Cloud Security Challenges and Solutions

Madhavi Dhingra
ITM College, Gwalior (M.P.), India
madhavi0685@gmail.com

***Abstract* – Cloud computing opens up a new world of opportunities for businesses, but mixed in with these opportunities are numerous security challenges that need to be considered and addressed prior to committing to a cloud computing strategy. This paper briefly describes the security challenges faced by the cloud, and the solutions in terms of the security technologies that will help in protecting and securing the cloud.**

Keywords- Cloud Computing Security, Cloud Security, Security, Cloud Challenges

I. INTRODUCTION

Cloud computing, which gets its name as a metaphor for the Internet [1], is becoming a popular term and has been used by an increasing number of organisations. In cloud computing environment, services are not provided by a single server or a small group of servers; instead, various computing and storage services are provided by some collection of data centres owned and maintained by a third party [2].

While cloud computing is more and more popular, security becomes a great concern due to the distributed nature of cloud. According to IDC [3], security became the biggest challenge to cloud computing.

A. Security Issues Associated with Cloud

There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers.[4] In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information.[5]

The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service.[6]Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking. This introduces an additional layer – virtualization - that itself must be properly configured, managed and secured.[7]

II. CLOUD CHALLENGES CATEGORIZATION

Cloud computing security challenges fall into three broad categories[8]:

A. Data Protection: Securing your data both at rest and in transit

Implementing a cloud computing strategy means placing critical data in the hands of a third party, so ensuring the data remains secure both at rest (data residing on storage media) as well as when in transit is of paramount importance. Data needs to be encrypted at all times, with clearly defined roles when it comes to who will be managing the encryption keys. In most cases, the only way to truly ensure confidentiality of encrypted data that resides on a cloud provider's storage servers is for the client to own and manage the data encryption keys.

B. User Authentication: Limiting access to data and monitoring who accesses the data

Data resting in the cloud needs to be accessible only by those authorized to do so, making it critical to both restrict and monitor who will be accessing the company's data through the cloud. In order to ensure the integrity of user authentication, companies need to be able to view data access logs and audit trails to verify that only authorized users are accessing the data. These access logs and audit trails additionally need to be secured and maintained for as long as the company needs or legal purposes require. As with all cloud computing security challenges, it's the responsibility of the customer to ensure that the cloud provider has taken all necessary security measures to protect the customer's data and the access to that data.

C. Disaster and Data Breach Contingency Planning

With the cloud serving as a single centralized repository for a company's mission-critical data, the risks of having that data compromised due to a data breach or temporarily made unavailable due to a natural disaster are real concerns. Much of the

liability for the disruption of data in a cloud ultimately rests with the company whose mission-critical operations depend on that data, although liability can and should be negotiated in a contract with the services provider prior to commitment. A comprehensive security assessment from a neutral third-party is strongly recommended as well.

Companies need to know how their data is being secured and what measures the service provider will be taking to ensure the integrity and availability of that data. Additionally, companies should also have contingency plans in place in the event their cloud provider fails or goes bankrupt.

III. SECURITY ISSUES BEFORE SELECTING A CLOUD

Cloud computing has "unique attributes that require risk assessment in areas such as data integrity, recovery, and privacy, and an evaluation of legal issues in areas such as e-discovery, regulatory compliance, and auditing," Gartner says.

Here are seven of the specific security issues Gartner says customers should raise with vendors before selecting a cloud vendor.[9]

- Privileged user access. Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls". Get as much information as you can about the people who manage your data. "Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access," Gartner says.

- Regulatory compliance. Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are "signaling that customers can only use them for the most trivial functions," according to Gartner.

- Data location. When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers, Gartner advises.

- Data segregation. Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. "Find out what is done to segregate data at rest," Gartner advises. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists. "Encryption accidents can make data totally unusable, and even normal encryption can complicate availability," Gartner says.

- Recovery. Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster. "Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure," Gartner says. Ask your provider if it has "the ability to do a complete restoration, and how long it will take."

- Investigative support. Investigating inappropriate or illegal activity may be impossible in cloud computing, Gartner warns. "Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then your only safe assumption is that investigation and discovery requests will be impossible."

- Long-term viability. Ideally, your cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your data will remain available even after such an event. "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application,"

IV. SECURITY SOLUTIONS FOR VIRTUAL MACHINES

Virtualization is the enabling technology for cloud computing. Organizations not leveraging cloud computing today are likely looking to cloud computing for tomorrow. Datacenters that have consolidated physical servers to multiple virtual machine instances on virtualized servers can take immediate steps to increase security in their virtualized environment, as well as prepare these virtual machines for the migration to cloud environments when appropriate.

The following outlines five distinct security technologies—firewall, intrusion detection and prevention, integrity monitoring, log inspection, and malware protection—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 environments.[10]

A. FIREWALL

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

- Virtual machine isolation
- Fine-grained filtering (Source and Destination Addresses, Ports)
- Coverage of all IP-based protocols (TCP, UDP, ICMP)
- Coverage of all frame types (IP, ARP)
- Prevention of Denial of Service (DoS) attacks
- Ability to design policies per network interface
- 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 systems 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 in these applications and OSs to provide protection against exploits attempting to compromise virtual machines. In particular, vulnerability rules shield a known vulnerability—for example, those disclosed monthly by Microsoft—from an unlimited number of exploits.

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.

An integrity monitoring solution should enable:

- On-demand or scheduled detection
- Extensive file property checking, including attributes
- Directory-level monitoring
- Flexible, practical monitoring through includes/excludes
- Auditable reports

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:

- Suspicious behavior detection
- Collection of security-related administrative actions
- Optimized collection of security events across your datacenter

E. VIRTUALIZATION-AWARE MALWARE PROTECTION

Virtualization-aware malware protection leverages APIs such as the VMware VMsafe APIs to secure both active and dormant virtual machines. Layered protection uses dedicated scanning virtual machines coordinated with real-time agents within each virtual machine. Virtualization-aware malware protection can also preserve performance profile of virtual servers by running resource-intensive operations such as full system scans from a separate scanning virtual machine.

- Prevention of malware impact on active and dormant virtual machines
- Protection from attacks that uninstall, inhibit, or fraudulently patch antivirus security
- Tight integration with virtualization management consoles
- Automatic security configuration of new virtual machines

V. SECURITY DEPLOYMENT CONSIDERATIONS

Cloud computing deployments are going to increase over time. Virtual environments that deploy the above mentioned security mechanisms on virtual machines, effectively make these VMs cloud-ready. Three additional considerations will help to maximize the effectiveness of any security deployment:

- Software agents on virtual machines enable greater security for these virtual machines. Consolidating protection mechanisms will enable economies of scale, deployment and ultimately cost savings for enterprises and service providers.
- Enterprises will not likely move all computing to cloud resources. Any security mechanisms should be consistent across physical, virtual and cloud computing instances of servers and applications. These deployments should also be able to be centrally managed and integration with existing security infrastructure investments such as virtual integration tools (for example, VMware vCenter), security information and event management solutions (like ArcSight, NetIQ, and RSA Envision),enterprise directories (Active Directory) and software distribution mechanisms (such as Microsoft SMS, Novel Zenworks and Altiris).
- Many tools that are currently deployed, such as software firewall and host-based intrusion prevention systems (HIPS), may migrate seamlessly to cloud environments. In addition, free tools and software, such as VM Protection, are available for deployment in virtual and cloud environments.

VI. CONCLUSION

As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through adoption of this new model. Cloud computing offers many benefits, but it also is vulnerable to threats. As the uses of cloud computing increase, it is highly likely that more criminals will try to find new ways to exploit vulnerabilities in the system. There are many underlying challenges and risks in cloud computing that increase the threat of data being compromised.

To help mitigate the threat, cloud computing stakeholders should invest heavily in risk assessment to ensure that the system encrypts to protect data; establishes trusted foundation to secure the platform and infrastructure; and builds higher assurance into auditing to strengthen compliance. Security concerns must be addressed in order to establish trust in cloud computing technology.

REFERENCES

[1] A. Velte, T. Velte, and R. Elsenpeter, Cloud computing: a practical approach, New York: McGraw-Hill, 2010.

[2] H. Jin, S. Ibrahim, T. Bell, L. Qi, H. Cao, S. Wu, and X. Shi, “Tools and technologies for building clouds”, in Cloud Computing: Principles, Systems and Applications, N. Antonopoulos and L.Gillam, Eds, London: Springer, 2010.

[3] IDC, IT Cloud Services User Survey, 2008.

[4] "Swamp Computing a.k.a. Cloud Computing". Web Security Journal. 2009-12-28. Retrieved 2010-01-25.

[5] Wik, Philip (2011-10). "Thunderclouds: Managing SOA-Cloud Risk". Service Technology Magazine. Retrieved 2011-21-21.

[6] Winkler, Vic. "Cloud Computing: Virtual Cloud Security Concerns". Technet Magazine, Microsoft. Retrieved 12 February 2012.

[7] Hickey, Kathleen. "Dark Cloud: Study finds security risks in virtualization". Government Security News. Retrieved 12 February 2012.

[8] Cloud Computing Security Challenges: http://www.webopedia.com/DidYouKnow/Hardware_Software/Security/cloud_computing_security_challenges_summary.html

[9] Gartner: Seven cloud-computing security risks: By Jon Brodkin. Retrieved JULY 02, 2008

[10] A Trend Micro White Paper | August 2009 : Cloud Computing Security

AUTHORS PROFILE

Madhavi Dhingra did MCA(Hons.) in year 2009, BCA in year 2005. Has worked as Assistant Systems Engineers in TCS, Mumbai in year 2009, worked as Lecturer in BVM College of Gwalior in year 2010,and is currently working as Assistant Professor in ITM College, Gwalior since 2011. Academic Achievements include qualifying UGC-NET and award of JRF in 2012. Also qualified GATE in same year. Five papers published in International Conferences and Journals. Member of IEEE, CSI and UACEE.