Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-24
National Conference on
A Modern Approach to Designing Implementation and Reinforcement of Quality Management System Organised by
ZES's, Zeal Institute of Management and Computer Application,
Narhe, Pune, Maharashtra, India
on 21st November 2019

A comparative study of cloud computing security models- Gaps and Opportunities

---

Dr.Rajesh Kumar Kashyap
Professor(MCA)ZIBACAR, Pune

Rajesh.kashyap@zealeducation.com

Abstract:

One of the most promising solutions in development in the Information technology sectoris attributed to the unprecedented growth in Cloud Computing which has made organizations technological worries a phenomenon of the past. Cloud computing acts as a means to maintain a flexible and scalable IT infrastructure that enables business agility for practicing managers who are trying to exploit the benefits of cloud computing for the efficient use of IT resources. Even though there are impending benefits arising out of cloud computing, there are a lot of risks and security concerns which are associated with it. This requires frequents security models being developed by cloud service providers to thwart the risks caused due to the vulnerabilities in the cloud. This research paper is an attempt to compare some of the existing cloud based security models and tries to find out the gaps existing in relation to the growing security concerns and tries to find out if there are any opportunities available to develop further measures to increase the security measures. Also a framework for a new model which can act as a replacement to the existing models which could make up for the gaps is attempted herewith.

Keywords—Cloud computing, Cloud Security models, vulnerabilities

Introduction:

The emergence of cloud computing has provided organizations with an opportunity of providing an array of on demand services in infrastructure, platform and software which are like the basic necessities of any IT enabled organizations. These services are designed in a way to cater to specific needs of customers of all sizes and capabilities. [1]. Software as a Service (SaaS) provided in the complete applications as a service such as CRM [2], whereas platform as a service(PaaS), such as a Google App Engine (GAE)[3], and infrastructure as a service (IaaS) which is playing an important role in providing an environment for deploying, running and managing virtual machines and storage.

Cloud computing provides an avenue for small and medium enterprises who otherwise have to make high capital investment for procuring IT infrastructure, highly skilled resources for development purposes and system administrators because of which they end with a high cost of ownership. What cloud computing provides is an alternative where it aims to deliver a network of virtual services which can be accessed virtually from literally anywhere from the world on a pay- as –use basis at a very competitive cost based upon the specific requirements of the organizations [1]. This in a way has reduced the large scale capital requirements to a large extent and provides an opportunity for organizations to focus on their core competencies and also delivering their value for their customers. Due to these benefits the adoption of cloud computing and the usage has increased manifold causing more organizations to join the bandwagon of cloud computing. But these benefits cannot override the security challenges and risks associated with cloud computing. Organizations have been constantly developing security models to thwart the risks caused due to the challenges in the cloud environment. But since cloud is a open source technology, there are many vulnerabilities which are getting constantly exposed and provides an opportunities for external hackers as well as malicious insiders who get access in the cloud system and cause damages. This is an attempt to compare the security architecture of the existing models and their capabilities in challenging the risks and to find out if there are any gaps

available followed by an attempt to list down the opportunities which can aide in development a comprehensive security model.

Cloud Computing and Security:

Cloud Security Alliance (CSA) which deals with cloud computing security has identified a set of 9 top threats named as 'Notorious Nine' which are:

1. Data breaches
2. Data loss
3. Traffic hijacking
4. Insecure interfaces and API's
5. Denial of Service
6. Malicious insiders
7. Cloud abuse
8. Insufficient due diligence
9. Technology vulnerabilities

Issues and Challenges:

Some of the major issues and challenges in cloud computing are Port Scanning, IP Spoofing, DNS poisoning and phishing.

- Packet Sniffing is an activity done by malicious users to analyze the data packets sent over a cloud.
- When a malicious user impersonates a legitimate users IP address to access information through the use of that IP address an IP Spoofing occurs.
- In case of the exhaustion of host servers which is caused by malicious users resulting in legitimate users not gaining access to resources, it results in a loss of cost to the company

as well time. When external users can cause so much damage it is easy for internal users who are authorized to gain access to resources without being detected.

- An Insider has higher privileges and higher access with respect to network, security, mechanism and resources for them to attack and cause more damage than caused by an external users.

Vulnerabilities in the cloud:

Some of the major cloud specific vulnerabilities are

- Insecure Interfaces and Application Programming Interfaces
- Malicious Insiders
- Virtualized Technology
- Data Loss or Leakage
- Account or Service Hijacking
- Unknown Risk Profile
- Session Riding and Hijacking
- Virtual Machine Escape
- Reliability and Availability of Service
- Insecure Cryptography
- Data Protection and Portability
- Vendor Lock In

Security Concerns:

Some of the major security concerns with the cloud are given below:

- Legal issues due to laws of the land.
- Incompatibility of one provider's access controls to another in case of transfer[9].

- Ownership issues related to the encryption keys
- Integrity of the data.
- The level of data which can be stored and the time period it can be stored.
- The issue of physical control of cloud security being compromised.
- Fluidic nature of virtual machines.
- In case of Payment Card Industry Data Security Standard (PCI DSS) data logs must be provided to security managers and regulators. [10][11[12]
- It is imperative for users to keep them up to date with application improvements to be sure they are protected.

Cloud Security Models:

The cloud based models which are taken for consideration are

1) Vormetric Data Security Platform
2) Trend Micro Secure Data
3) Open VPN server
4) AWS EC2-Classic network
5) IETF IP Security Architecture (IPSec)

1. **Vormetric Data Security Platform:** The Vormetric Data Security Platform is built on an extensible infrastructure and features several products that can be deployed individually, while offering efficient, centralized key management. These products deliver capabilities for transparent file-level encryption, application-layer encryption, tokenization, cloud encryption gateway, integrated key management, and security intelligence logs. Through the platform's centralized key management and flexible implementation, it enables users to address security policies and compliance mandates across databases, files, and big data environments—whether assets are located in the

cloud, virtual or traditional infrastructures. With this platform's comprehensive, unified capabilities, users can efficiently scale to address your expanding security and compliance requirements, while significantly reducing total cost of ownership (TCO).

Key Attributes:-

The key attribute of this solution is

- Low total cost of ownership
- Maximizing staff and resource efficiency
- Strengthening security compliance

2. **Tren Micro Secure Data:** Trend Micro Secure data helps to ensure compliance with data protection solutions built into a unified, centrally managed framework powered by the Trend Micro™ Smart Protection Network™.Enterprise Data Protection secures data from gateway to mobile devices by integrating a full set of data security products within your existing Trend Micro enterprise security suite. By combining threat and data protection in a flexible, centrally-managed solution, it lowers the cost and effort to deploy and manage while closing critical security and compliance gaps—for complete end user protection.

Enterprise Data Protection product set includes:

- Trend Micro™ Integrated Data Loss Prevention
- Trend Micro™ Mobile Security
- Trend Micro™ Endpoint Encryption
- Trend Micro™ Email Encryption Gateway

3. **Open VPN server:** OpenVPN Access Server is a full featured secure network tunneling VPN software solution that integrates OpenVPN server capabilities, enterprise management capabilities, simplified OpenVPN Connect UI, and OpenVPN Client software packages that accommodate Windows, MAC, Linux, Android, and iOS environments. OpenVPN Access Server supports a wide range of configurations, including secure and granular remote access to internal network and/ or private cloud network resources and applications with fine-grained access control.

4. **AWS EC2-Classic network :**

   Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) cloud. Using Amazon EC2 eliminates the need to invest in hardware up front, so organizations can develop and deploy applications faster. Amazon EC2 can be used to launch as many or as few virtual servers as needed, configure security and networking, and manage storage. Amazon EC2 enables options to scale up or down to handle changes in requirements or spikes in popularity, reducing the need to forecast traffic.

Amazon EC2 provides the following features:

- Virtual computing environments, known as *instances*
- Preconfigured templates for your instances, known as *Amazon Machine Images (AMIs)*, that package the bits you need for your server (including the operating system and additional software)
- Various configurations of CPU, memory, storage, and networking capacity for your instances, known as *instance types*

- Secure login information for your instances using *key pairs* (AWS stores the public key, and you store the private key in a secure place)
- Storage volumes for temporary data that's deleted when you stop or terminate your instance, known as *instance store volumes*
- Persistent storage volumes for your data using Amazon Elastic Block Store (Amazon EBS), known as *Amazon EBS volumes*
- Multiple physical locations for your resources, such as instances and Amazon EBS volumes, known as *regions* and *Availability Zones*
- A firewall that enables you to specify the protocols, ports, and source IP ranges that can reach your instances using *security groups*
- Static IP addresses for dynamic cloud computing, known as *Elastic IP addresses*
- Metadata, known as *tags*, that you can create and assign to your Amazon EC2 resources
- Virtual networks you can create that are logically isolated from the rest of the AWS cloud, and that you can optionally connect to your own network, known as *virtual private clouds* (VPCs)

5. IETF IP Security Architecture (IPSec) :

IPsec is designed to provide interoperable, high quality,cryptographically-based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, detection and rejection of replays (a form of partial sequence integrity), confidentiality (via encryption), and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection in a standard fashion for all protocols that may be carried over IP (including IP itself). IPsec includes a specification for minimal firewall functionality, since that is an essential aspect of access control at the IP layer. Implementations are free to provide more sophisticated

firewall mechanisms, and to implement the IPsec-mandated functionality using those more sophisticated mechanisms.

Based upon the analysis of the usage of these existing models, the following are the drawbacks or the missing GAPS in these models. These Gaps are what provides an opportunity for a better security model which will take case of these and provides scope for better data security in a cloud based environment.

PARA METERS	GAPS				
	VORMETRIC DATA SECURITY PLATFORM	TREND MICRO SECURE DATA	OPEN VPN SERVER	AWS CLASSIC	IETF IP SECURITY ARCHITECTURE (IPSEC)
FIREWALL SECURITY	Does Not Provide	Does Not Provide	Encrypt data in transit using PKI – Certificates between AWS VPC and other Network	An EIP is disassociated from your instance when you stop it.	Can be Implemented

HOST LEVEL ACCESS CONTROL	Does Not Provide	Does Not Provide	Require a dedicated EC2 Instance with hourly charges.	Separate subnet creation is not possible	Not available
NATTING FACILITY	Does Not Provide	Does Not Provide	2 Factor authentication is provided	Does Not Provide	Does Not Provide
COST OF OWNERSHIP	License Model very high	License Model very high	Requires separate Public IP	Public IP is required to access Internet, there by exposing the instance to world	very high
TIME OF IMPLEMENTATION	More Time Required	More Time Required	More Time Required	Normal Time Required	More Time Required

Proposed Model:

The model here proposed will have the following additional features which are being missed in the existing security models in cloud computing.

1. Providing Host access Control at all levels.
2. Providing a Public IP is not mandatory for Internet access, and it can be accessed through NAT Instance which acts as Gateway.

3. Proving Natting facility with NAT instances
4. Options to create separate subnets in VPC
5. Providing data-at-rest encryption.
6. Providing comprehensive firewall security through Security Group & Network ACL's
7. Providing minimal cost of ownership by not using a license based subscription model
8. Reduced implementation time
9. To provide data in transit encryption using SSH because of which all data traffic can be routed through SSH Tunneling.
10. Should not be requiring additional Instance for every activity. NAT instance doubles up as SSH Gateway point from where tunneling can be done to other instances.

Thus if we are able to develop a comprehensive model which includes these suggested features it will be most beneficial for Small and Medium enterprises who are apprehensive about exploiting die to the cost of ownership as well the growing scale of vulnerabilities and the risks involved in using them. This paper is not an attempt to find the pitfalls in the models being in existence but an attempt to explore additional opportunities which if taken care would increase the usage of cloud among the stakeholders.

References:

[1] R. Buyya, C. Yeo, S. Venugopal, J. Broberg, I. Brandic, Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems, Vol. 25, No. 6, pp. 599–616, 2009.

[2] M. Cusumano, Cloud computing and SaaS as new computing platforms, Communications of the ACM Vol. 53, No. 4, pp. 27–29, 2010.

[3] E. Ciurana, Developing with Google App Engine, Apress, Berkeley, CA, USA, 2009.

[4] Leavitt, N. Is Cloud Computing Really Ready for Prime Time, IEEE Computer, Vol. 42, No. 1, pp. 15–20, 2009.

[5] H.Takabi, J.B.D.Joshi, G.Ahn., ―Security and Privacy Challenges in Cloud Computing Environments‖, IEEE Security Privacy Magazine, Vol 8, pp.24-31, 2010.

[6] S. Qaisar, K.F. Khawaja, Cloud Computing: Network/Security Threats and Countermeasures, Interdisciplinary journal of con-temporary research in business, Vol.3, No 9, p. 1323-1329, 2012.

[7] J.R. Winkler, Securing the Cloud: Cloud Computer Security Techniques and Tactics, Technical EditorBillMeine, Elsevier Publishing, 2011.

[8] P. Mell and T. Grance, ―The NIST Definition of Cloud Computing, Effectively and Securely Using the Cloud Computing Paradigm‖, DOI=http://csrc.nist.gov/groups/SNS/cloud-computing/cloudcomputing-v26.ppt.

[9] M. Casassa-Mont, S. Pearson and P. Bramhall, "Towards Accountable Management of Identity and Privacy: Sticky olicies and Enforceable Tracing Services", Proc. DEXA 2003, IEEE Computer Society, 2003, pp. 377-382

[10] https://www.pcisecuritystandards.org/index.shtml

[11] http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_ Security_Standard, 24 January 2010

[12] J. Salmon, "Clouded in uncertainty – the legal pitfalls of cloud computing", Computing, 24 Sept 2008, http://www.computing.co.uk/computing/features/2226701/clouded-uncertainty-4229153

[13] KrešimirPopović, ŽeljkoHocenski," Cloud computing security issues and challenges", MIPRO 2010, May 24-28, 2010, Opatija, Croatia

[14] Gartner: Seven cloud-computing security risks, 02 July 2008,http://www.infoworld.com/d/security-central/gartnerseven-cloud-computing-security-risks-853?page=0,0