ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 3, pp: (116-121), Month: July - September 2014, Available at: www.researchpublish.com

Cloud Computing Security

Suresh Babu. E

Department of Computer Science and Engineering
Saveetha School of Engineering, Thandalam, Chennai,Tamil Nadu, India

Abstract: **It is no secret that cloud computing is becoming more and more popular today and is ever increasing in popularity with large companies as they share valuable resources in a cost effective way. Due to this increasing demand for more clouds there is an ever growing threat of security becoming a major issue. This paper shall look at ways in which security threats can be a danger to cloud computing and how they can be avoided.**

Keywords: **Cloud Computing, Network Security.**

1. INTRODUCTION

Cloud computing is internet based where shared resources; software and information are provided to computers and other devices on-demand. The pioneer of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) are both well known examples. While these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. As a result, users are at the mercy of their cloud service providers for the availability and integrity of their data. Downtime of Amazon's S3 is such an example. [1]

The three main aspects of cloud computing are software as a service, platform as a service and infrastructure as a service. A SaaS provider typically hosts and manages a given application in their own data centre and makes it available to multiple tenants and users over the Web. Some SaaS providers run on another cloud provider's PaaS or IaaS service offerings. Oracle CRM On Demand, Salesforce.com, and Netsuite are some of the well known SaaS examples. Platform as a Service (PaaS) is an application development and deployment platform delivered as a service to developers over the Web. It facilitates development and deployment of applications without the cost and complexity of buying and managing the underlying infrastructure, providing all of the facilities required to support the complete life cycle of building and delivering web applications and services entirely available from the Internet. This platform consists of infrastructure software, and typically includes a database, middleware and development tools. A virtualized and clustered grid computing architecture is often the basis for this infrastructure software. Some PaaS offerings have a specific programming language or API. For example, Google App Engine is a PaaS offering where developers write in Python or Java. EngineYard is Ruby on Rails. Sometimes PaaS providers have proprietary languages like force.com from Salesforce.com and Coghead, now owned by SAP. Infrastructure as a Service (IaaS) is the delivery of hardware (server, storage and network), and associated software (operating systems virtualization technology, file system), as a service. It is an evolution of traditional hosting that does not require any long term commitment and allows users to provision resources on demand. Unlike PaaS services, the IaaS provider does very little management other than keep the data centre operational and users must deploy and manage the software services themselves--just the way they would in their own data centre. Amazon Web Services Elastic Compute Cloud (EC2) and Secure Storage Service (S3) are examples of IaaS offerings. [2]

Further more the most popular cloud types are private, public and hybrid clouds. In a private cloud, the infrastructure for implementing the cloud is controlled completely by the enterprise. Typically, private clouds are implemented in the enterprise's data centre and managed by internal resources. A private cloud maintains all corporate data in resources under the control of the legal and contractual umbrella of the organization. This eliminates the regulatory, legal and

security concerns associated with information being processed on third party computing resources. In a public cloud, external organizations provide the infrastructure and management required to implement the cloud. Public clouds dramatically simplify implementation and are typically billed based on usage. This transfers the cost from a capital expenditure to an operational expense and can quickly be scaled to meet the organization's needs. Temporary applications or applications. With burst resource requirements typically benefit from the public cloud's ability to ratchet up resources when needed and then scale them back when they are no longer needed. In a private cloud, the company would need to provision for the worst case across all the applications that share the infrastructure. This can result in wasted resources when utilization is not at its peak. [2]

1.1. Security Threats

Cloud computing and web services run on a network structure so they are open to network type attacks. One of these attacks is the distributed denial of service attacks. If a user could hijack a server then the hacker could stop the web services from functioning and demand a ransom to put the services back online. To stop these attacks the use of syn cookies and limiting users connected to a server all help stop a DDOS attack. Another such attack is the man in the middle attack. If the secure sockets layer (SSL) is incorrectly configured then client and server authentication may not behave as expected therefore leading to man in the middle attacks. [3]

Another type of attack is network sniffing. With a packet sniffer an attacker can capture sensitive data if unencrypted such as passwords and other web service related security configuration such as the UDDI (Universal Description Discovery and Integrity), SOAP (Simple Object Access Protocol) and WSDL (Web Service Description Language) files. Port scanning is also another threat which can be used by an attacker. Port 80 is always open due to it being the port that the web server sits on. However this can easily be encrypted and as long as the server software is configured correctly then there should be no intrusion. [4]

Other attacks include SQL injection where a hacker can use special characters or terms to return unintended data For example, strings that may end up in a WHERE clause of an SQL statement may be tricked into including more information. For instance a parameter value of X' or 1=1 may cause a whole table to be returned as 1=1 is always seen as true. Also cross site scripting where inserting code into a field or URL that gets executed hands over control or sensitive data to the attacker. Successful cross site scripting attacks can lead to buffer overflows, DOS attacks, inserting spyware and malicious code into visiting browsers and violation of user privacy. [5]

Other such risks which are marked as high risk in cloud security are:

Loss Of Governance: in using cloud infrastructures, the client necessarily cedes control to the CloudProvider (CP) on a number of issues which may affect security. At the same time, SLAs may not offer a commitment to provide such services on the part of the cloud provider, thus leaving a gap in security defences. [6]

Lock-In: there is currently little on offer in the way of tools, procedures or standard data formats or services interfaces that could guarantee data, application and service portability. This can make it difficult for the customer to migrate from one provider to another or migrate data and services back to an in-house IT environment. This introduces a dependency on a particular CP for service provision, especially if data portability, as the most fundamental aspect, is not enabled.[6]

Data Protection: Cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer (in its role as data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g., between federated clouds. On the other hand, some cloud providers do provide information on their data handling practices. Some also offer certification summaries on their data processing and data security activities and the data controls they have in place, e.g., SAS70 certification. . [6]

Insecure Or Incomplete Data Deletion: when a request to delete a cloud resource is made, as with most operating systems, this may not result in true wiping of the data. Adequate or timely data deletion may also be impossible (or undesirable from a customer perspective), either because extra copies of data are stored but are not available, or because the disk to be destroyed also stores data from other clients. In the case of multiple tenancies and the reuse of hardware resources, this represents a higher risk to the customer than with dedicated hardware. [6] .As you can see the attacks are

very similar to that of a standard network. Other attacks which may not be specific to the cloud are lack of physical authentication such as biometrics and swipe cards. Mis-configuration may also contribute to the loss of data or allow a hacker to gain entry. Others may include un-patched operating system software, use of un-trusted software and tools within the cloud. A number of counter measures shall be discussed now in the next section.

1.2. *Security Measures*

To help further increase the security of users in the cloud, private clouds can be formed. One example of this is the Amazon Virtual private Cloud (VPC). The idea of a private cloud is to allow a company to create a secure and seamless bridge between the company's existing IT structure and the AWS cloud. Amazon VPC enables enterprises to connect their existing infrastructure to a set of isolated AWS compute resources via a Virtual Private Network (VPN) connection, and to extend their existing management capabilities such as security services, firewalls, and intrusion detection systems to include their AWS resources. As example of this is shown below in figure 1 – [7]

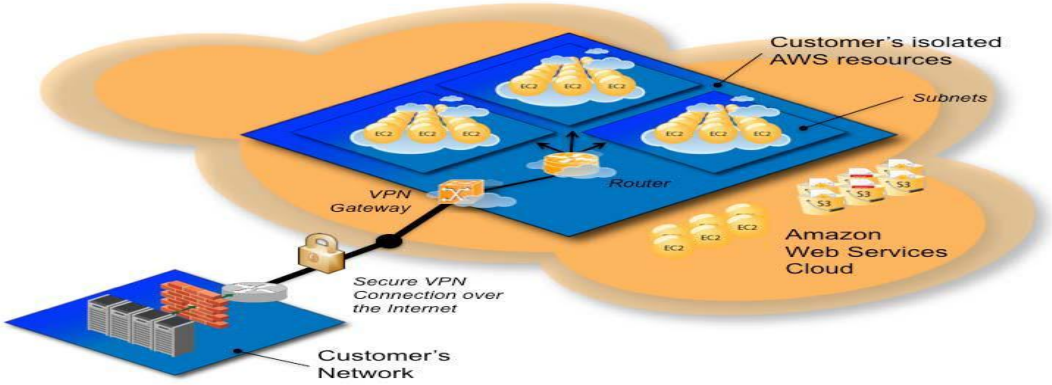

Figure 1 - Shows a possible VPN to help increase cloud security.

To secure the structure that is to be implemented we need to come up with a security analysis process. This will include what type of assets there are to be protected from a company point of view, what threats can be run against a company, what countermeasures can be put in place to stop these attacks from taking place. When dealing with assets we need to look at what assets are we trying to protect and what properties of these assets must be protected. For dealing with threats we must look at what kind of attacks can be launched against a company with this type of structure. [8]. When it comes to the topic of assets in a company we need to look at aspects such as customer data, customer applications and client computing devices. This would include confidentially, integrity and availability of the data. Confidentiality deals with the unauthorised access of data, integrity dealing with the safe enclosure of data and of course availability dealing with the data being available to the customer at all times. Types of threats include failures in provider security, attacks by a customer or hacker, availability and reliability issues. The customer must trust the provider security therefore it is essential that it be monitored regularly. [8]

Attacks by a customer could be provider resources like CPU usage and storage shared with un-trusted parties. Customer data and applications must run separately and failure to do so may effect the confidentially, integrity and availability principles (CIA). To prevent this we can use the measures already discussed such as the VPNs and VLANs and strong encryption along with secure transport layer security. Threats that fall under availability and reliability issues are increased completion causes increased failure, clouds are prominent attack targets and internet reliability is sometimes not reliable. To counter these planning for down time is essential as is using public clouds for non-essential applications. [8].Another popular security method is the hypervisor. The Amazon web service makes use of it in its cloud. Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor, taking advantage of paravirtualization. Because paravirtualized guests rely on the hypervisor to provide support for operations that normally require privileged access, it is possible to run the guest OS with no elevated access to the CPU. This explicit virtualization of the physical resources leads to a clear separation between guest and hypervisor, resulting in strong security separation between the two. [7].

A fire wall is also essential and Amazon web services also recommend an implementation method for this. Amazon EC2

provides a complete firewall solution; this mandatory inbound firewall is configured in a default deny mode and the Amazon EC2 customer must explicitly open any ports to allow inbound traffic. The traffic may be restricted by protocol, by service port, as well as by source IP address (individual IP or CIDR block). The firewall can be configured in groups permitting different classes of instances to have different rules, for example the case of a traditional three-tiered web application. [7] .The group for the web servers would have port 80 (HTTP) and port 443 (HTTPS) open to the world. The group for the application servers would have port 8000 (application specific) accessible only to the web server group. The group for the database servers would have port 3306 (MySQL) open only to the application server group. All three groups would permit administrative access on port 22 (SSH), but only from the customer's corporate network. Highly secure applications can be deployed using this expressive mechanism. The firewall is controlled not by the host/instance itself, but requires the customer's X.509 certificate and key to authorize changes, thus adding an extra layer of security. [7]

Within EC2, the host administrator and cloud administrator can be separate people, permitting two man rule security policies to be enforced. In addition, AWS encourages customers to apply additional per-instance filters with host-based firewalls such as IP tables. This can restrict both inbound and outbound traffic on each instance. The level of security afforded by the firewall is a function of which ports are opened by the customer, and for what duration and purpose. The default state is to deny all incoming traffic, and developers should plan carefully what they will open when building and securing their applications. Well-informed traffic management and security design is still required on a per-instance basis. A figure of the firewall can be seen in figure 2 [7]

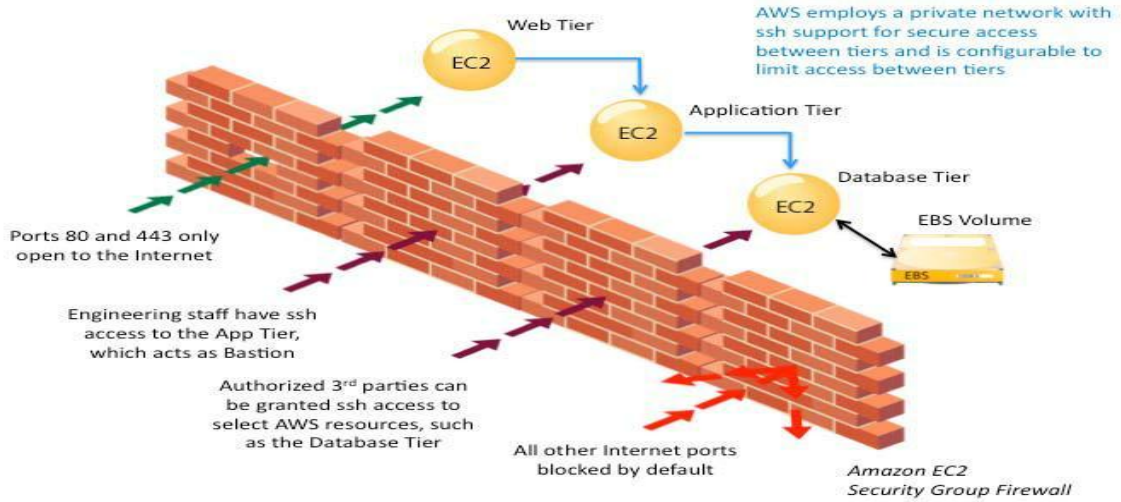

Figure 2 - shows a potential cloud computing firewall solution.

1.3. Advantages and Disadvantages Of Cloud Computing

Cloud computing is no doubt a fantastic technology and continues to grow in popularity and more and more companies are investing in a cloud for their company. Cloud computing presents IT organizations with a fundamentally different model of operation, one that takes advantage of the maturity of web applications and networks and the rising interoperability of computing systems to provide IT services. Cloud providers specialize in particular applications and services, and this expertise allows them to efficiently manage upgrades and maintenance, backups, disaster recovery, and failover functions. As a result, consumers of cloud services may see increased reliability, even as costs decline due to economies of scale and other production factors. Other advantages include reduced costs as resources are shared and re-used within the cloud. [9]

So it is fair to say that the main benefits of cloud computing to a company are as follows:

Reduced Cost
Cloud technology is paid incrementally, saving organizations money.

Increased Storage
Organizations can store more data than on private computer systems.

Highly Automated
No longer do IT personnel need to worry about keeping software up to date?

Flexibility
Cloud computing offers much more flexibility than past computing methods.

More Mobility
Employees can access information wherever they are, rather than having to remain at their desks.

Allows IT to Shift Focus
No longer having to worry about constant server updates and other computing issues, government

Organizations will be free to concentrate on innovation. [10]

The technology is of course not without its flaws. One of the main issues is security. All vital data is stored on an external server by an external provider. As mentioned many simple network attacks can work on company clouds. Theoretically, data stored in the cloud is unusually safe, replicated across multiple machines. But on the off chance that your data goes missing, you have no physical or local backup. Another disadvantage is that it requires a constant connection. Since you use the Internet to connect to both your applications and documents, if you don't have an Internet connection you can't access anything, even your own documents. This would certainly count towards a loss of business. Another issue and downside is speed. Everything about the cloud, from the interface to the current document, has to be sent back and forth from your computer to the computers in the cloud. Latency and performance issues are common in clouds and to perform adequately, require a high speed connection. Of course geographical and similar factors will come into play. [11]

2. CONCLUSION

Cloud computing offers real alternatives to IT departments for improved flexibility and lower cost. Markets are developing for the delivery of software applications, platforms, and infrastructure as a service to IT departments over the "cloud". These services are readily accessible on a pay-per-use basis and offer great alternatives to businesses that need the flexibility to rent infrastructure on a temporary basis or to reduce capital costs. Open source clouds such as the Ubuntu cloud offer smaller businesses the chance to try out the benefits of cloud computing. Once cloud computing technology has been improved and network technology has also been improved a real golden opportunity exists for the future. Each cloud solution must however be tailored to each company but they can all benefit from the numerous advantages the technology brings to the table. The technology is still in early days but already there is much hype surrounding the technology and with impressive results so far this will continue to grow. [2]

REFERENCES

[1] Ren K Et Al. 2009. Ensuring Data Storage Security in Cloud Computing. [Online] Available from: www.ece.iit.edu/~ubisec/IWQo S09 .pdf [Accessed on 26th January 2011].

[2] Oracle. 2009. Architectural Strategies for Cloud Computing. [Online] Available from: http://www.oracle.com/technology/architect/entarch/pdf/architectural_strategies_for_cloud_computing.pdf [Accessed on 26th Febuary2011]

[3] Scarfone K, Singhal A, Winograd T. 2007. Guide to Secure Web Services. [Online] Available from: http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf[Accessed 26th Dec 2010]

[4] Amazon Web Services. 2009. Amazon Virtual private Cloud. [Online] Available from: http://aws.amazon.com/vpc/ [Accessed 26th April 2010]

[5] Yang A. 2003. Guide to XML Web Services Security. [Online] Available from: http://www.cgisecurity.com/ws/WestbridgeGuideToWebServicesSecurity.pdf[Accessed 26th April 2010]

[6] Catteddu D. 2010. Cloud Computing. [Online] Available from: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment [Accessed 26th April 2010]

[7] Amazon Web Services. 2009. Amazon Web Services: Overview of Security Processes. [Online] Available from: http://aws.amazon.com/ec2/[Accessed 26th April 2010]

[8] Hanna S. 2009. Cloud Computing: Finding the Silver Lining. [Online] Available from: http://www.ists.dartmouth.edu/docs/HannaCloudComputingv2.pdf[Accessed 26th April 2010]

[9] Educase. 2009. 7 Things You Should Know About Cloud Computing. [Online] Available from: http://www.educause.edu/Resources/7ThingsYouShouldKnowAboutCloud/176856[Accessed 6th Febuary 2011]

[10] Anon. 2008. Six Benefits of Cloud Computing. [Online] Available from: http://web2.sys-con.com/node/640237 [Accessed 6th Febuary 2010]

[11] Miller W. 2009. Disadvantages of Cloud Computing. [Online] Available from: http://www.informit.com/articles/article.aspx?p=1324280&seqNum=2[Accessed 26th Nov 2010].