ISSN No. 0976-5697

Volume 4, No. 6, May 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICAL

Available Online at www.ijarcs.info

A Review Paper on Cloud Computing Security

Miss. Trupti S. Lokhande*, Prof. Rajeshri R. Shelke
M.E. (CSE) *, CSE Department
H. V. P. M College of Engineering & Technology
Amravati, Maharashtra.
lokhandetrupti22391@gmail.com*, rajeshrishelke@rediffmail.com

Abstract: Cloud computing has become an increasingly popular means of delivering valuable, IT-enabled business services. Adopting cloud technology can be an affordable way to get access to a dynamically scalable, virtualized computing environment. The cloud provider is responsible for the environment, so organizations can make use of resources for short periods of time without having to maintain the environment when it is not being used. While cloud computing models are attractive because of their flexibility and cost effectiveness, certain challenges must be addressed in order to provide a viable option to traditional data services. First and foremost is the issue of security. The externalized aspect of outsourcing can make it harder to maintain data integrity and privacy, support data and service availability, demonstrate compliance, and secure highly available access to applications and information. In short, cloud computing can present an added level of risk.
This paper discusses security and availability-related challenges in cloud computing environments. The paper takes a closer look at the shared security responsibilities that exist between consumer and provider. Finally, the paper investigates high availability concerns and demonstrates how to help improve the resilience of your virtual servers in a cloud computing environment.

Keywords: cloud computing, security, IaaS, PaaS, SaaS

I. INTRODUCTION

A. *What Is Cloud Computing?:*

Cloud computing refers to the use of networked infrastructure software and capacity to provide resources to users in an on-demand environment. With cloud computing, information is stored in centralized servers and cached temporarily on clients that can include desktop computers, notebooks, handhelds and other devices. Cloud infrastructure can reside within the company's datacenters (as internal clouds or on-premise solutions) or on external cloud computing resources (off-premise solutions available through service providers). It encompasses any subscription-based or pay-per-use service that extends existing IT capabilities. Typically, Clouds utilize a set of virtualized computers that enable users to start and stop servers or use compute cycles only when needed (also referred to as utility computing). By design, cloud computing is scalable, flexible and elastic offering IT staff a way to easily increase capacity or add additional capabilities on demand without investing in new and expensive infrastructure, training new personnel or licensing more software service over a net-work, including storage, routers, virtual systems, hardware and servers.

B. *Three delivery models:*

a. ***Software as a Service (SaaS):*** The consumer uses an application, but does not control the operating system, hardware or network infrastructure on which it's running.

b. ***Platform as a Service (PaaS):*** The consumer uses a hosting environment for their applications. The consumer controls the applications that run in the environment (and possibly has some control over the hosting environment), but does not control the operating system, hardware or network infrastructure on which they are running. The platform is typically an application framework.

c. ***Infrastructure as a Service (IaaS):*** The consumer uses "fundamental computing resources" such as processing power, storage, networking components or middleware. The consumer can control the operating system, storage, deployed applications and possibly networking components such as firewalls and load balancers, but not the cloud infrastructure beneath them. They are shown below

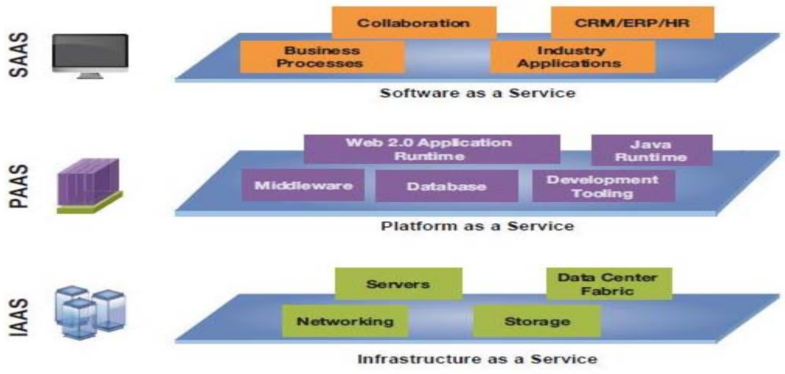

Figure: 1

II. SECURITY AND COMPLANCE IN CLOUD COMPUTIG

A. *Security Stack in cloud computing:*

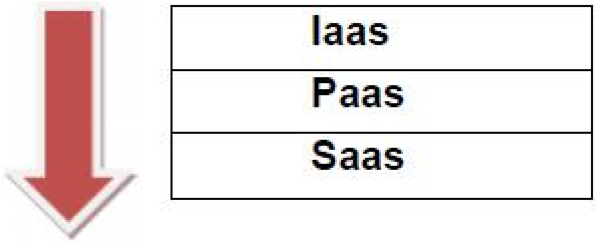

Figure: 2

Lower down the stack the cloud vendor provides, the more security issues the consumer has to address or provide.

B. *Security Issues in SaaS:*

Following key security element should be carefully considered as an Integral part of the SaaS deployment process:

a. Data Security
b. Network Security
c. Data locality
d. Data integrity
e. Data access
f. Data Segregation
g. Authorization and Authentication
h. Data Confidentiality
i. Web Application security
j. Data Breaches
k. Virtualization vulnerability
l. Availability
m. Backup
n. Identity Management on sign-on process

C. *Security Issues in PaaS:*

1.In PaaS, the provider might give some control to the people to build applications on top of the platform. But any security below the application level such as host and network intrusion prevention will still be in the scope of the provider. 2. Applications sufficiently complex to leverage an Enterprise Service Bus (ESB) need to secure the ESB directly, leveraging a protocol such as Web Service (WS) Security. The ability to segment ESBs is not available in PaaS environments. Metrics should be in place to assess the effectiveness of the application security programs. 3. Hackers are likely to attack visible code, including but not limited to code running in user context. They are likely to attack the infrastructure and perform extensive black box testing. The vulnerabilities of cloud are not only associated with the web applications but also vulnerabilities associated with the machine-to-machine Service Oriented Architecture (SOA) applications.

D. *Security Issues in IaaS:*

Taking virtual machines, which contain critical applications and sensitive data, off premise to public and shared cloud environments creates security challenges for organizations that have relied on network perimeter defense as the main method to protect their datacenter. It may also revoke compliance and breach security policies. OS Security issues also alive in IaaS.

III. SECURITY CONCERNS IN CLOUD COMPUTING

While cloud computing has the potential to make IT operations leaner and less expensive, many of the respondents of the 8th annual Global Information Security survey that was published in the CIO magazine have qualms about security, and more than 60 percent of the respondents admitted to having little to no confidence in the ability to secure assets that are placed in the cloud .The seven security concerns as shown in Figure2.

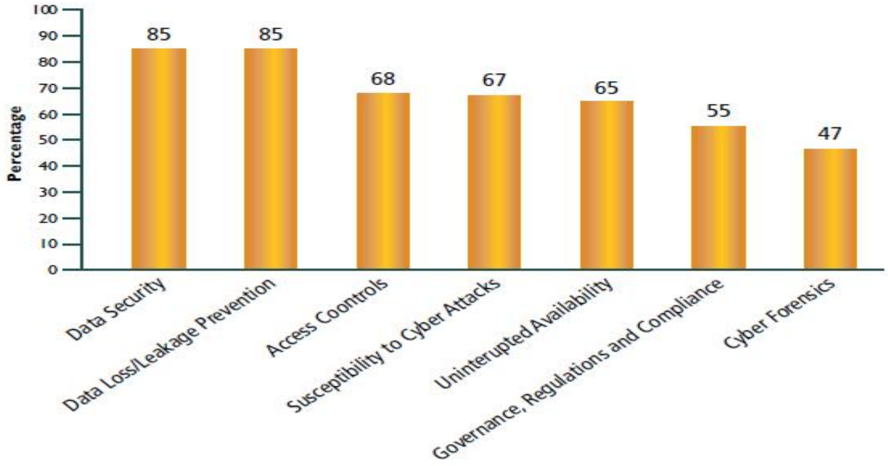

Figure 2. Security Concerns in Cloud Computing

A. *Data Security:*

The primary security concern in cloud computing is data disclosure to unauthorized systems or personnel. When an organization's data is placed in what seems to be a nebulous cloud, the data owner is in the inside of the organization while the data custodian (provider) is on the outside, making it text format. The data needs to be protected using cryptographic protection mechanisms such as encryption or hashing. In order to facilitate easy migration in the cloud, data storage considerations must also factor in the metadata of the network segment and the application.

B. *Access Controls:*

Next only to confidentiality assurance, access control is the most important security concern in the model of cloud computing. This is particularly true when applications and data are hosted in a public cloud. When multiple tenants are supported by a cloud, then the scope of any breach is not contained to a single tenant. The breach of an application in a shared hosted cloud could result in the breach of other applications that use the same pool of resources in that cloud The model of cloud computing, as the storage media will need to be provisioned again, one must resort to the weakest form of data disposal, which is overwriting (or formatting).

C. *Data Loss or Leakage Prevention*:

When infrastructure and systems are provisioned dynamically, it is likely that the data that resides on that shared pool of resources can be leaked to entities that have access to those same infrastructural components. One element of confidentiality assurance is the ability to dispose data securely. In clouds that house storage media not controlled by the tenant, verification of data disposal mechanisms so that there is no remanence is crucial

D. *Susceptibility to Cyber Attacks:*

The cyber threats that are observed in the model of cloud computing are not that different from the traditional mode of computing. Both from a programming as well as from a hosting perspective, focus on security is required. The Cloud Security Alliance's publication entitled "Top Threats to Cloud Computing" mentions seven top threats. These include the abuse and nefarious use of computing resources using cracking techniques and malware, insecure application programming interfaces, malicious insiders, shared technology vulnerabilities such as virtualization exploits of the hypervisor and cloud bursting which is characterized by the inability of the cloud to handle spiked demands, data loss/leakage, hijacking of accounts, services and traffic, and an unknown risk profile of the provider due to the general lack of transparency into the provider's inner workings, processes, and procedures.

E. *Uninterrupted Availability:*

Cloud computing has an impact on the availability tenet of security. There are two main schools of thought when it comes to the availability of resources in the cloud computing model. On one hand, one may argue that because the processing load is distributed in the cloud, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks cannot cause significant damage in the cloud. On the other hand, the consumer of the provider's services will still be liable to bear the cost in this pay-per-use model of computing. This cost may quite easily be greater than the cost of downtime caused by the DoS or DDoS attacks. Additionally, the centralization of cloud services can reduce the attack surface but this could also create a single point of failure and so layered defense strategies are essential.

F. *Governance, Regulations and Compliance (GRC) in the Cloud:*

Two of the biggest concerns that the adopters of cloud computing have is their uncertainty in enforcing security policies at the provider site, and their inability to support compliance audits in the cloud. Though the assurance responsibilities are spread between the cloud service provider and the consumer (tenant), since adequate governance frameworks and regulations are still lacking, the onus is on the side of the consumer to not only verify the existence of adequate protection mechanisms, but in some cases to be responsible for the protection mechanism themselves. For example, Amazon essentially requires that the user or enterprise consumer handle all data encryption and key management, while Amazon provides services for data recovery and auditing. At no time should governance, risk, and compliance activities be outsourced. The Cloud Security Alliance is a commendable undertaking that aims to establish and promote best practices in the cloud.

G. *Cyber Forensics in the Cloud:*

The elasticity of the cloud, where users pay only for what they need on demand, provides challenges to a cyber forensics investigator, since resources such as disk space and memory that are allocated to one's organization today may be gone or overwritten by tomorrow, or, even worse, allocated to someone else (including potentially your competitor). Additionally, the lack of understanding of the underlying infrastructure in the IaaS model makes it difficult, upon a breach, for an investigator to gather evidence. With blurred ownership boundaries, the collection of physical evidence using static and live forensic tools from virtual environments is a challenge.

IV. SOLUTION APPROACHS

The following outlines four distinct security technologies –firewall, intrusion detection and prevention, integrity monitoring and log inspection- that can be deployed as software on virtual machines to increase protection and maintain compliance integrity of servers and applications as virtual resources move from on-premise to public cloud environment

A. *Firewall:*

Decreasing the attack surface of virtualized servers in cloud computing environments. A bi-directional firewall, deployed on individual virtual machines can provide centralized management of server firewall policy. It should include predefined templates for common enterprise server types and enable the following:

a. Virtual machine isolation
b. Fine-grained filtering(Source and Destination Address, Ports)
c. Coverage of all IP-based protocols (TCP, UDP, ICMP, …)
d. Coverage of all frame types (IP, ARP, …)
e. Prevention of Denial of Service (DoS) attacks
f. Ability to design policies per network interface
g. Location awareness to enable tightened policy and the flexibility to move the virtual machine from on-premise to cloud resources

B. *Intrusion Detection and Prevention (IDS/IPS):*

Shield vulnerabilities in operating system and enterprise applications until they can be patched, to achieve timely protection against known and zero-day attacks. As previously noted, virtual machines and cloud computing servers use the same operating systems, enterprise and web applications as physical servers. Deploying intrusion detection and prevention as software on virtual machines shields newly discovered vulnerabilities these applications and OSs to provide protection against exploits attempting to compromise virtual machines.

C. Integrity Monitoring:

Integrity monitoring of critical operating system and application files (files, directories, registry keys and values, etc.) is necessary for detecting malicious and unexpected changes which could signal compromise of cloud computing resources. Integrity monitoring software must be applied at the virtual machine level.

D. Log Inspection:

Log inspection collects and analyzes operating system and application logs for security events. Log inspection rules optimize the identification of important security events buried in multiple log entries. These events can be sent to a stand-alone security system, but contribute to maximum visibility when forwarded to a security information and event management (SIEM) system or centralized logging server for correlation, reporting and archiving. Like integrity monitoring, log inspection capabilities must be applied at the virtual machine level. Log inspection software on cloud resources enables:

a. Suspicious behavior detection
b. 2.Collection of security-related administrative actions
c. Optimized collection of security events across your data cent

V. CONCLUSION

After discussing the security issues this paper conclude that we should be careful about the security concerns while putting our business on Cloud. There are open research challenges in cloud computing security which demand intensive research. The security model should be probably secure. Security as a Service should be provided to the cloud users.

VI. REFERENCES

[1]. www.cloudreadyscurity.com

[2]. www.cloudsecurityalliance.org/guidance

[3]. Definition of Cloud Computing by the National Institute of Standards and Technology (NIST). 2011 (ISC)2 Global Information Security Workforce Study 8th Annual Global Information Security Survey, CIO Clash of the Clouds, Kim S. Nash. CIO Magazine. May 2010

[4]. CSO Magazine, November 2010. Security Questions for Big Clouds – Gregory Machler Clearer Definition, New Metrics for Cloud Security. CSO, Jan 2010.

[5]. Ariel Silverstone Cloud Assurance Still Missing. Allan Carey Cloud Computing for the Federal Community. Hannah Wald. Information Assurance Technology Analysis Center (IATAC) Newsletter. Volume 13 Number 2. Spring 2010.

[6]. Establishing Trust in Cloud Computing. Dr. Bret Michael and Dr. George Dinolt. Information Assurance Technology Analysis Center (IATAC) Newsletter. Volume 13 Number 2. Spring 2010.

[7]. Turbulence in the Clouds. Peter Fretty. Infosecurity Professional. Issue Number 12. Pp 8-11.

[8]. Cyber Forensics in the Cloud. Scott Zimmerman and Dominick Glavach. Information Assurance Technology Analysis Center (IATAC) Newsletter. Volume 14 Number 1. Winter 2011.

[9]. Top Threats to Cloud Computing, Version 1.0. Cloud Security Alliance.

[10]. www.malwaredomainlist.com/

[11]. blogs.zdnet.com/security

[12]. www.programmableweb.com

[13]. securitylabs.websense.com/content/Blogs