RESEARCH ARTICLE OPEN ACCESS

Cloud-Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds

Prof. Amol Jadhao, Kunal Anand, Shashank Dhar, Sagar Mukharia
Department of Computer Science
Pune University, and DYPIET Ambi
India

ABSTRACT

The Security is one of the most significant concern towards using of cloud computing system either in government Sector's or in private sector's, hence we introduced the concepts of a cloud architecture reference model provides us a wide range of security assurances; which justify the degree of confidentiality and integrity offered by a CCSs and CSPs. It uses four level of multi-tenants IaaS cloud architectures which is equipped with lots of alternative of cloud control security & to show high probability of security.

Keywords:- CCSs, CSPs

I. INTRODUCTION

Cloud is one of the most important terms in today's era, So we need to know about what is cloud computing?-so, Cloud computing is a kind of storing service w/o any physical appearance, which can access only over internet. It's flexibility and scalability is more beneficial to all, but When we talk about involvement of unauthorized user's laid to security concern; because there are lot's of confidential data poured on it. Hence the big question is arises; can we trust on CSPs to protect cloud tenant data or not! Or whrather CCSs can prevent the unauthorized disclosure of sensitive data information or data.

The most important terms in cloud is virtualization, which provides invisible connectivity where as another terms like CCSs (cloud computing services) which is used for start, move, stop, and rescheduled the work load services on demand and CSPs (Cloud service provider) is used as service providing throughout the corner.

VMs runs on computing h/w that may be shared by cloud tenants. This is a phase from where a serious attacks is detected; because from this steps the services gets distributed throughout the different organization. So; a million dollar question is arises like can this problem statement prevents us from problem like pattern isolation and the hypervisor (HIV) get's solved by using IaaS trust Services. Hence fedral government has issued security controls that CSPs must implement to obtain FEDRAMP CCSs security certification that are totally based on National Institute Of Standards & Technology (NIST)cloud security guidelines.

But these steps cannot assures the 100% security to the user's; So the main motive is to publish this paper to provide a wide details of I a a S, CCS s, and CSPs to show how the problem's of security gets handled by our services provider's.

Cloud – Trust can asses the relative level of security offered by alternatives CSPs or cloud architecture. While IaaS is infrastructure as a service which gets involved with this service and provides u s more secure layers at the virtualization; because it covers all the h/w related security

Which never seen in the case of cloud computing.

It uses the probability based consideration on Navies Bayesian network rule to implement more secure environment

Hence it includes two key high level security rules to collect all the security status at a single frame. These are the keys shown below;

>There is a probability of an access high values of data based on APT.

>Probability the APT is detected by cloud tenant or CCS Security monitoring system.

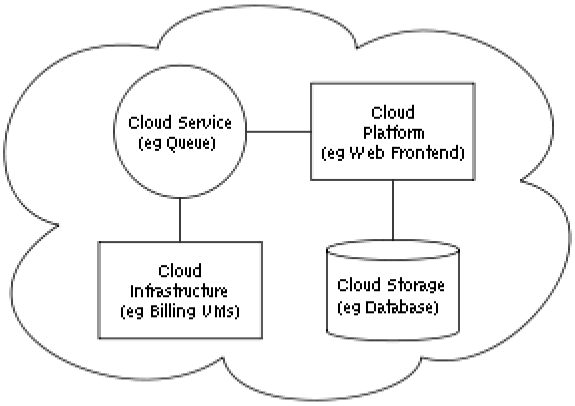
The very first point express about the high values data can be erased from the CCS, While Second is to express about detection of intrusions into a tenant's cloud n/w.

II. EXISTING SYSTEM

Today there are too many problems faced by small co-operates companies and also even by big companies facing security problems but they pays a lots of money on it. So there are problems related to overloading the cloud tenants services by the provider's it is arises due to using old system concepts based on plat-form services.

III. EXISTING SYSTEM ALGORITHMS

Specifically, Here We Are Going To Apply Navies Bayesian Networks Channel To Short Security Concern Over Cloud Tenant Data Storage.


Cloud Service (eg Queue)
Cloud Platform (eg Web Frontend)
Cloud Infrastructure (eg Billing VMs)
Cloud Storage (eg Database)

In the above diagram we show the existing architectural diagram which clears how the older version works.

IV. PROPOSED SYSTEM

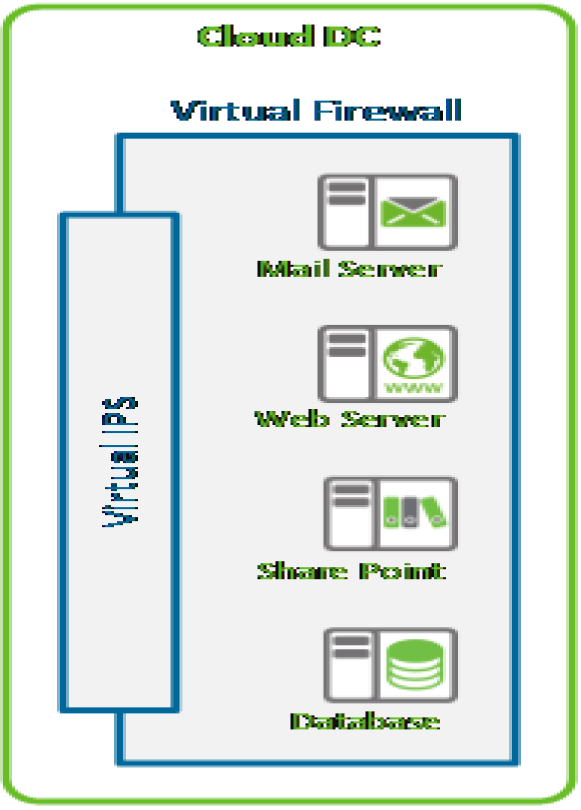
This level provides quantitative high level security assessments of IAAS, CCSs and CSPs.

Cloud trust is only the unique attacks deployed on the system.

- We illustrated that the use of cloud trust was used in US government agency and it shows how CCSs architectures protect that government data.

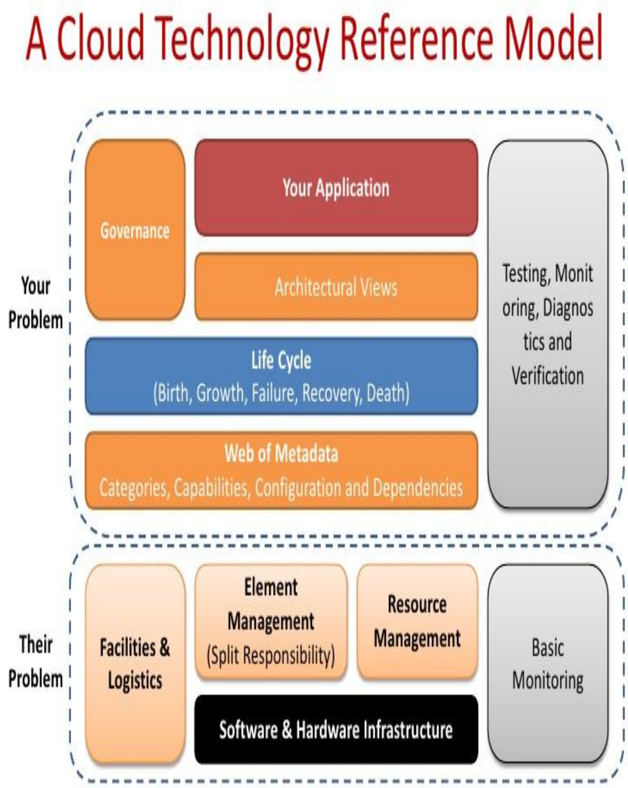
- We define a trust zone (TZ) which is just the addition of network segmentation and identity and access management (IAM) controls. Cloud TZs can be implemented devices, virtually using virtual firewall and switching applications. IAM systems use usernames, passwords, and access control lists (ACLs). Access is granted for legitimate requests from users that have been authenticated and authorized. These proposed system is a logical ones with it limited boundry.

There is a diagram of virtual system which indicate the security level of cloud.



As we seen in above diagram where to many share points is located like web server, share point, database, mail server.

ARCHITECTURE & REFERENCE MODEL


A Cloud Technology Reference Model
Your Problem
Governance
Your Application
Architectural Views
Life Cycle
(Birth, Growth, Failure, Recovery, Death)
Web of Metadata
Categories, Capabilities, Configuration and Dependencies
Testing, Monitoring, Diagnostics and Verification
Their Problem
Facilities & Logistics
Element Management (Split Responsibility)
Resource Management
Software & Hardware Infrastructure
Basic Monitoring

This is how we limited the work on cloud deployment system based on infrastructure. Here we are providing testing and diagnosis blocks to checks an error or attacks at every single time. In the same block some application is providing and etc. This blocks represents the site of your problems menu, where as in the blocks of their problems represents the all problems related to service provider.

Types of Attacks explained in short;
>CCS ATTACKS PATH :- It includes outsiders and insider attacks. Outsider attacks means to attacks on cloud by taking three ways. The very first attacks decrease the cloud strength by applying rool mechanism in which the hole order of cloud gets destroyed. The Second outsider attacks through sealing the basic important documents. The last is attacks through those valid documents which was stolen by attacker and it helps him to accessing the service of cloud on existing id
>VM CPU & CHANNEL ATTACKS :- This attacks is only based on VM vulnerabilities as it takes advantages of VM co-residency which occurs only when the same h/w is shared by more than two VMs.

Here the all information can be cleaned from the target VM if the attacker's attacks on VM. Here we only define the VM when it they get operated and controlled in a specific and same physical machine and HV due to its co-resident.

Hence this provides a safe ways to detect attackers hence it first identify the valid documents and if it verify its correctness then VM permits To use the existing services.

V. CONCLUSIONS

- There are many more players in the on-demand market that many reports acknowledge

- These range from basic infrastructure offerings (IaaS), through platform support (PaaS) to full applications (SaaS)

- The long term cost of ownership may at first not

seem to add up, but take into consideration other factors such as reduced risk and added value and for many organization on-demand services make a lot of sense

At last we demonstrate how to use probability based calculation for security management services in future works. By applying Networks rules of Navies Bayseian theorm.

ACKNOWLEDGMENT

This work is supported by Prof.Amol Jadho, Prof.Mangesh Manake, Prof. Sharmila chopade of DYPIET,Ambi.

Also The online guide from youtube, providing me a wide ides about this topics.

REFERENCES

[1] W. Jansen and T. Grance, “Guidelines on security and privacy in public cloud computing,” *NIST Spec. Publ.*, pp. 800–144, 2011.

[2] P. Mell and T. Grance, “The NIST Definition of Cloud Compu-ting.” NIST, 2011.

[3] P. Jamshidi, A. Ahmad, and C. Pahl, “Cloud Migration Re-search: A Systematic Review,” IEEE Transactions on Cloud Compu-ting, vol. 1, no. 2, pp. 142–157, 2013.

[4] L. Vaquero, L. Rodero-Merino, and D. Morán, “Locking the sky: a survey on IaaS cloud

security," *Computing*, vol. 91, no. 1, pp.93–118, Jan, 2011.

[5] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in *Proceedings of the 16th ACM conference on Computer and communications security*, 2009, pp. 199–212.

[6] A. Sood and R. Enbody, "Targeted Cyber Attacks-A Superset of Advanced Persistent Threats," *IEEE Security and Privacy.*, Vol. 11, no. 1, Jan.-Feb., 2013.

[7] B. Krekel, "Capability of the People's Republic of China to conduct cyber warfare and computer network exploitation," U.S.-China Economic and Security REview Commission, Northrop Grumman Corp., DTIC Document, 2009.

[8] *FedRAMP Security Controls*, Federal Chief Information Officer's Council, [Online]. Available: http://cloud.cio.gov/document/fedramp-security-controls. [Ac-cessed: 29-Oct-2014].

[9] S. Zevin, *Standards for security categorization of federal information and information systems*. DIANE Publishing, 2009.

[10] M. Walla, "Kerberos Explained," May, 2000. [Online]. Availa-ble: http://technet.microsoft.com/en-us/library/bb742516. aspx. [Accessed: 12-Jan-2014].

[11] Microsoft, "Federation trusts," Aug 22, 2005. [Online]. Availa-ble: http://technet.microsoft.com/en-us/library/cc738707(v= ws.10).aspx. [Accessed: 12-Jan-2014].

[13] Amazon Web Services, "AWS | Amazon Virtual Private Cloud (VPC) – Secure Private Cloud VPN." [Online]. Available: http://aws.amazon.com/vpc/. [Accessed: 12-Jan-2014].

[14] J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gru-schka, and L. Lo Iacono, "All your clouds are belong to us: security analysis of cloud management interfaces," in *Proceedings of the 3rd ACM workshop on Cloud computing security workshop*, 2011, pp. 3–14.

[15] V. J. Winkler, *Securing the Cloud: Cloud computer Security tech-niques and tactics.* Elsevier, 2011.

[16] *Network Infrastructure Technology Overview*, Version 8, Release 3, Defense Information Systems Agency, August 27, 2010.

[17] G. Keeling, R. Bhattacharjee, and Y. Patil, "Beyond the Hyper-visor: Three Key Areas to Consider When Securing Your Cloud Infrastructure Platform," presented at the VMWorld 2012, San Fran-cisco, August, 2012 [Online]. Available: http://www.vmworld.com/docs/DOC-6257 [Accessed: 29-Oct-2014]

[18] A. Regenscheid, "BIOS Protection Guidelines for Servers (Draft)," 800-147B, Jul. 2012 [Online]. Available: http://csrc.nist.gov/publications/drafts/800-147b/draft-sp800-147b_july2012.pdf [Accessed: 29-Oct-2014].

[19] Trusted Computing Group, "Trusted Platform Module (TPM) Summary." [Online]. Available: http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary. [Accessed: 12-Jan-2014].

[20] S. Chalal, et. al., "Evolution of Integrity Checking with Intel® Trusted Execution Technology: an Intel IT Perspective." Intel, Aug. 2010 [Online]. Available: http://www.intel.com/content/dam/doc/white-paper/intel-it-security -trusted-execution-technology-paper.pdf. [Accessed: 29-Oct-14].