. Int J Comput Appl (0975-888) June 2012;47(18).

[6] Laniepce S, Lacoste M, Kassi-Lahlou M, Bignon F, Lazri K, Wailly A. Engineering intrusion prevention services for iaas clouds: the way of the hypervisor, 2013 IEEE seventh international symposium on service-oriented system engineering.

[7] Sabahi F. Secure virtualization for cloud environment using hypervisor-based technology. Int J Mach Learn Comput February 2012;2(1).

 [8] Wei L, Zhu H, Cao Z, Dong X, Jia W, Chen Y, Vasilakos AV. Security and privacy for storage and computation in cloud computing. Inf Sci 2014;258:371–86www.

elsevier.com/locate/ins.

[9] Qin Z, Zhang Q, Wan C, Di Y. State-of-the-art virtualization security in cloud computing. J Inf Comput Sci 2012;9(6):1487–97http://www.joics.com.

[10] Nawaz Brohi S, Adib Bamiah M, Nawaz Brohi M, Kamran R. Identifying and analyzing security threats to virtualized cloud computing infrastructures, In Proceedings of 2012 international of cloud computing, technologies, applications and management.

 [11] Miller CD. Associate in AMI- partners. Secuirty in the cloud: concern/excitement?, on July 10th. 2012http://www.ami-partners.com/blog.

[12] Wueest C, Barcena MB, O'Brien L. Mistakes in the Iaas cloud could put your data at risk. http://www.symantec.com/content/en/us/enterprise/media/security\_response/whitepapers/mistakes-in-the-iaas-cloud-could-put-your-data-at-risk.pdf; May 2015.

[13] Zissis D, Lekkas D. Addressing cloud computing security issues. Future Gener Comput Syst 2012;28:583–92www.elsevier.com/locate/fgcs.

[14] Mathisen E. Security challenges and solutions in cloud computing. On 5th IEEE International conference on digital ecosystems and technologies (IEEE DEST 2011). 2011.

 [15] Chen D, Zhao H. Data security and privacy protection issues in cloud computing, International conference on computer science and electronics engineering 2012.

 [16] Negi T, Chaudhary S, Rautela S. Data security in cloud computing. Int J Adv Res Comput Sci Software Eng May 2015;5(5) ISSN: 2277 128X, Available online at

www.ijarcsse.com.

 [17] Kaur S, Khurmi DS. A review on security issues in cloud computing. Int J Comput Sci Technol March 2016.