

# SECURITY CHALLENGES IN REALIZING VIRTUAL CLOUD INFRASTRUCTURE

Tanigaiarassane Djearamane  
Engineering Manager  
Cisco Systems India Pvt. Ltd.  
Chennai, India  
tdjearam@cisco.com

S. Siva Sathya  
Department of computer Science  
Pondicherry University  
Puducherry, India  
ssivasathya@gmail.com

**Abstract** — The advent and adoption of Cloud computing platforms, virtualization of components, be it at platform or software level has grown significantly. Though there are several advantages that are enlisted for cloud adoption, the use of cloud in virtualized environment brings new challenges for cloud adopters – security being the paramount. The goal of this paper is to introduce cloud, security, latest technologies like SDN, NFV embracing Cloud and their multiplier effect on cloud security challenges.

**Keywords**-Cloud computing, cloud security, SDN, NFV

## I. INTRODUCTION

NIST [1] describes cloud computing as “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”.

The advantages of cloud as seen by its proponents [3] are

1. Location independent resource pooling
2. On demand self service
3. Broad network access
4. Rapid elasticity
5. Measured services

The above features provided by most of cloud providers have given a compelling reason for the corporate CXO’s to adopt this technology as part of the business and IT plan. These gave them the cost advantage with respect to agility, speed of adoption and cost saving benefits without compromise on the business and IT functions they achieved with traditional asset management techniques.

Cloud offerings come in three service and four deployment models.

### A. Service model

Service model define what service the cloud offers. Cloud providers offer three types of services – Software as a service, Platform as a Service and Infrastructure as a service. The service model will signify one of the above.

Some examples for service models are email as a service for SAAS, Providing Operating System, Programming

execution, database to the consumers based on a subscription for PAAS and Virtual machines for computing for IAAS.

### B. Deployment model

These define who accesses the service. Cloud deployment can be done in 4 ways – Public, Private, Hybrid and Community clouds. Public cloud is provisioned for use to general public. The cloud in present in the providers premise and generally accessed via public Internet. Private cloud is provisioned for use for a single organization. The infrastructure is owned, maintained and operated by the organization or third party or a combination of them and it may exist on or off the premise. A specific community of users who have shared concerns provisions community cloud for use. Hybrid cloud is a combination of public, private and community clouds that remain as unique entities but are bound by standardized or proprietary technology.

The rest of the paper discuss about current challenges in cloud adoption, how security is implemented in cloud, challenges from a security perspective, opportunities and areas of focus due to the cloud virtual environment usage in technologies like Software Defined Network and Network Functions virtualizations and the future research work in these areas. The organization of the paper is as follows: challenges in cloud adoption in sections 2 and 3, various security facets to be accounted in for cloud deployments in section 4. Later in section 4, I shall introduce you to the latest concept and technologies that are ready to embrace virtualized environment in cloud and conclude with briefing on the security challenges introduced by the latest entrant and future course of work in section 6.

## II. CHALLENGES IN CLOUD ADOPTION

Cloud adoption has been growing steadily across public and private sectors owing to the advantages that cloud deployment brings to a consumer. With so many talking points for cloud adoption there still remain challenges for business and IT leaders to adopt this new business model [2].

Some of the critical factors that hamper cloud adoption are

a. Loss of control. In a cloud deployment, the consumer does not have control over the location of data or infrastructure. This lets the consumer to be at the mercy of cloud provider on his/her business critical information.

b. Multi tenancy. In a cloud environment, one has to reside and share the resource with other users. This leads to a situation where privacy could be breached. The user is again at the mercy of the provider for data privacy and security.

c. SLA. Organization having their own Service Level agreements, now have to depend on the providers' capability and agreement of provide services based on an SLA. Service availability now is at the mercy of the capability of a third party provider. d. Elasticity. From a situation where you had the entire capacity at your disposal to complete dependence on

the capability of the provider to give additional resource is scary for the end user.

Beyond these challenges, security in cloud remains the single largest factor that stand in the way of cloud adoption. The different challenges that one walks into when embracing cloud and how these are being taken care from a security perspective is discussed in subsequent sections of this paper.

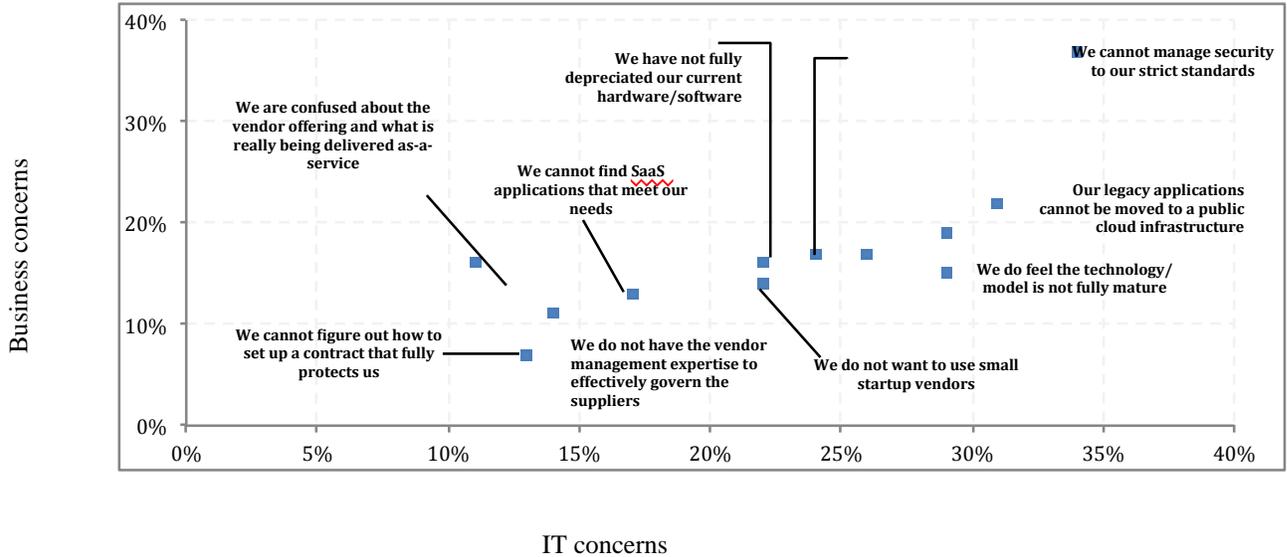


Figure 2.1 - Forrsights Business Decision-Makers Survey, Q4 2012 [3]

### III. SURVEY FINDINGS ON CLOUD ADOPTION AND SECURITY

Forrsights survey conducted in 2013 [3] with Business leaders and IP decision makers convey that applications of stricter security norms and adherence to the compliance requirements tops their cloud adoption concerns.

According to survey from Cloud alliance release Feb 2013[4], data breach is considered as the top most threat followed by data loss, account or service hijacking and others.

The survey by leading research institutes indicates increase in market share for cloud deployment and security in cloud remain the top concern for enterprise CEOs and CIOs. With this in context, there is serious effort expanded in implementing security controls and security policies to secure cloud deployments and increase the confidence of users and organizations to shift from traditional computing model to cloud computing. Doing so, will help both cloud providers and users to reap the benefit of this model.

The table-3.1 below summarizes the security responsibility between the cloud provider and user in different services models. The nature of security responsibility among stakeholders limits cloud adoptions. The role of security in a service model is not very clearly outlined. Cloud, with its challenges in adoption viz multi-tenancy, loss of control – organizations, users who seek cloud for their service is wary of the expectations on them to provide security.

Service model	Cloud Provider	Cloud Consumer
Software as a Service	Full accountability of up to software security	Use secure browser/ clients
Platform as a Service	Responsible for infrastructure and platform level security	Responsible for the security in hosted application
Infrastructure as a Service	Responsible for providing secure infrastructure – computing, storage, network	Responsible for application and platform services

Table 3.1 Security responsibilities in Cloud

With cloud being managed by third party cloud providers, security of information - confidentiality, integrity and

availability is seen as one of the critical factors that hamper cloud adoption.

#### IV. SECURE INFORMATION MANAGEMENT

In the ISO 7498-2 standard [14], produced by The International Standards Organization (ISO), Information Security should cover a number of suggested themes.

- Identification & authentication
- Authorization
- Confidentiality
- Integrity
- Non repudiation
- Availability

Also as per, the IEEE paper published in 2004 [6] on Basic Concepts and Taxonomy of Dependable and Secure Computing, security refers to

Confidentiality - absence of unauthorized disclosure of information

Integrity - absence of improper system alterations

Availability - readiness for correct service.

Securing cloud can be looked from a three dimensional perspective

- a. Compliance to the standards
- b. Securing the physical assets
- c. Securing the software assets.

Most of the commercial and open source cloud platforms have taken measures to provide security in all the above aspects.

##### A. Compliance to standards

Cloud security – in addition to the steps taken by the cloud providers on securing data and information within their purview, it is essential that cloud deployments are governed by compliance regulations by government and independent statutory regulators. This, once adhered can bring in confidence to cloud users on the security of cloud. USG agencies are required to accept only cloud providers are assessed and authorized through the Federal Risk and Authorization Management Program (FedRAMP) and have received a FedRAMP Provisional ATO issued by the Joint Authorization Board (JAB) [1].

The European council is actively working on standards to promote cloud adoptions [5].

Amazon web services has compliance program as part of its cloud-computing platform that ensures compliance to industry and government requirement for security and data protection standards. It adheres to standards like SOC1, SOC2, FISMA, FedRAMP, FIPS140-2 etc.

Windows Azure Trust center is run to ensure that AZURE platform is in compliance to the standards. AZURE is FedRAMP certified.

By bringing in such standard regulations from government

agencies for adopting cloud platforms will give an end user the confidence on Cloud platform's security.

##### B. Securing physical assets

Hardware layer security comprises of security at the perimeter of data centers and security at hardware layer in hypervisors. Though many security algorithms are implemented to safeguard the software aspect of cloud, is very essential that physical layer is attended to due to heavy dependency of clouds on virtualization. One of the top challenges in security is Insider threat. This cannot be avoided completely by merely protecting the software layer. Every cloud deployment should have multilayer security at their data center premise. This involves presence of security agency manning the building to implementation of multifactor authentication for the authorized staff entering the facility.

Amazon implements controlled authorization and multifactor authentication for the personnel allowed inside their data centre facility. Also stricter revocation policies are put in place once the duration for facility access for any personnel expires.

Another aspect of physical security is implementing security at hardware level of the data center servers. Different vendors adopt many physical layer securities. While choosing a server for cloud data centre, ensure that you choose the one that has physical layer security enabled in them.

As part of the hardware/physical security, Open Stack suggests to use hypervisors that would support one or more of the following hardware authentication & authorization techniques. - Trusted platform module (TPM), Intel trusted execution technology (TXT), Dynamic root for trusted measurement (DRTM), Unified Extensible Firmware Interface (UEFI). Hypervisor selection should be done based on the security features available in them – Kernel samepage merging, Xen security modules, xVirt, TXT, Apparmor – Linux security module implementing MAC, cgroups:linux kernel feature to control resource page[21] are some of the features to look for while selecting hypervisors for your cloud deployment.

##### C. Securing the software layer

Virtualization is the core component of Cloud deployment. It is very essential that every hypervisor be protected with sufficient security mechanism such that any intrusion and data security breaches are thwarted at virtualized layer. This is taken care by altering the permission for Host and guest operating systems that resides on the hypervisors. Guest operating systems should not be given the privilege to access overall resource pool of the hypervisor and should be given the privilege to access only the resources allotted for the Virtual machine instance.

In this section, different security implementations and study done on confidentiality, Integrity and availability at software layer is discussed.

Author/Cloud Solution	Confidentiality	Integrity	Availability
Jinzu Kong	Trusted computing technology for isolation of VMs		Cloud provider can compromise
Johannes K. Chiang et al.	Open ID, O'Auth		
Uma Somani et al. [15]		Digital signature with RSA encryption	
Amazon EC2	SSL, AES 256 (Amazon SSE)	HMAC-SHA1/HMAC-SHA256;	Availability zones S3 – objects are stored across multiple locations
Open stack	AES 128/192 TDES RSA	Serpent SHA1 SHA2	Cluster server
Hiroshi Fujinoki [19]		Split cloud	

Table 4.1 Security implementations in research and cloud solutions

Confidentiality - is to ensure absence of unauthorized disclosure of information. Letting the right user gaining access to resources. This is addressed through proper Authentication and Authorization mechanisms.

Thomas Ludescher [7] implemented Kerberos based ticket delegation based authentication in e-science infrastructure to enable authentication across sites thereby enabling collaboration among researchers.

It is highly recommended that any access in public domain be done through TLS/SSL methods. For encryption of data, Open Stack environment can be configured with TLS/SSL libraries. This library is tested for FIPS140-2 and found to be fairly secure. [21]. Cryptography standards available with Open Stack are AES 128/192 bits for protected data transfer, protection of data at rest. TDES 168 bits for protected data transfer, RSA 1024/2048/3072 bits; DSA 16 bits for Identification, authentication and protected data transfer, serpent; two fish for data at rest [21]

They deploy Host based intrusion detection system to alert the administrators or going with remedial action automatically. Some of the projects recommended are OSSEC, Samhain, Tripwire, AIDE[21].

From an authorization perspective, the recommendations are to use Thirdparty CA for Public and in-house CA for private cloud.

Authorization/Authentication on a Virtualized environment are done through SSH public/private key pair to restrict root access only to authorized originator. Federated authentication/authorizations are advocated in a multi cloud environments. WS- Fed is an option that can be used in a Federated environment.

A Secure, Scalable and Fine-Grained Access Control System in Cloud Computing, providing requisite access control on the network and port boundaries keeps unauthorized access at bay. The access controls can be extended to port/application level to keep the perimeter secure.

Integrity- To ensure absence of improper system alterations. Data integrity at rest and during motion is largely enabled through the application of encryption techniques.

Uma sonani et al. [9] has recommended Digital signature with RSA encryption to enhance integrity of data during motion. Openstack recommends SHA1; SHA2 – data at rest and transfer for data integrity check [21].

Hiroshi Fujinoki et al. [8] had recommended split clouds for data maintaining data integrity, whereby the data access is isolated from the provider and is handled at a remote location. This will help to counter the malicious insider threat to date integrity in cloud storage.

Availability: Availability of service at all layers is a key differentiator for the success of Cloud. Multi-cloud environments are seen as an option for increasing availability of services in a cloud. Multi cloud can be shared between Public/private, more than one public clouds or more than one private clouds. Amazon web services have availability zones, which have redundant servers to fall back when a service/server is taken out of operations. Every cloud computing platform provider offers high Confidentiality, Integrity and Availability mechanisms at Hardware and Software layers.

Open Stack uses pacemaker cluster stack to provide high availability. It focuses on both active/passive and state full and stateless services. Yu Gu [13] et al. recommends DR-Cloud with the participation from all cloud providers to storing Disaster recovery content to make the DR method more economical and feasible.

## V. ADVANCEMENT IN CLOUD ADOPTION - SDN AND NFV ARCHITECTURES AND THEIR IMPACT ON CLOUD

New technologies like Software Defined Network (SDN) and Network Functions Virtualization (NFV) suggest adopting cloud – the virtualization component of it for deploying their solutions. Both of these technologies are working towards moving in part or more of the network components to virtual environment. This section briefs about these technologies and brings out the challenges in cloud security in the next section.

SDN is an effort to move the control plane of Network devices such as routers and switches to virtualized environment. By doing so, an administrator can have the complete access to the control plan of switches and routers. This will enable him to alter/manage the flow of the network from a remote data centre. By having the virtualized component on a cloud environment, the user can take advantage of its agility and speed factors. Openflow, the group that drives the SDN technology is looking to Open Stack cloud computing platform for its SDN deployment. [11].

There are security concerns regarding the fact that all the network information are contained in a single server[17]. The

OpenFlow switch specification [19] describes the use of transport layer security (TLS) with mutual authentication between the controllers and their switches. However, the security feature is optional, and the standard of TLS is not specified.

NFV is an ISG activity within ETSI, dedicated to creating architecture to host network features and functions on general-purpose servers instead of on purpose-built network appliances. [12]. It is seen as an alternative to solve the Communication service providers need to make their infrastructure agile and quicker to make use of the latest services. With the advent of OTT networks, the service providers are in a critical challenge to upgrade their infrastructure to meet the latest demand for new services.

Network functions virtualizations looks to use Virtualized environment that is the core for Cloud computing as an important alternative to host the visualized functions. In a broadcast system, the entire network from sourcing, acquisition to the set tops at home can be added as NFV components and hosted in the cloud-virtualized environment. The ETSI aims at solving this problem by using standard virtualized environments. Work on this area has started at the earnest and once the NFV gets into prominence, this should reduce the cost of infrastructure, as these functions will be provided as a hosted service.

#### VI. CURRENT CHALLENGES IN CLOUD AND FUTURE STUDIES

Researchers and the cloud providers have made advances in securing the cloud and have started gaining the cloud users confidence. The concern on security is reducing from previous surveys (40% of the concerns is around security and compliance [3]), though it remains their highest demotivator for adoption.

The plan to bring in network related functionalities into the cloud throws in new challenges on cloud – its infrastructure and security. Some of the important areas that require further work for cloud are:

1. While implementing encryption, access control and backup mechanism, we need to take into consideration the unique requirements of cloud. With the advent of cloud, the volume of data that is stored and are in motion between the cloud users and cloud data store is manifold compared to the previous model where it was limited to the data storage and motion of a single organization. When we look at table 4.1, on the security implementation from the current providers, most of the algorithms are implemented considering the entire data set. If we were to apply this on a huge volume of data stored in cloud data centre, it will result in large time for data encryption and introduces latency of data retrieval and transmission. In order to overcome this, research has to be focused on applying techniques (like hashing) on a subset of data (at rest and travel). We need to move to a situation where there are industry-approved algorithms that work on subset of data for encryption.

2. With the plan of moving the heart of processing in network systems as envisioned by SDN and NFV, speed and performance of the Cloud computing network component is

very critical. By moving the network functions into the cloud, the cloud becomes prone to network attacks – recently we have seen a DDoS attack at 400 Gbps. If such an attack is to happen on a Cloud network, it will lead to fall of many corporates. Saving the network system from malicious intruders is a serious issue that requires work. Sandra Scott-Hayward[17] et.al discuss about the increased potential of DoS attack because of the very nature of SDN of enabling centralized controller and programmability for the network.

3. Security responsibility in cloud services model is shared with end users. This is another de motivator for cloud user. We need to move most or entire security responsibility in all service models towards Cloud provider.

The areas of Network security, encryption on fewer data sets and moving the security responsibility entirely into cloud provider needs additional work from both cloud providers and researchers.

#### VII. CONCLUSION

In recent past, Cloud providers had embraced added security measure through compliance regulation and adoption of standard security methods. This has helped the users to adopt Cloud for their requirement. But, by the introduction of new models, technologies that depend on cloud features for their deployment, has introduced new security challenges to cloud infrastructure. SDN and NFV has increased the cases for larger cloud adoption by corporates as part of their infrastructure and cloud planning. There is a need for creating nimble security and cryptography methods that can aid to secure the cloud without much impact to the performance of the cloud, network and network elements.

#### REFERENCES

- [1] NIST Security Reference Architecture by NIST Cloud Computing Standards Roadmap Working Group - Special Publication 500-291, Version 2
- [2] The Management of Security in Cloud Computing by Ramgovind S, Eloff MM, Smith E et.al in Information Security for South Africa (ISSA), 2010
- [3] The True State of Cloud Adoption by James Staten and Charlie Dai, 2013
- [4] The Notorious Nine Cloud Computing Top Threats in 2013 from Cloud Security Alliance
- [5] <http://www.cloudstandardscustomerCouncil.org>
- [6] Basic Concepts and Taxonomy of Dependable and Secure Computing by Algirdas Avizienis, Fellow, IEEE, Jean-Claude Laprie, Brian Randell, and Carl Landwehr, Senior Member, IEEE in IEEE Transactions on Dependable and Secure Computing volume:1, Issue:1, 2004
- [7] Security concept and implementation for a Feilhauer, Peter Brezany in Seventh International Conference on Availability, Reliability and Security (ARES), 2012
- [8] Split Clouds: New Security Architecture for Protecting User Information from Cloud Insiders - Designs, Implementation, and Performance Evaluations by Hiroshi Fujinoki and Siamak

- Mahmoudian Dehkordi in 2012 6th International Conference on New Trends in Information Science and Service Science and Data Mining (ISSDM)
- [9] Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing by Uma Somani, Kanika Lakhani, Manish Mundra in 2010 1st International Conference on Parallel Distributed and Grid Computing (PDGC),
- [10] <http://docs.openstack.org/training-guides/content/module001-ch004-openstack-architecture.html>
- [11] <https://www.opennetworking.org/sdn-resources/onf-specifications>
- [12] <http://www.cloudfv.com>
- [13] DR-Cloud: Multi-Cloud Based Disaster Recovery Service by Yu Gu, Dongsheng Wang, and Chuanyi Liu in *TSINGHUA SCIENCE AND TECHNOLOGY* journal – Volume 19, Number 1, February 2014
- [14] ISO.ISO 7498-2:1989. Information processing systems- Open Systems Interconnection. ISO 7498-2
- [15] Authentication, Authorization And File Synchronization On Hybrid Cloud On Case Of Google Docs, Hadoop, And Linux Local Hosts Johannes K. Chiang et.al. in 2013 International Symposium on Biometrics and Security Technologies (ISBAST),
- [16] A practical approach to improve the data privacy of virtual machines Jinzhu Kong in 2010 IEEE 10th International Conference on Computer and Information Technology (CIT)
- [17] Network innovation using open flow – A survey by Adrian Lara, Anisha Kolasani, Byrav Ramamurthy in *Communications Surveys & Tutorials, IEEE* (Volume:16 , Issue: 1 )
- [18] SDN Security: A Survey by Sandra Scott-Hayward, Gemma O’Callaghan and Sakir Sezer in 2013 IEEE SDN for Future Networks and Services (SDN4FNS)
- [19] “OpenFlow Switch Specification Version 1.3.2,” Open Networking Foundation, version 1.3.2, April 25,2013
- [20] Network Functions Virtualization - An Introduction, Benefits, Enablers, Challenges & Call for Action in october 22-24, 2012 at the “SDN and OpenFlow World Congress”, Darmstadt-Germany
- [21] OpenStack Security Guide – March 19,2014

#### AUTHORS PROFILE

**Tanigaiarssane Djeareamane** is a Software professional with experience in developing Enterprise and Service provider solutions for Network Management, Security and Video domain. He is a regular keynote speaker and participant in International conferences related to Computers and communication. Currently he is working with Cisco Systems India Pvt Ltd. on video solutions for Service provider market.

**S.Siva Sathya** is an Associate Professor in the Department of Computer Science in Pondicherry University, Pondicherry. She did her B.Tech, M.Tech and Ph.D. in Pondicherry University. Her area of specialization is Evolutionary Algorithms. Her research interests include Data Mining, Bio-inspired computing and optimizations. She has published a number of research papers in International journals and conferences.