Security Architecture for multi-Tenant Cloud Migration

Manikandasaran S. S. and Raja S.

***Abstract*—In today's competitive IT world Cloud Computing is the word rolling around in all activities of IT companies. Thus, everyone is transforming their infrastructure from legacy infrastructure to cloud computing which is very feasible, and Cost effective. Finally, it can scale up and scale down instantly on demand basis. When companies think about the cloud adoption, security is the biggest issue and data is stored in software defined environment. This paper addresses security parameters which need to be mainly considered for cloud migration. Cloud service provider is responsible for building fence around the underlying infrastructure i.e. Compute, network and storage. Security is the main controller for adopting the cloud environment. In Cloud computing, security issues are identified with different layers. In this paper, new architecture is proposed for achieving data confidentiality and data integrity in multitenant workload migration into cloud. This architecture ensures that tenant has secure relationship between source and destination data centers via staging area. This staging area has capability to migrate the workload in different hypervisors. Workload meets security guidelines through this migration process from beginning to end.**

***Index Terms*—Cloud security, multitenant, data confidentiality, data migration, software defined functionalities (SDF).**

I. Introduction

Internet is the contributing factor towards various technologies that have been developed since its inception. Over the last few years' cloud computing paradigm has witnessed an enormous transformation towards its adoption [1]. The cloud model gives great interest to service provider because it represents the next wave of innovation sweeping across the internet and presents tremendous business opportunities for those who successfully define and implement a new paradigm (ex. Airbnb, Uber, Grab etc.). Cloud computing has shared pool of resources such as Network, Storage, Servers that can be rapidly provisioned with minimal management effort. The end user does not need to own the infrastructure [2]. Cloud provides services in visualized manner. Cloud providers always ready provide computing resources instantly is known as on-demand computing. Cloud has reliable storage for which it maintains many data centers. Users' data are kept in more than two data center for evading physical damage of data stored in the cloud data centers. In fact, it can be accessed from anywhere in the world [3]. Cloud provides more efficient data management to maintain the users' data. Enterprises are interested on the cloud because of its intelligent and user friendly services [4]. Though there are many advantages in cloud, it has some issues in security of data in cloud. Security is top most challenge in cloud environment that has to be addressed [5].

Cloud computing can be provided in several delivery or deployment models [6].

- Public Cloud:

A public cloud is one in which the cloud infrastructure is made available to the public or large industry group over the internet. The infrastructure is not owned by the user, but when an organization provides cloud services, host is on premises. Services can be provided either at no cost, as a subscription or under pay as you go model.

- Private Cloud

A private cloud refers to a cloud solution where the infrastructure is provisioned for the exclusive use of a single organization. The organization often acts as a cloud service provider to internal business units that obtain all the benefits of a cloud without having to provision of their own infrastructure. By consolidating and centralizing services into a cloud, the organization is benefited from centralized service management and economies of scale.

- Hybrid Cloud

A hybrid cloud, as the name implies, is a combination of various cloud types (public, private, or community). Each cloud in the hybrid mix remains a unique entity, but is bound to the mix of technology that enables data and application portability. The hybrid approach allows a business to take advantage of the scalability and cost-effectiveness of a public cloud without exposing its applications and data beyond the corporate intranet.

- Community Cloud

A community cloud shares the cloud infrastructure across several organizations in support of a specific community that has common concerns (for example, mission, security requirements, policy, and compliance considerations). The primary goal of a community cloud is to have participating organizations to realize the benefits of a public cloud, such as shared infrastructure costs and a pay-as-you-go billing structure, with the added level of privacy, security, and policy compliance usually associated with a private cloud.

In addition, the industry recognizes three cloud computing service models (IaaS, PaaS, SaaS), although others exist [7].

- Infrastructure as a Service (IaaS)

Infrastructure as a service is a cloud computing in which a vendor provides user access to computing resources such as servers, storage and networking. Organizations use their own platforms and applications within a service provider's infrastructure.

Manuscript received March 9, 2018; revised May 11, 2018.

Manikandasaran S. S. is with Christhuraj Institute of Computer Applications, Christhu Raj College, Panjappur, Tiruchirappalli (e-mail: moni.tamil@gmail.com) .

Raja S. is with the Department of Computer Science, Christhu Raj College, Panjappur, Tiruchirappalli (e-mail: rajasjc@gmail.com).

doi: 10.18178/ijfcc.2018.7.2.518

- Platform as a Service (PaaS)

Platform as a service is a cloud computing offering that provides users with a cloud environment in which they can develop, manage and deliver applications. In addition to storage and other computing resources, users are able to use a suite of prebuilt tools to develop, customize and test their own applications.

- Software as a Service

Software as a service is a cloud computing offering that provides users with access to a vendor's cloud-based software. Users do not install applications on their local devices. Instead, the applications reside on a remote cloud network accessed through the web or an API. Through the application, users can store and analyze data and collaborate on projects.

Cloud computing is differed from other computing by its essential characteristics that are on-demand service, broad network access, pooled resources, rapid scaling and metered billing [8]. Users try to adopt this computing but due to some security problems in migration into cloud, users are struggled to adopt this environment. This paper proposes architecture to secure migration of legacy infrastructure into cloud.

This paper organized as follows: Section I Introduction describes Cloud computing basics and its characteristics, Section II Related Work discusses various works done in this same area, Section III Problem Definition explains the issues regarding migration of data into cloud, Section IV Proposed Work elucidates new architecture to address the migration problem in cloud. Section V Expected Output delivers the expected outcome derived from the proposed architecture, Section VI Advantages of Proposed Work describes the advantages of the proposed work and Section VII Conclusion presents conclusion of the paper.

II. Related Work

Cloud migration is the biggest challenge to enterprise to migrate their infrastructure into cloud. There is no proper method to transfer data into with full security. Some researchers have worked in this same area to find solution for migrating issue in cloud. This section describes some of the work previously done by different authors.

Joydipto [9] discussed about cloud migration techniques. The migration techniques include standardization and cloud migration considerations. The author discussed about methodology which help to migrate workloads into the cloud without re-architecting or re-engineering existing application topology. The paper did not address any security related consideration when migrating to cloud both data and virtual machine. This paper has various cloud migration patterns such as Traditional IT to public cloud, Private cloud to public cloud, Private cloud to hybrid cloud, Public cloud to private cloud and Public cloud to public cloud.

Khadjia *et al*. [10] proposed architecture for cloud migration process and addressed four types of migration strategies. This paper did not address about security methodology or techniques during migration process. This proposed model provides analysis of cloud migration strategy and preliminary feasibility analysis. This paper focuses main re-design and re-deploy of existing workload when decides to migrate into cloud.

Virendra *et al*. [11] addressed data migration security issues in cloud and proposed predictive based encryption and decryption techniques for data migration in the cloud. The proposed encryption technique is suitable for HDFS (Hadoop Distributed File System.

Jun-feng *et al*. [12] discussed about different migration strategies to the cloud. This paper discussed legacy system migration to the cloud and addressed challenges & issues. The migration methodology requires re-architecting the applications. It does not address any security issues and methodology during legacy system migration to the cloud.

Zeb *et al*. [13] proposed techniques for virtual machine migration to intercloud which includes mutual authentication, data confidentiality and integrity of VM. This paper addressed the intercloud VM migration securely which uses elliptic curve diff helmen and SHA-256 algorithm for entire VM migration process. During this entire VM migration process, the authentication and authorization are happening mutually between source and destination cloud. The data confidentiality and data integrity is still need to be concentrate on this paper.

III. Problem Definition

In recent cloud computing adoption strategies, Cloud computing users are facing many obstacles when migrate the existing workload, as it is from on-premises to cloud datacenters securely. Each tenant is currently sharing dedicated link between on-premises data center to cloud datacenter which is highly possible for data compromise between tenants, because tenants do not have secure tunneling. The tenants do have compatibility issue when moving to cloud since the cloud data center is fully functional by software defined environment rather than legacy systems.

The cloud user faces challenges when converting from legacy server to virtual machine and virtual machine to virtual machine. Cloud user faces challenges when they wish to change the hypervisor of running VM from on-premises to Cloud Datacenter securely and it's required to consider the security parameters. This is the major issue and is to be considered in the proposed model with new architecture in cloud computing environment.

IV. Methodology

Cloud promotes business opputunities to different level of users. Users may be an enterprises to get business through cloud for which they need to migrate their infrastructure into cloud. During, cloud migration users meet some security issues. This paper proposes new archtieture to address the issues in migration of data into cloud. The paper proposes Stageing Area in the process of cloud migration to address the security issues in it. Fig. 1 depicts different phases in proposed architecture to migrate the VM and data into cloud.

The proposed architecture has different phases to migrate from on-premises data center to cloud data center. Among this phases, staging area focuses the secure migration of Virual

machine and data. Table I describe different phases in cloud migration.

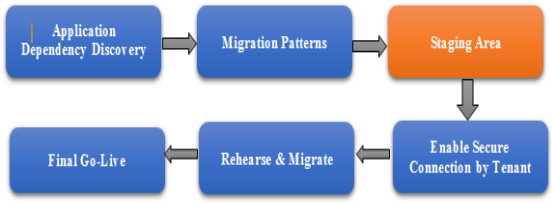

Fig. 1. Methodology for migrating on-premises data to cloud data center.

TABLE I: DESCRIPTION OF DIFFERENT MIGRATION PHASES

Migration Phases	Description
Application Dependency Discovery	It covers initial baseline discovery of existing foot print of the server details.
Migration Patterns	Migration pattern consists of 4 types (i) Live Migration (ii) Enhanced Live Migration (iii) Import & Export Migration (iv) Migration Using Replications
Staging Area	staging consists a pool of resources which built by loaner hardware
Enable Secure Connection By Tenant	Secure connection represents the segregation of tenants with the help of Network Function Virtualization. If we don't segregate the tenant from cloud data centers, users are able to view the tenant's workload since cloud data center is open to the world.
Rehearse & Migrate	Once secure connection is enabled for tenants, It has to check whether able to migrate VM and data
Final Go-Live	If the test phase is completed then migration starts to transfer the VM and data seamlessly.

V. PROPOSED SECURITY ARCHITECTURE

Security architecture is proposed for migrating into cloud environment in a secure manner. In proposed architecture, Staging area plays vital role in workload migration in end-to-end. To construct this staging area required new security policy, encryption algorithm and conversion techniques for achieving data confidentiality and data integrity. Feasibility study is required to know enough workloads which needs compute power, storage space in target cloud data center. The secure connection is established by setting up the temporary compute nodes in stage area. Establish the connection between tenants to segregate the traffic. Segregate the tenants by industries due to regulatory requirement.

The proposed architecture can define the protection of workload from on-premises data center to cloud data center with the help of defined staging area.

A. Staging Area

Staging area represents the transportation of workloads between on-premises data center to cloud data center. It has segregation between multiple tenants to isolate secure transmission of workloads.

The staging area prevents threats and malicious attacks from the cloud data center. In the existing architecture, dedicated link used to establish connection between multiple data centers, to move the workload insecurely because of multiple tenants. Current industry practices this method to transfer the workload from on-premises data center to cloud data center. The proposed architecture provides secure transport mechanism to migrate the workload with minimum cost and also used for multitenant cloud migration. The migration strategy is really dependent on network virtualization since cloud datacenter is network centric. The hypervisors are in staging area is to ensure that no vulnerability found during migration. Minimal effort is enough for workload migration, if the staging area is established and it is more cost-effective method with respect to resource. Staging area uses minimal resource to migrate the workload.

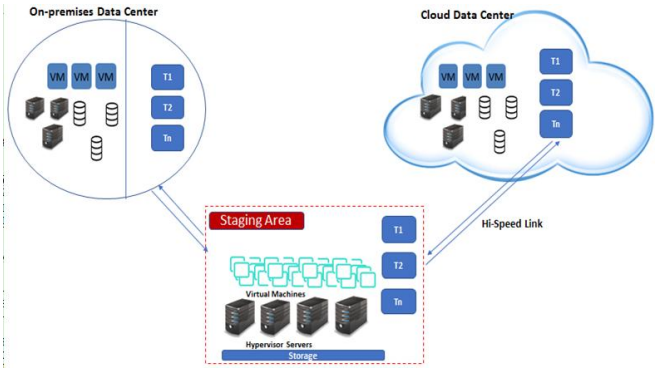

Fig. 2. Proposed security architecture for cloud migration.

If user wishes to replace the underlying hypervisor, then staging area helps to convert it into target location. Fig. 2 depicts the proposed security architecture.

Notations used in the architecture are described below,

- Tn1,Tn2,……Tnn →Tenants
- TL1,TL2,……TLn →Tenant Link
- DC1 →On-premises Data center
- Cloud DC →Cloud DataCenter
- DL →Dedicated Link

Following are the different components used in the proposed security architecture.

- ***Datacenter****:* the datacenter comprises multiple tenants with leased equipment's which includes mixed of physical and virtual servers and physical network devices.
- ***Cloud data center:*** The cloud data center provides software defined functionalities for compute, network and storage with multiple tenants. It comprises multiple hypervisors for the end users.
- ***Tenants:*** Tenants are who hosted their infrastructure a service from any cloud service provides such as (Amazon, IBM, Google and Microsoft).
- ***Direct link***: It is high speed link to establish between one data center to another data center such optical fibre, WAN link.

VI. ADVANTAGES OF PROPOSED ARCHITECTURE

The proposed security architecture provides advantages that, cloud users can securely migrates their workload to cloud environment with any intervention. Functional Testing and Non-Functional Testing should be carried out during end to end workload migration for securing the migration. The main advantage in the architecture is the introduction of Staging area. It provides the following advantages to cloud users.

- Tenants are capable to establish the secure connection between on-premises datacenter to cloud data centers.
- In Multitenant cloud, one tenant cannot view other tenant workloads by segregating the link.
- This staging achieves data confidentiality, data integrity and privilege management.
- It supports one hypervisor to multi hypervisor with software defined functionalities (SDF).
- The proposed architecture is eligible to migrate simple and complex workload.

VII. Interpretation of Research Work

By implement this architecture, Tenants can move their workloads from on-premises datacenter to cloud data center seamlessly and securely with the help of loaner hardware. Tenants can achieve data confidentiality and data integrity. In completion of workload migration, application consistency is maintained and it's available to the business users immediately. Staging area is responsible to validate the vulnerability of workload. It is continuously checks the data integrity and eligibility to move the target cloud data center and it confirms that it will be moving into right tenant place in cloud data center by using private and public key mechanisms. Staging area is periodically checked the routing policy to ensure that only trusted tenant have secure tunneling by routing techniques

VIII. Conclusion

The end users face issues and challenges when they are decided to move their existing workload into cloud due to security concerns. Currently, the cloud service providers are offering techniques and tools for one-to-many tenants and not available for many-to-many tenants use cases. In this paper, the proposed security architecture is used to achieve multitenant workload migration technique in a secure manner. The paper has described the workload migration techniques with multitenant and multi hypervisor environment in targeted cloud datacenter for achieving data confidentiality and data integrity. The proposed architecture is eligible to migrate simple and complex workload. In future, the proposed model will be implemented and achieved for better results.

References

[1] K. El Makkaoui, A. Ezzati, A. Beni-Hssane, and C. Motamed, "Cloud security and privacy model for providing secure cloud services," in *Proc. IEEE International Conference*, 2016, pp. 81-86.

[2] M. Yuan, S. N. Pang, and Q. Gao, "Design and development of data security automatic testing system on public cloud," in *Proc. IEEE International Conference on Software Engineering and Service Science (ICSESS)*, 2016, pp. 992-995.

[3] S. F. Lai, H. K. Su, W. H. Hsiao, and K. J. Chen, "Design and implementation of cloud security defense system with software defined networking technologies," in *Proc. IEEE International Conference on Information and Communication Technology Convergence (ICTC)*, 2016, pp. 292-297.

[4] S. K. Abd, R. T. Salih, S. A. R. Al-Haddad, F. Hashim, A. B. H. Abdullah, and S. Yussof, "Cloud computing security risks with authorization access for secure multi-tenancy based on AAAS protocol," in *Proc. IEEE TENCON 2015 - 2015Region 10 Conference*, 2015, pp. 1-5.

[5] L. Arockiam and S. Monikandan, "Data security and privacy in cloud storage using hybrid symmetric encryption algorithm," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, issue 8, pp. 3064-3070, 2013.

[6] T. Aslan, P. G. Croes, L. Rosca, and M. Stern, *Cloud Security Guidelines for IBM Power Systems*.

[7] IaaS, PaaS and SaaS – IBM Cloud service models. [Online]. Available: https://www.ibm.com/cloud/learn/iaas-paas-saas

[8] N. Jayapandian, N. Zubair Rahman, A. M. J. Md Sangavee, and R. B. Divya," Improved cloud security trust on client side data encryption using HASBE and Blowfish," in *Proc. R. 2016 IEEE Online International Conference on Green Engineering and Technologies (IC-GET)*, pp. 1-6 , 2016

[9] B. Joydipto, "Moving to the cloud: Workload migration techniques and approaches," in *Proc. IEEE International Conference on High Performance Computing*, 2012.

[10] S. Khadija and B. Faouzia, "Methods Migration from On-premise to Cloud," *IOSR Journal of Computer Engineering Ver. IV*, vol. 17, issue 2, ver. 4, pp. 58-65, 2015.

[11] V. S. Kushwah, and S. Aradhana, "A Security approach for data migration in cloud computing," *International Journal of Scientific and Research Publications*, vol. 3, issue 5, 2013.

[12] J. F. Zhao and J. T. Zhou, "Strategies and methods for cloud migration," *International Journal of Automation and Computing*, vol. 11, pp – 143, 2014.

[13] T. Zeb, A. Ghafoor, A. Shibli, and M. Yousaf, "A secure architecture for inter-cloud virtual machine migration," *Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 24-35, 2014.

S. S. Manikandasaran is working as director in Christhuraj Institute of Computer Application, Christhu Raj College, Tiruchirappalli, Tamil Nadu, India. He has 10 years of experience in teaching and 9 years of experience in research. He is completed his MCA and M.Tech in Bharathidasan University, Tiruchirappalli in 2007 and 2009 respectively and also completed his Ph.D degree in Manonmaniam Sundaranar University, Tirunelveli in 2015. He has attended many international and national conferences, seminars and workshops. He has published 40 research articles in the international / national conferences and journals. He has delivered more than 20 lecturers in various national level seminars, symposium and conferences. His research interests are cloud computing, network security, cloud security, IoT and web technology.

S. Raja is research scholar in Christhu Raj College, Department of Computer science, Tiruchirappalli, Tamil Nadu, India. He has 12 years of experience in IT industry. He is completed his M.Sc. in Bharathidasan University, Tiruchirappalli in 2005. He has attended many International and national conferences, seminars and workshops. He has delivered more than 5 international and national conferences. His research interests are cloud computing, cloud security, cloud IoT and big data analytics.