Security Issues and Solutions for Cloud Computing

Sherin Sreedharan[1], G.Kalpana[2]
[1]*M-Tech, Computer Science and Engineering.*
Dr.MGR Educational and Research Institute University.
Chennai-600095, India.
[2]*Assistant Professor, Computer Science and Engineering.*
Dr.MGR Educational and Research Institute University.
Chennai-600095, India.

***Abstract*—The "lower costs" of cloud services, "flexibility" and the "speed of deployment" are all vastly demanded by most of the organizations in today's world. However, a common concern remains amongst large enterprises is about the handover of the control of data to cloud providers. It is true that many technology hosting businesses are equipped to provide basic cloud services, but it is necessary for users to be satisfied that the host can protect the confidentiality, integrity and availability of data with controls and measures that are extensive, efficient and sophisticated. However, the perception of complicating a cloud's architecture, simply because of apparent security risks, should be resisted; a fine line has to be drawn between practicality and security. This paper gives an insight into the understanding on CLOUD, the service models available, Key challenges in setting up the CLOUD, focuses on the Security Issues related to CLOUD and describes the Security reference model.**

***Keywords*— Infrastructure-as-a-Service (IaaS); Platform-as-a-Service (PaaS); Software-as-a-Service (SaaS); Virtual Machine (VM)**

I.INTRODUCTION

Cloud computing has emerged as a way for IT businesses to increase capabilities on the fly without investing much in new infrastructure, training of personnel or licensing new software. The Cloud Computing offers dynamically scalable resources provisioned as a service over the web and so guarantees lots of economic advantages to be distributed among individuals and organizations. Cloud supports individuals and small businesses snap their fingers and instantly set up enterprise-class services.

Though the term Cloud Computing is becoming popular within the Information Technology (IT) market, at the same time issues like network performance, security ramifications and accountability are also associated with it. There are many security concerns associated with cloud computing, however, most of these issues fall into two main categories: (1) Security issues faced by cloud providers (organizations providing Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), or Infrastructure-as-a-Service (IaaS) via the cloud) and (2) security issues faced by their customers.

Enterprises, government agencies and service providers that operate cloud environments – as well as equipment vendors that build the network infrastructure gear on which clouds run 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. Technology enablers such as cloud performance and security testing tools can help them do that, as well as help them measure whether the metrics and results expected from the cloud are actually being delivered. During this paper, we offer a summary on security problems with Cloud Computing.

The paper is organized as follows. In Section II, we provide the service provider security issues. In section III security issues faced by the end user that apply to different Cloud Computing scenario, Then, In Section IV we outline the layered reference architecture for Security solutions. Finally concludes this paper in Section V.

II.SERVICE PROVIDER SECURITY ISSUES

The public cloud environments offered by the cloud supplier must ensure that a cloud computing resolution fulfills the security and privacy requirements of the respective organizations. The cloud supplier has to provision the safety controls necessary to safeguard the organization's information and applications, and additionally the proof provided regarding the effectiveness of these controls migrating organizational information and functions into the cloud.

Securing Data in Transmission

Encryption techniques are used for data in transmission. To provide the protection for data only goes where the customer wants it to go by using authentication and integrity and is not modified in transmission. SSL/TLS protocols are used here.

In Cloud environment most of the data is not encrypted in the processing time. But to process data for any application that data must be unencrypted. In a fully homomorphism encryption scheme advance in cryptography which allows data to be processed without being decrypted. To provide the confidentiality and integrity of data-in-transmission to and from cloud provider by using access controls like authorization, authentication, auditing for using resources, and

ensure the availability of the Internet-facing resources at cloud provider.

Privacy

Privacy is the one of the Security issue in cloud computing. Personal information regulations vary across the world and number of restrictions placed by number of countries whether it stored outside of the country. For a cloud service provider, in every jurisdiction a single level of service that is acceptable. Based on contractual commitments data can store within specific countries for privacy regulations, but this is difficult to verify. In private and confidential customer data fast rising for the consequences and potential costs of mistakes for companies that handle. But professionals develop the security services and the cloud service privacy practices. An effective assessment strategy must cover data protection, compliance, privacy, identity management, secure operations, and other related security and legal issues.

User Identity

In Organizations, only authorized users across their enterprise have access to the data and tools that they require, and all unauthorized users are blocked for access. In Cloud environments support a large enterprise and various communities of users, so these controls are more critical. Clouds begin a new level of privileged users working for the cloud provider is administrators. And an important requirement is privileged user monitoring, including logging activities. This monitoring should include background checking and physical monitoring. To coordinate authentication and authorization with the enterprise back-end or third-party systems are identity federation and rapid on boarding capabilities. For allowing users to easily and quickly leverage cloud services use single sign-on capability is required to simplify user logons for both the cloud and internally hosted applications.

Accounting and Accountability

Accounting and Accountability is a main cost-effective driver behind operation a Cloud Computing service is charging the customers according to their actual usage and another flooding attack on a Cloud service is drastically increasing the bills for Cloud usage. For computational power usage there is no “upper limits” then the client running the flooded service most likely has to foot the bill for the workload caused by the attacker.

III. END USER SECURITY ISSUES

Whether organizational data sits in a cloud or in a traditional or a legacy system, data will still be vulnerable to hacking and other intrusive attacks. Encryption may go a long way to reduce the risk, but information security is only as good as the security policies defined by the BUSINESS. TO REDUCE RISK these policies should be adopted for good result by an organization. The client organization have some mechanism to find vulnerable code or protocols at entry points like servers, firewalls, or mobile devices and upload patches on the native systems as soon as they are found. The cloud should secure from any user with malicious intent that will conceive to gain access to information or pack up a service.

Authentication

In the cloud environment, the primary basis for access control is user authentication and access control are more important than ever since the cloud and all of its data are accessible to all over the Internet. Trusted Platform Module (TPM) is a widely available and stronger authentication than username and passwords. Trusted Computing Groups (TCG’s) is IF-MAP standard about authorized users and other security issue in real-time communication between the cloud provider and the customer. When a user is reassigned or fired, the customer’s uniqueness management system can report the cloud provider in real-time so that the user’s cloud access can be revoked or modified within seconds. In cloud any fired user is logged, they would be immediately disconnected. Trusted Computing enables authentication of client nodes and other devices for improving the security in cloud computing. The frequently targeted attack is authentication in hosted and virtual services. The secure mechanisms are used to the authentication process for frequent target of attackers by different ways to Authenticate users based on different information know by the user.

Browser Security

In a Cloud environment, remote servers are used for computation. The client nodes are used for input/output operations only, and for authorization and authentication of information to the Cloud. A standard Web browser is platform independent client software useful for all users throughout the world. This can be categorized into different types: Software-as-a-Service (SaaS), Web applications, or Web 2.0. TLS is used for data encryption and host authentication

The Legacy Same Origin Policy is the insertion of scripting languages into Web pages for access rights for scripts. In this is to allow access read or write operations the same origin on content, to disallow but from the different origin any access on content. Origin means “the same application”, it can be defined with domain name, protocol, port in a web. But some problems with the SOP, but it could be solved with “origin” definition. In the case of WWW it’s not working properly. Security requirements for to protect both data during transport, and to authenticate the server’s domain name in Web applications is TLS.

Attacks on Browser-based Cloud Authentication are one of the security problems with browser-based protocols in Cloud Computing and it is not capable to generate cryptographically valid XML tokens. So, it can possible with a trusted third party. Login is not possible at a server due to the fewer credentials in browser, So HTTP forward it to the Passport login server. After entering username and password from user, then the Passport server convert this authentication into a Kerberos token, it can redirected to the requesting server from other HTTP redirect. Kerberos tokens are not clear to the browser and are the security problem with Passport, and it protected by the SOP. But any attacker can access those tokens then he accesses all services of the victim. Secure Browser-based Authentication is the situation is not suggested, but we can perform for better results by combined SOP and TLS for secure FIM protocols. In Cloud Computing by using TLS Browser Enhancements are very limited in an authentication center. It is not possible for XML Signature, the browser can be added many Web Service functionalities by simply loading an appropriate JavaScript library during runtime. So, the browser security API can be adding the enhancements XML Encryption and XML Signature.

IV. Security Solutions

The F5 Powered Secured Cloud

The F5 BIG-IP Local Traffic Manager (LTM) Application Delivery Controller with advanced load balancing also inspects all inbound and outbound application content.

- LTM is a powerful security tool that prevents network- and application-based protocol attacks. Out of the box, LTM protects both the applications being delivered from it and the network to which it is attached.
- LTM offers a unified approach to security solutions, but are not limited to packet filtering, port lockdown, denial of service (DoS) attack protection, network/administrative isolation, protocol validation, rate shaping, SSL termination, and more.
- F5 BIG-IP Application Security Manager (ASM), a web application firewall, not only protects against common vulnerabilities such those listed in the OWASP Top 10, but it also tightens control over the data with fine-grained policies. With BIG-IP ASM, the ability to control “who has access to the data”, the type of data available, and if the data can be exchanged,- even in Cloud.

F5 can help both the vendor and customer with solutions like BIG-IP Edge Gateway and BIG-IP Access Policy Manager (APM). BIG-IP Edge Gateway uses SSL technology to bring together access security, acceleration, and application availability services to enable context-aware, policy-controlled, secure, and optimized access to applications. BIG-IP APM is a flexible, high-performance access and Security platform; which it you can manage access to networks and applications by implementing solid security policies. By bringing these services together and driving user and group identity into the network, policy and service levels can be set based on identity and location. Access based on context makes the Internet, and the cloud, faster, more predictable, and more secure network for the enterprise, which is especially beneficial for mobile users and IT administrators.

Secure services based on SSL VPN offer endpoint security, giving IT administrators the ability to see who is accessing the organization and what the endpoint device’s posture is to validate against the corporate access policy. Strong AAA services, L4 and L7 user Access Control Lists, and integrated application security help protect corporate assets and maintain regulatory compliance. Availability services give administrators global traffic management capabilities to direct users to the best site based on location, L2-L4 switching, integrated routing, and an IPv6 gateway

With the integrated iSessions enabled by BIG-IP WAN Optimization Module, IT departments can connect with their cloud environment through an optimized, encrypted tunnel. Because maintaining control over data in the cloud is paramount, some organizations like to “house” their data at the corporate data center and have the cloud access it when requested. This process can certainly have performance implications but here too, the secure optimized iSessions tunnel provides the pipe from the data to the cloud. Symmetric, adaptive compression enables the tunnel to use the best compression ratio for the bandwidth available and adjusts the data stream to better use bandwidth, CPU, and compression rates. The branch office also benefits from the acceleration services. Whether for back-up scenarios or just keeping information up to date, symmetric data de-duplication only updates the changes to the data (rather than transferring the entire file), thus saving bandwidth. There is also support for CIFs and MAPI acceleration, and hardware-accelerated (SSL and compression) and L7 rate shaping, including QOS mode.
BIG-IP Edge Gateway policies can be imported and exported, web applications are secure and accelerated and offers modes for remote access, internal LAN control, and public and private wireless.

Cloud Security Reference Architecture

Reference architectures are useful for understanding how various recommendations come together to provide a complete solution. Enterprises that are interested in cloud computing models should consider the following reference architecture to ensure adequate security and optimal functionality.

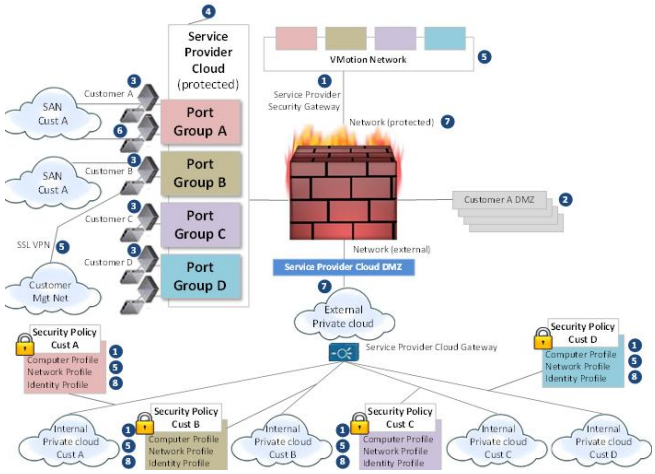

Fig. 1. Cloud Security Reference Architecture

Diagram Key

1. Security Profile per Compute Profile;
2. Security DMZ per vApp
3. OS Management
4. Resource Management
5. Security Profile per Network
6. Data Security
7. Security Authentication, Authorization and Auditing
8. Identity Management

Security profile per compute profile:
Administrators should communicate enterprise corporate security policy and server tier firewall rules that are defined within a vApp to the service provider. This should include corporate server security patch levels, anti-virus status and file-level access restrictions. The VMware vCloud reference architecture provides a method to communicate the policies and server tier firewall rules for the vApp.

Security DMZ for vApp:
The service provider needs to validate the patch level and security level prior to bringing a vApp into the production environment. The VMware vCloud reference architecture should include a DMZ area for validating the vApp and mitigating any security violations according to each enterprise's security profile.

OS Management:

It is important to understand the security hardening performed around the service provider's library of OSs and patching policies. Administrators should update traditional security policies that govern the service provider's hosting environment to ensure that virtual machines are hardened and patched within the standard enterprise policies.

Resource Management:
The service provider needs to separate and isolate the resources each customer virtual machine uses from other customers' virtual machine resources to prevent DDoS attacks. These attacks are usually caused by log files not having limits or CPU or memory utilization increasing on a single virtual machine through memory leaks or poorly behaving applications.

Security profile per network:
In addition to the vApp having a computer security profile, there should also be a network security profile to ensure perimeter and Web access security. This includes functionality like switch and router Access Control Lists (ACLs), perimeter firewall rules, or Web application security (Application Firewall, URL Filtering, whitelist and blacklists). The VMware vCloud reference architecture provides a method to communicate the network security profile.

A critical component of the reference architecture is the isolation of networks; enterprises need to ensure that service providers implement separate management networks and data networks per customer. In other words, there needs to be complete isolation between each customer's virtual machine and the data traffic connecting to their virtual machines. In addition, service providers should have a separate network for VMware VMotion and VMware VMsafe. Enterprises should request that service providers encrypt all management traffic, including VMware VMotion events. Many enterprises will require encryption of data packets via SSL/IPSec, or management connectivity via SSL or SSH. Some service providers offer only shared or open connectivity. At a minimum, all management connectivity should be provided via SSL.

Data Security:
Enterprises should request service providers provide access paths to only the physical servers that must have access to maintain the desired functionality. Service providers should accomplish this through the use of zoning via SAN N-Port ID virtualization (NPIV), LUN masking, access lists and permission configurations.

Security Authentication, authorization and auditing:

Cloud service provider environments require tight integration with enterprise policies around individual and group access, authentication and auditing (AAA). This involves integrating corporate directories and group policies with the service provider's policies. Service providers should offer stronger authentication methods to enterprises, such as 2-factor hard or soft tokens or certificates. The enterprise should require a user access report, including administrative access as well as authentication failures, through the service provider portal or via a method that pulls this data back to the enterprise. The VMware vCloud reference architecture provides a method to communicate the access controls and authentication needs to the service provider.

V.CONCLUSION

In this paper, we explored the provider and the end user cloud security threats and vulnerabilities. Organizations that are implementing cloud computing by expanding their on-premise infrastructure, should be aware of the security challenges faced by cloud computing. To protect against the compromise of the compliance integrity and security of their applications and data, defense in depth approach must be applied. In this paper, a reference cloud computing security architecture has been presented. In future, the proposed architecture may be modified with the advancement of security technologies used for implementing this reference cloud security architecture. Too several controls may be ineffective and inefficient, if the advantages outweigh the prices and associated risks.

REFERENCES

[1] "Security and high availability in cloud computing environments" , IBM Global Technology Services Technical White Paper ,IBM , June 2011

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

[3] V. Krishna Reddy, B. Thirumal Rao, Dr. L.S.S. Reddy, P.Sai Kiran "Research Issues in Cloud Computing " Global Journal of Computer Science and Technology, Volume 11,Issue 11, July 2011

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

[5] What cloud computing really means. InfoWorld. http://www.infoworld.com/d/cloudcomputing/what-cloud-computing-really-means-031?page=0,0

[6] K. Thirupathi Rao et al., "High Level Architecture to Provide Cloud Services Using Green DataCenter", in Advances in Wireless and Mobile Communications (AWMC) Volume 3 Number 2, pp 109-119, Research India Publication ISSN 0973-6972 (2010).

[7] Top 7 threats to cloud computing. HELP NET SECURITY. http://www.netsecurity.org/secworld.php?id=8943

[8] M.Jensen, N.Gruschka et al., "The impact of flooding Attacks on network based services" Proceedings of the IEEE International conference on Availability, Reliability and Security (ARES) 2008.

[9] Mathisen, "Security Challenges and Solutions in Cloud Computing" 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST2011) , Daejeon, Korea, 31 May -3 June 2011.

[10] "Cloud Security Questions? Here are some answers "http://cloudcomputing.syscon.com/node/1330353