ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 5, July 2012

An Initial Approach to Provide Security in Cloud Network

Dr. S. Srinivasu, K.P.R KrishnaChaitanya, K.Naresh Kumar

Abstract: -Cloud computing is a flexible, cost-effective and proven delivery platform for providing business or consumer IT services over the Internet. Cloud resources can be rapidly deployed and easily scaled, with all processes, applications and services provisioned "on demand" regardless of user location or device. As a result, cloud computing gives organizations the opportunity to increase their service delivery efficiencies, streamline IT management and better align IT services with dynamic business requirements. In many ways, cloud computing offers the "best of both worlds" providing solid support for core business functions along with the capacity to develop new and innovative services. Although the benefits of cloud computing are clear, so is the need to develop proper security for cloud implementations. Because without a security policy, the availability of cloud service can be compromised. The policy begins with assessing the risk to the network and building a team to respond. Continuation of the policy requires implementing a cloud security [1, 5] change management practice and monitoring the network for security violations in cloud.

Key Words: Cloud computing, Policy Management, Security Violations, Cloud Services, DHCP Servers, Cloud Controls Matrix.

I.INTRODUCTION

Cloud computing provides Internet-based services, computing, and storage for users in all markets including financial, healthcare, and government. This new approach to computing allows users to avoid upfront hardware and software investments, gain flexibility, collaborate with others, and take advantage of the sophisticated services that cloud providers offer. However, security is a huge concern for cloud users.

Cloud services and virtualization are driving significant shifts in IT spending and deployments. Cloud services give companies the flexibility to purchase infrastructure, applications, and services, from third-party providers with the goal of freeing up internal resources and recognizing cost savings. Virtualization allows maximum utilization of hardware and software, increasing cost savings, as well.

***Dr. S. Srinivasu**, CSE, Anurag Engineering College, (e-mail: sanikommusrinu@gmail.com). Kodad, AP, India, 9849676303.*

***KPR Krishna Chaitanya**, IT, Anurag Engineering College, (e-mail: krishnachaitanya.kpr@gmail.com). Kodad, AP, India, 9491892935.*

***K. Naresh Kumar**, CSE, Anurag Engineering College, (e-mail: nareshk03@ gmail.com). Kodad, AP, India, 9849777621.*

BENEFITS FOR THE CLOUD COMMUNITY

With the exponential increase in data deposited in cloud environments (both public and private), research in the area of data, information, and knowledge stored and processed in the cloud is timely. Data is stored in many different forms, and processed in a myriad of methods. There is a need for an authoritative voice in making sense of the key concerns with data storage and processing techniques. There is also an urgent requirement to align current practices with governance, risk and compliance regulations.

Cloud providers have recognized the cloud security concern and are working hard to address it. In fact, cloud security is becoming a key differentiator and competitive edge between cloud providers. By applying the strongest security techniques and practices, cloud security may soon be raised far above the level that IT departments achieve using their own hardware and software.

Before customers will entrust their IT needs to a cloud services [2], they need two things: first, assurance that the cloud infrastructure is secure and compliant, and second, visibility into their own security and compliance in cloud or managed infrastructure. Managed service and cloud providers have the technology and support they need to address these cloud computing security concerns. That means customers can move to the cloud with confidence. It also means you, as a provider, have the opportunity for unprecedented growth and market differentiation in this highly competitive space. So it is very important to develop a cloud service which possess highly secure. For that each cloud resource center [4] has to fallow below strategy

· define policy management.
· perform a risk analysis on that.
· taking counter action for that.

II. UPSIDES AND DOWNSIDES OF THE CLOUD

Cloud computing is being adopted at a rapid rate because it has a large number of upsides for all kinds of businesses and increases efficiency. Enterprises are reducing storage costs by using online storage solution providers. This allows the enterprise to store massive amounts of data on third party servers. One of the major advantages is that the storage capacity is scalable and thus, the enterprise only pays for the

amount of storage that it needs. Additionally, access to the data is available through any Internet connection.

Scalability and allocation of resources are the major advantages of virtualization. Virtualization allows administrators to use processing power more efficiently and share resources across hardware devices by servicing multi-tenant customers. Administrators can bring up virtual machines (VMs) [6] and servers quickly without having the overhead of ordering or provisioning new hardware. Hardware resources that are no longer required for a service or application can be reassigned quickly and extra processing power can be consumed by other services for maximum efficiency. By leveraging all the available processing power and un-tethering the hardware from a single server model, cost efficiencies are realized in both private and public clouds.

Though the introduction of cloud computing is by no means the first technology shift to cause major security concerns, it is a significant milestone. Until recently, most organizations have stored and managed their most critical information assets in physically separated data centers either on their own premises or within rented cages at large hosting providers.

But these upsides are tempered with potential downsides. Minimizing the data security risks, while moving and storing data, was easier for organizations to control within private data centers than within the cloud. Storing data in the cloud means that data will be intermingled on shared servers. If companies leap into cloud without considering the unintended consequences, critical corporate data like customer information and intellectual property are at increased risk.

One of the most concerning downsides is the potential loss of control over some or all of the cloud environment that houses the data. Cloud computing is often divided into three main service types: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) and each impacts data control and governance a little differently. With IaaS, the customer may have full control of the actual server configuration granting them more risk management control over the environment and data. In PaaS, the provider manages the hardware and underlying operating system [7] which limits enterprise risk management capabilities on those components. With SaaS, both the platform and the infrastructure are fully managed by the cloud provider which means if the underlying operating system or service isn't configured properly the data in the higher layer application may be at risk.

There are a number of ways to protect data in the cloud. Some have already been referenced, such as access controls and monitoring. The purpose of this document is not to provide a comprehensive overview of cloud security. There are a number of excellent resources for readers that are looking for additional insight on the subject including the Security Guidance for Critical Areas of Focus in Cloud Computing and Cloud Controls Matrix (CCM) [8] both available from the Cloud Security Alliance (CSA).

III. DEFINE POLICY MANAGEMENT AND PERFORM A RISK ANALYSIS ON THAT.

While the public IT cloud has a silver lining for many adopters, it isn't without draw-backs, especially in regards to data protection. Once data has gone into a public cloud, data security and governance control is transferred in whole or part to the cloud provider. Yet cloud providers are not assuming responsibility, e.g. Amazon's web services contract states "we strive to keep your content secure, but cannot guarantee that we will be successful at doing so, given the nature of the internet". When handing over the data, the enterprise forfeits all control of the security of the data, unless they protect the data beforehand.

One of the best ways to leverage the cost and efficiency benefits of the cloud and virtualization while keeping sensitive information secure, is to protect the data using a security solution that delivers data-centric, file-level encryption that is portable across all computing platforms and operating systems and works within a private, public or hybrid cloud computing environment.

Now a day's preventing security threats coming from outside cloud is not a big deal. if it is within the organization ?

Hence it is recommend creating usage policy statements that outline users' roles and responsibilities with regard to security. Create a general policy that covers all network systems in cloud and data within the company. If any company has identified specific actions that could result in punitive or disciplinary actions against an employee, these actions and how to avoid them should be clearly articulated in this document.

Low Risk Systems or data or virtual machines in cloud that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would not disrupt the business or cause legal or financial ramifications. The targeted system or data can be easily restored and does not permit further access of other systems.

Medium Risk Systems or data or virtual machines in cloud that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause a moderate disruption in the business, minor legal or financial ramifications, or provide further access to other systems. The targeted system or data requires a moderate effort to restore or the restoration process is disruptive to the system.

High Risk Systems or data or virtual machines in cloud that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause an extreme disruption in the business, cause major legal or financial ramifications, or threaten the health and safety of a person. The targeted system or data requires significant effort to restore or the restoration process is disruptive to the business or other systems.

Next assign this risk level to each core network devices, distribution network devices, access network devices, network monitoring devices in cloud. If we implement the same thing at Network equipment such as switches, routers, DNS servers, and DHCP servers [3] can allow further access into the network, and are therefore either medium or high risk devices. It is also possible that corruption of this equipment could cause the network itself to collapse. If we do so 80% problem is slaved.

Once you've assigned a risk level, it's necessary to identify the types of users of that cloud environment.

Admin of that cloud*:* responsible for internal users and network resources.
Internal users: It helps to provide limitation for local users while accessing cloud services.
Outside Partners External users with a need to access some resources.

System	Description	Risk Level	Types of Users
ATM switches	Core network device	High	Administrators for device configuration (support staff only); All others for use as a transport
Network routers	Distribution network device	High	Administrators for device configuration (support staff only); All others for use as a transport
ISDN or dial up servers	Access network device	Medium	Administrators for device configuration (support staff only); Partners and privileged users for special access
Firewall	Access network device	High	Administrators for device configuration (support staff only); All others for use as a transport
DNS and DHCP servers	Network applications	Medium	Administrators for configuration; General and privileged users for use
External e-mail server	Network application	Low	Administrators for configuration; All others for mail transport between the Internet and the internal mail server
Internal e-mail server	Network application	Medium	Administrators for configuration; All other internal users for use

Taking Counter action (Responding to risk)

IV. APPROVING SECURITY CHANGES

Security changes are defined as changes to network equipment that have a possible impact on the overall security of the cloud service .the security policy should identify specific security configuration requirements in non-technical terms. In other words, instead of defining a requirement as "No outside sources FTP connections will be permitted through the firewall", define the requirement as "Outside connections should not be able to retrieve files from the inside network". Admin will need to define a unique set of requirements for that organization.

The security team should review the list of plain language requirements to identify specific network configuration or design issues that meet the requirements. Once the team has created the required network configuration changes to implement the security policy, you can apply these to any future configuration changes. While it's possible for the security team to review all changes, this process allows them to only review changes that pose enough risk to warrant special treatment.

Security Violations

When a violation is detected, the ability to protect network equipment, determine the extent of the intrusion, and recover normal operations depends on quick decisions. Having these decisions made ahead of time makes responding to an intrusion much more manageable. The first action following the detection of an intrusion is the notification of the security team. Without a procedure in place, there will be considerable delay in getting the correct people to apply the correct response. Define a procedure in your security policy that is available 24 hours a day, 7 days a week. Next you should define the level of authority given to the security team to make changes, and in what order the changes should be made. Possible corrective actions are:

· Implementing changes to prevent further access to the violation.

· Isolating the violated systems.

· Contacting the carrier or ISP in an attempt to trace the attack.

There are two reasons for collecting and maintaining information during a security attack: to determine the extent to which systems have been compromised by a security attack, and to prosecute external violations. The type of information and the manner in which you collect it differs according to your goal.

To determine the extent of the violation, do the following:

1. Record the event by obtaining sniffer traces of the network, copies of log files, active user accounts, and network connections.

2. Limit further compromise by disabling accounts, disconnecting network equipment from the network, and disconnecting from the Internet.

3. Backup the compromised system to aid in a detailed analysis of the damage and method of attack.

Look for other signs of compromise. Often when a system is compromised, there are other systems or Accounts involved.

4. Maintain and review security device log files and network monitoring log files, as they often provide clues to the method of attack.

Following this example, create a monitoring policy for each area identified in your risk analysis. We recommend monitoring low−risk equipment weekly, medium−risk equipment daily and high−risk equipment hourly. If you require more rapid detection, monitor on a shorter time frame.

Lastly, your security policy should address how to notify the security team of security violations. Often, your network monitoring software will be the first to detect the violation. It should trigger a notification to the operations center, which in turn should notify the security team, using a pager if necessary.

To resolve this problem we can use the RSA Adaptive Authentication as a solution.RSA Adaptive Authentication is a comprehensive authentication and risk management Platform providing cost-effective protection for an entire user base. Adaptive Authentication monitors and authenticates user activities based on risk levels, institutional policies and customer segmentation and can be implemented with most existing authentication methods including:

Invisible authentication: Device identification and profiling

Out-of-band authentication: Phone call, SMS or e-mail

Challenge questions: Question- or knowledge-based authentication

Multi-credential framework: For those organizations wanting more choices, Adaptive Authentication is designed to easily integrate with a large selection of other authentication methods. The Multi-credential Framework allows organizations to develop authentication methods via RSA Professional Services, "in-house" or through third parties, to customize Adaptive Authentication.

Site-to-user authentication: Assuring users that they are transacting with a legitimate Website by displaying a personal security image and caption that has been pre-selected by the user at login.

V. CONCLUSION

A cloud is an attractive infrastructure solution for web applications since it enables web applications to dynamically adjust its infrastructure capacity on demand. Hence along with services is important to concentrate on security also. Policy management may solve security problem. But it will not give 100% alternate for the security problems in cloud services. Hence we have to check alternates for every time. Because security problems in cloud computing does not have the permanent solutions.

REFERENCE

1. https://cloudsecurityalliance.org/
2. AT&TCloudServices:https://www.synaptic.att.com/clouduser/compute_overview.htm
3. DHCPServer:http://technet.microsoft.com/en-us/windowsserver/dd448608.aspx
4. CloudResourceCenter:http://www.deitel.com/ResourceCenters/Programming/CloudComputing/tabid/3057/Default.aspx
5. NISTCloudReferenceandArchitecture:http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/ReferenceArchitectureTaxonomy.
6. VirtualMachines:Virtualizationvs.Emulation: http://www.griffincaprio.com/blog/2006/08/virtual-machines-virtualization-vs-emulation.html
7. OperatingSystem: http://www.computerhope.com/os.htm
8. https://cloudsecurityalliance.org/research/ccm/(Cloud Control Matrix)

Author Profile

Dr. S. Srinivasu received Ph.D (Computer Science Engineering) from University of Allahabad, Master of Technology from Mahatma Gandhi Kashi Vidyapeet, Varanasi, U.P. His research interests include Network Security and Cryptography (Security). He is currently working as a Professor in the department of Computer Science and Engineering in Anurag Engineering College, Kodad. He is a life member of ISTE and member of CSI.

K.P.R.Krishna Chaitanya received Master of Technology (Computer Science & Engineering) from Jawaharlal Nehru Technological University (JNTUH). My research interests include Information Security, Cloud Computing and Grid Computing. Presently working as an Assistant Professor in the department of IT in Anurag Engineering College (AEC), Ananthagiri(V), Kodad(M), Nalgonda(Dt.), Andhra Pradesh, India. He is a professional member of ACM.

K. Naresh Kumar received Master of Computer Applications (MCA) from Osmania University. Master of Technology (Computer Science & Engineering) from Jawaharlal Nehru Technological University (JNTUH). My research interests include Information Security, Web Services, Cloud Computing and Mobile Computing. Presently working as an Associate Professor in the department of CSE in Anurag Engineering College (AEC), Ananthagiri(V), Kodad(M), Nalgonda(Dt.), Andhra Pradesh, India.