The Security Issues and Challenges In Hybrid Cloud

Venkatakoti Reddy.G[1], B Harish Raj[2], Dr.P.Bhaskara Reddy[3]
[1]Dept of Computer Science and Engineering
[2]Assistant.Professor, Dept of Computer Science and Engineering
[3]Professor, Dept. of Electronics and Communication Engineering
[1, 2, 3] HITS, TS, India

Abstract- *Present day's information technology organizations are faced with an increase in the challenge and convolution of improve their IT finances for the best potential shipment of service to inner and outer clients. Decrease infrastructure costs, establish IT management, and raise service shipment. The cloud based more than companies are maintained the ADP earnings work and upload unofficial data regular to the work contributor cloud environs. The hybrid cloud consists where the protect services contributor are responsibility for the infrastructure, security controls and security proficiency recommend by the cloud service. The cloud present provides service new technology to suitable secures the data and approach that occupy on their physical infrastructure. We are proposed in this paper present threats and fire wall of the service to maintain the combined member of staff and contract record with entry in approach control authority guidelines for a cluster and extensive advance in the cloud.*

Keywords- cloud, infrastructure, security

I. INTRODUCTION

The cloud computing consists of different technologies security issues in hybrid cloud. The normally speak about generally facing cloud security issues are related to physical local area network and systems and servers. Two sides of personal subjects of attacks, data theft. The cloud physical servers are opposite and controlled by the companies. The cloud sever provide more than one servers are distributed the different customers. The single customer didn't support cloud client. Generally one or more customers are can do all Mainly identify particular the end points are attacks to cyber – attacks with the objective to steal data. Here can be find out different between single use potential subjects of attacks who may become victims through individual attacks on private cloud servers. Sometimes the company total applied to cyber data crime. It is true or not but attacks are target to particular person are much easier in the on-permission solutions.

The cloud servers service support the point view, there is also the security challenge when the one or more than customer it is multi tenancy. The distributing of the resources between more than clients. The design of security issues authorised responsibility maintain to solution provide and the customer own itself. In case the multi customers are facing the security issues apply additional service provided to Third Party Company solve the secure service [10].

Cloud divided to possible the certain secure into different area consists infrastructure as a service, platform and application layer, administration and compliant. The infrastructure area service covers to possible threats in physical layer. The customer has access to the parts in the on-permission solution, but the cloud is managed provide the application layer present by all applications are provided with in the cloud customer. The area of the problems related compliance to obtain laws and regulations are that maintain in giving area association with cloud computing, data storage, risk assessment, certifications and quality standards in the related state organizations [11].

II. PROPOSED HYBRID CLOUD SOLUTIONS

The main issues from personal experience with customers.

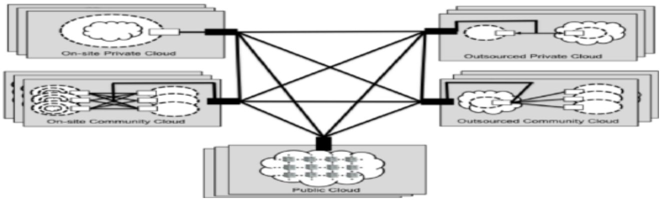


Fig:1 . Hybrid cloud source

1. Relocation of area controllers to the cloud.

Support of more dealers is (for ex. When a more number of Desktop Computers) that at least one area controller is reality left as an in- home server (for ex. Un physically operating as a model server). Security should be done over an IPsee VPN channel with in directional faith. Often the authorized authentication is reality clarify with the corporate access within the faith talent of the in particular area [13][14].

2. Union with organized IS.

Is another burden that customers have when they consider relocation to the cloud (relocation of some services in the cloud). Mostly it is required to manage in union of enterprise systems, more n are beyond mainly with the secure of the network between the public and private cloud servers. The services can authenticate to the area controller based on its location. It require to take into report that the systems, which last in-home infrastructure enclose extra confidential data

.

3. Government wants to clarify the demand of private cloud, but source at a company.

The term "Outsource private cloud "is a un sufficient bit false mow ever this plan is workable. Specific location is given by cloud providers for the entire private cloud, which is complete in the text of an remote security boundary**.**

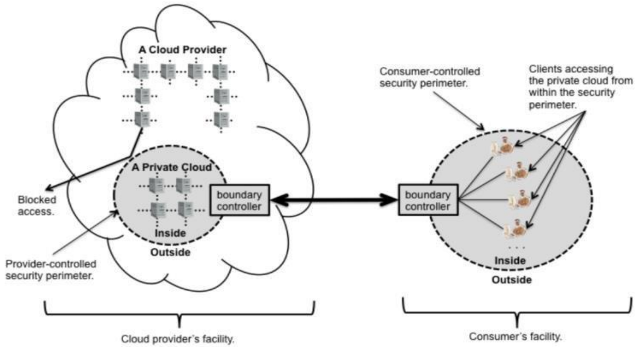

A Cloud Provider
A Private Cloud
Blocked access.
boundary controller
Inside
Outside
Provider-controlled security perimeter.
Consumer-controlled security perimeter.
Clients accessing the private cloud from within the security perimeter.
boundary controller
Inside
Outside
Cloud provider's facility.
Consumer's facility.

Fig-2. Outsource private cloud, source

III. SOLUTION PROSPECTS

A. The first option is a position, where a company has its own infrastructure with information systems or virtualization and possibly private cloud- thus provides its employee virtualized applications (eg. App-v) or a full displayed model of an Infrastructure as a Service private cloud design on one of hypervisors (Microsoft, VMWare, Citrix or others). The plan company wants to reduce the usage of infrastructure to change it to the cloud. The company part of the IaaS will continue at the company operating its information system. The second part option will be reallocated or removed. Then the public cloud will be invest predefine services (mail server), which will be network to the physical servers (onsite) see figure 3)

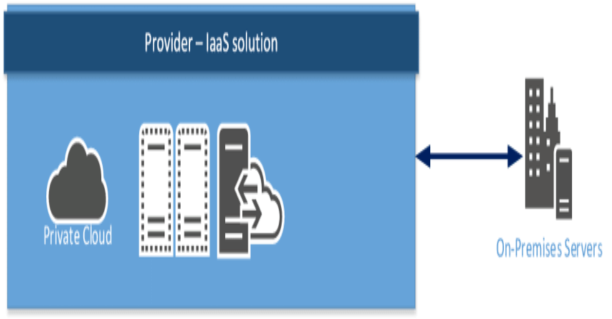


Figure 3 **On-Premise Infrastructure connected to IaaS**

User authentication is reality clarify each of two over particular accounts (login to cloud services), unite authentication (i.e network area filter company with authentication in the cloud) or possibly even through adding a second option in the form of multi-factor authentication (ex. Cell phone)

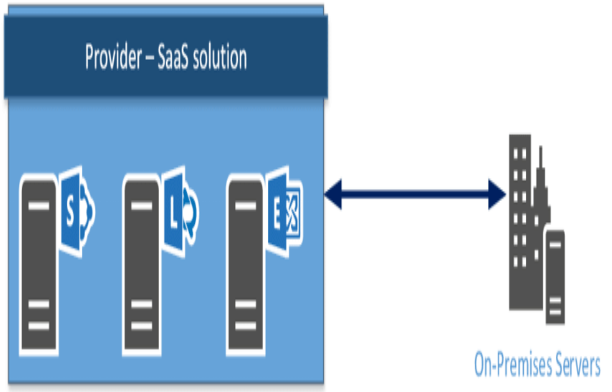
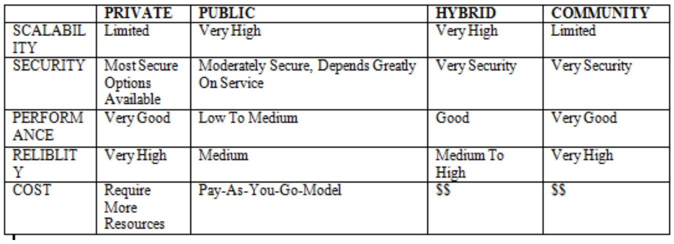


Figure 4 On-Premise Infrastructure connected to SaaS

B. The second option is a schema where a company has the same infrastructure as in the first one, but wants to relocation virtualized servers to the public cloud (IaaS). The advantage of such a schema is mainly a brighten of physical servers, reducing the cost and employees (administrators) etc. Here can be idenfied the security change in pathway between private and publicIaaS. Government and companies have to clarify serval key points that confuse selecting sure hybrid cloud solutions. Data that is inside the company cannot be change to the cloud, either due to data confidentiality due to requirement to have them in on- premise solutions by the law or other any ISO stands. If the data will be relocation to the public cloud, where it will be physical data stored question asking? Companies often do not want their data to leave the country and search for a cloud provider with data centres in the Czech Republic of this reason [15].



	PRIVATE	PUBLIC	HYBRID	COMMUNITY
SCALABILITY	Limited	Very High	Very High	Limited
SECURITY	Most Secure Options Available	Moderately Secure, Depends Greatly On Service	Very Security	Very Security
PERFORMANCE	Very Good	Low To Medium	Good	Very Good
RELIBLITY	Very High	Medium	Medium To High	Very High
COST	Require More Resources	Pay-As-You-Go-Model	$$	$$

Figure-5 Overview of parameters regarding to cloud deployment models.

IV. SOLUTION DESIGN

A private cloud outsourcing secure solution provide final customer the company require within the infrastructure to use. The private cloud in the in home private cloud incorporate outsource of limit of additional service if its require provide their own servers and take their infrastructure can be changed to environment to a public cloud. It will provide Software as a Service (SaaS) service takes risk only delicious data.

Where there is private cloud that is both hosted/outsourced by a provider- a company with a centre in the republic and placed In- home infrastructure on the another side. The distribution of services and therefore not necessarily wants to have complete redundancy of all the services in private cloud provides in –home infrastructure. The manages provides commit infrastructure with in all security requirements for personal agreements written to administration. This company is internal services and physical servers solve the secure issues. The sharing of hardware along customer support of physical infrastructure and proper communication implemented to hybrid plot done. The authentication wants on-site infrastructure operates to danger systems. Next take immediately to connect the system authentication secure channel with servers that are located at the provider (virtual private network, encrypt, multiple authentication etc.). If any problem facing diving services will be operated with in a private in –home solutions within an internal solution that tend to be service on authentication and identity management, document management for under legislation. If another information system it is not possible to move to a private cloud for n different reasons.

V. CONCLUSIONS

The cloud solutions surely solve specific problems of our time and bring a lot of value in use. In the form of cost saving infrastructure services. Mainly maintains returns of finances. First of all immediately to plan the transition. Then mainly risk problems facing services issues. The services are provides find similar or small less in the cloud environment in –home infrastructure. The highest security risk of the “path or Channel” between the in –home and cloud infrastructure of provide service. It is maintained the quality and security of the customers own infrastructure and the wants to secure the web site connection. Another challenged issue remains centralizing the authentication of personal users, under deployment, and constantly supplemented with new additions to the “simple” authentication. For examples authentication using biometrics and mobile phones, face recognition .etc.

REFERENCES

[1] KPMG,”KPMG-Exploring the Cloud- A Global study of Governments’ Adoption of Cloud KPMG [2]. KMMG,” Cloudjakocestakusporamvestatnisprave.”[online].Available.https://www.kpmg.com/cz/cs/issueandinsights/articlespublications/press-releases/stranky/cloud-jakocesta-kusporam-ve-statni-sprave-sprave.aspx [Accessed: 24-Mar-2015].

[2] Amazon Web Services, “AWS GovCloud(US) Region Overview –Government Cloud Computing ,” Amazon Web Services , Inc, 2015. [Online]. Available: http://aws.amazon.com/govcloud-us/.[Accessed: 11-Apr-2015].

[3] IBM Software and IBM Smart Cloud Social collaboration for Government, IBM Smart Cloud social Collaboration for Government,”IBMsmart Cloud Social Collaboration for Government, 30-Dec-2014 [Online]. Available: http://www01.ibm.com/software/lotus/cloud/goveremnt/[Accessed: 11-Apr2015].

[4] ”MicrosoftAzure Government.”[Online].Available: http://azure.mircosoft.com/enus/features/gov/.[Accessed:24-Nar-2015].

[5] D. Brown, “Now Available: VMware vCloud Government Service | The Journey to Hybrid Cloud,” The Journey to Hybrid Cloud, 2015. [Online].Available: http://www.hybridcloudforum.com/646/nowavailable-vmware-vcloud-government-service. [Accessed: 24-Mar-2015].

[6] P. Mell and T. Grance, “The NIST Definition of Cloud Computing.” National Institute of Standards and Technology, Sep-2011.

[7] M. Carvalho, “Secaas-security as a service,” Inf. Syst. Secur. Assoc., vol. 9, no. 10, pp. 20–24, 2011.

[8] N. Oza, K. Karppinen, and R. Savola, “User experience and Security in the Cloud an Empirical Study in the Finnish Cloud Consortium.pdf.” VTT Technical Research Centre of Finland.

[9] L. Badger, T. Grance, R. Patt-Corner, and J. Voas, “Cloud Computing Synopsis and Recommendations.” National Institute of Standards and Technology, May-2012.

[10] E. A. Fischer and P. M. Figliola, “Overview and Issues for Implementation of the Federal Cloud Computing

Initiative: Implications for Federal Information Technology Reform Management.” Congressional Research Service, Library of Congress, 2015.

[11] O. Sharma, P. Das, and R. K. Chawda, “Hybrid Cloud Computing with Security Aspect,” Int. J. Innov. Adv. Comput. Sci., vol. 4, no. 1, pp. 76–80, 2015.

[12] B. Hunt, “Windows Azure Hybrid Cloud Authentication and Access Architectures – Discussion (31 Days of Windows Servers (VMs) in the Cloud – Part 31 of 31) - The IT Pro Exchange - Site Home - TechNet Blogs,” TechNet blog, 2013. [Online]. Available: http://blogs.technet.com/b/bobh/archive/2013/01/31/windows-azure-hybrid-cloud-authentication-and accessarchitectures-discussion-31-days-of-windows servers-vms-in-the-cloud-part-31-of-31.aspx. [Accessed: 12-Apr-2015].

[13] Juniper Networks, Inc., “Identity Federation in a Hybrid Cloud Computing Environment Solution Guide.” Juniper Networks, Inc., 2009.

[14] Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing v3.0.” Cloud Security Alliance, 2009.

[15] Carpathia, “Hybrid Cloud Solutions for Government Agencies: How to Have the Best of All Worlds | Blog,” Hybrid Cloud Solutions for Government Agencies: How to Have the Best of All Worlds, 04-May2015. [Online]. Available: http://carpathia.com/blog/hybrid-cloud-solutions-for-government-agencieshow-to-have-the-best-of-all-worlds/. [Accessed: 24-Mar-2015]