Cloud Computing Challenges and Related Security Issues

Traian Andrei, ta8@wustl.edu (A project report written under the guidance of Prof. Raj Jain)

Download

Abstract

The field of cloud computing is still in its infancy as far as implementation and usage, partly because it is heavily promoted by technology advancement and is so high resource dependent that researches in academic institutions have not had many opportunities to analyze and experiment with it. However, cloud computing arises from the IT technicians desire to add another layer of separation in processing information. At the moment, a general understanding of cloud computing refers to the following concepts: grid computing, utility computing, software as a service, storage in the cloud and virtualization. These refer to a client using a provider's service remotely, also known as in the cloud. Even if there is an existent debate on whether those concepts should be separated and dealt with individually, the general consensus is that all those terms could be summarized by the cloud computing umbrella. Given its recent development and scarcity of academic published work, many discussions on the topic of cloud security have surfaced from engineers in companies that provide the aforementioned services. Nevertheless, academia is developing in a significant presence, being able to address numerous issues.

Table of Contents

1. Introduction

Cloud computing is not an innovation per se, but a means to constructing IT services that use advanced computational power and improved storage capabilities. The main focus of cloud computing from the provider's view as extraneous hardware connected to support downtime on any device in the network, without a change in the users' perspective. Also, the users' software image should be easily transferable from one cloud to another. Balding proposes that a layering mechanism should occur between the front-end software, middle-ware networking and back-end servers and storage, so that each part can be designed, implemented, tested and ran independent from subsequent layers. [Balding08] This paper introduces the current state of cloud computing, with its development challenges, academia and industry research efforts. Further, it describes cloud computing security problems and benefits and showcases a model of secure architecture for cloud computing implementation.

2. Current View

Critics argue that cloud computing is not secure enough because data leaves companies' local area networks. It is up to the clients to decide the vendors, depending on how willing they are to implement secure policies and be subject to 3rd party verifications. Salesforce, Amazon and Google are currently providing such services, charging clients using an on-demand policy. [Mills09] references statistics that suggest one third of breaches are due to laptops falling in the wrong hands and about 16% due to stolen items by employees. Storing the data in the cloud can prevent these issues altogether. Moreover, vendors can update application/OS/middleware security patches faster because of higher availability of staff and resources. According to cloud vendors, most thefts occur when users with authorized access do not handle data appropriately. Upon a logout from the cloud session, the browser may be configured to delete data automatically and log files on the vendor side indicate which user accessed what data. This approach may be deemed safer that storing data on the client side. There are some applications for which cloud computing is the best option. One example is the New York Times using Amazon's cloud service to generate PDF documents of several-decade old articles. The estimated time for doing the task on the Times' servers was 14 years, whereas the cloud provided the answer in one day for a couple hundred dollars. [Weinberg08] However, the profile of the companies that currently use the cloud technology includes Web 2.0 start-ups that want to minimize material cost, application developers that want to enable their software as a service or enterprises that are exploring the cloud with trivial applications. The fact that cloud computing is not used for all of its potential is due to a variety of concerns. The following surveys the market in terms of continuous innovation, academia and industry research efforts and cloud computing challenges.

2.1 Innovation

Nevertheless, there numerous ways in which cloud computing can expand on the issue of security. For example, QualysGuard is a compilation of products that are used to discover network weaknesses. It is used by over 200 companies in Forbes Global 2000, so it acquired significant acceptance in the marketplace. QualysGuard main idea is to place an appliance behind the firewall that would monitor various security issues. The box encrypts all its data and has no access to client stored data; however, it does contain a back porch by allowing a certain IP address and admin to modify scripts and credentials. In this fashion, it proposes a new type of security to the cloud, so that whenever an attack is made on a certain service, it may be monitored by a 3rd party and cut off before it disrupts proper access or attempts to falsely validate itself to the cloud.

2.2 Academia and Industry Partnership

The Open Cloud Consortium (OCC) is a group formed by universities and IT companies looking to investigate new ways of improving computing and storage costs across various cloud platforms and integrate communication standards among different providers. This is a relatively new group formed in the mid-2008, which confirms the novelty of the field. The OCC has undertaken the following goals:

. development of standards for cloud computing and frameworks for interoperating between clouds

. develop benchmarks for cloud computing

. support reference implementations for cloud computing, preferably open source reference implementations

. manage a test bed for cloud computing - the Open Cloud Testbed

. sponsor workshops and other events related to cloud computing

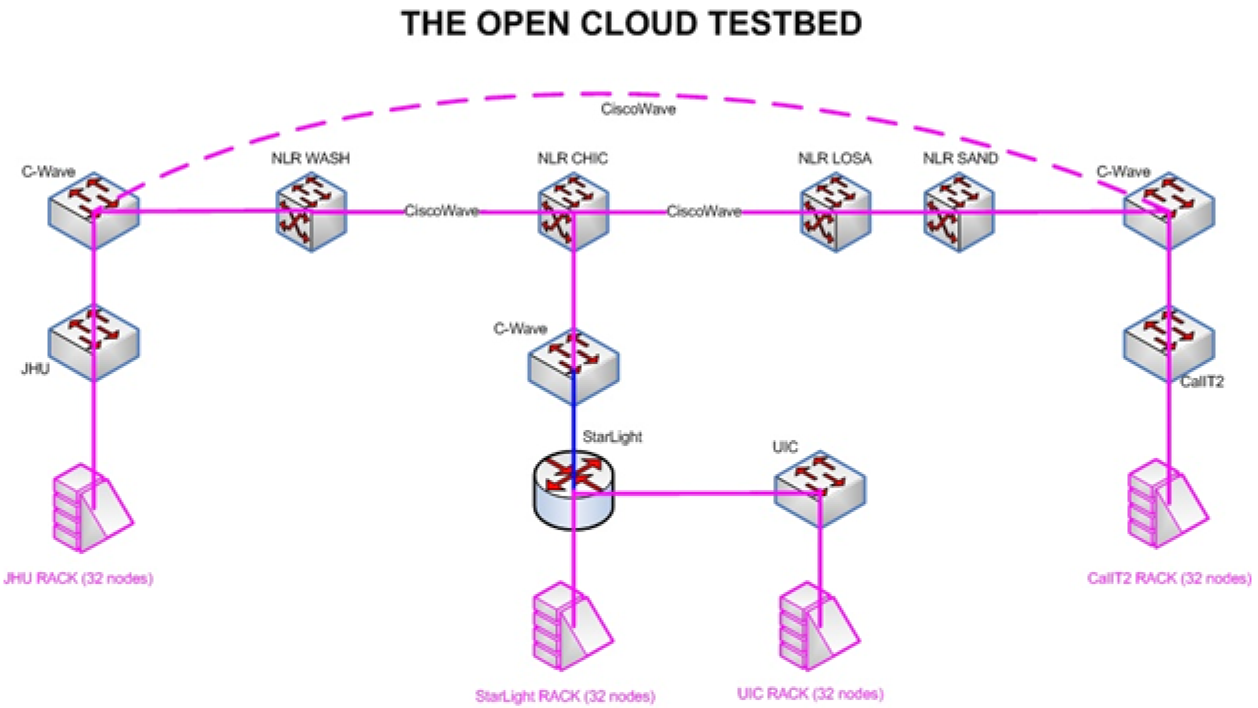

Figure 1 . OCC Network Topology

The architecture in fig. 1 shows the OCC network and the connection among server racks at University of Illinois at Chicago, StarLight in Chicago, Calit2 in La Jolla and John Hopkins University in Baltimore to the switches, routers and wide area routers in between. Using the aforementioned architecture, the OCC published has worked towards implementing high traffic flow design and protocols among several locations. [OCC08]

2.3 Cloud Computing Challenges

Challenges that cloud computing currently faces in being deployed on a large enterprise scale:

. Self-healing - in case of application/network/data storage failure, there will always be a backup running without major delays, making the resource switch appear seamless to the user.

. SLA-driven - cloud is administrated by service level agreements that allow several instances of one application to be replicated on multiple servers if need arises; dependent on a priority scheme, the cloud may minimize or shut down a lower level application.

. Multi-tenancy - the cloud permits multiple clients to use the same hardware at the same time, without them knowing it, possibly causing conflicts of interest among customers.

. Service-oriented - cloud allows one client to use multiple applications in creating its own.

. Virtualized - applications are not hardware specific; various programs may run on one machine using virtualization or many machines may run one program.

. Linearly scalable - cloud should handle an increase in data processing linearly; if "n" times more users need a resource, the time to complete the request with "n" more resources should be roughly the same.

. Data management - distribution, partitioning, security and synchronization of data.

3. Security Challenges

Start-up companies often lack the protection measures to weather off an attack on their servers due to the scarcity of resources - poor programming that explores software vulnerabilities (PHP, JavaScript, etc) open ports to firewalls or inexistent load-balance algorithms susceptible to denial of service attacks. For this reason, new companies are encouraged to pursue cloud computing as the alternative to supporting their own hardware backbone. However cloud computing does not come without its pitfalls. For starters, a cloud is a single point of failure for multiple resources. Even though network carriers such as AT&T believe a distributed cloud structure is the right implementation, it faces major challenges in finding the optimal approach for low power transmission and high network availability [Croll08]; some people believe that major corporations will shy away from implementing cloud solutions in the near future due to ineffective security policies. One problem comes from the fact that different cloud providers have different ways to store data, so creating a distributed cloud implies more challenges to be solved between vendors.

3.1 Data Security

Security refers to confidentiality, integrity and availability, which pose major issues for cloud vendors. Confidentiality refers to who stores the encryption keys - data from company A, stored in an encrypted format at company B must be kept secure from employees of B; thus, the client company should own the encryption keys.
Integrity refers to the face that no common policies exist for approved data exchanges; the industry has various protocols used to push different software images or jobs. One way to maintain data security on the client side is the use of thin clients that run with as few resources as possible and do not store any user data, so passwords cannot be stolen. The concept seems to be impervious to attacks based on capturing this data. However, companies have implemented systems with unpublished APIs, claiming that it improves security; unfortunately, this can be reversed engineered; also, using DHCP and FTP to perform tasks such as firmware upgrades has long been rendered as insecure. Nevertheless, products from Wyse are marketed with their thin client as one of the safest, by using those exact features. [Balding08]

Lastly, the most problematic issue is availability, as several companies using cloud computing have already experienced downtime (Amazon servers subject to what appeared to be a denial of service attack). Other things to keep in mind are contract policies between clients and vendors, so that data belongs only to the client at all times, preventing third parties to be involved at any point. Also, authentication should be backed by several methods like password plus flash card, or password plus finger print, or some combination of external hardware and password. One benefit of cloud computing is that client software security does not need to be enforced as strictly as before. This aspect concerns the view of cloud computing as software as a service, as it becomes more important to ensure security of data transfer rather than a traditional secure application life cycle.

3.2 Cloud Computing Security Issues

[Gartner08] identified seven issues that need to be addressed before enterprises consider switching to the cloud computing model. They are as follows:

. privileged user access - information transmitted from the client through the Internet poses a certain degree of risk, because of issues of data ownership; enterprises should spend time getting to know their providers and their regulations as much as possible before assigning some trivial applications first to test the water

. regulatory compliance - clients are accountable for the security of their solution, as they can choose between providers that allow to be audited by 3rd party organizations that check levels of security and providers that don't

. data location - depending on contracts, some clients might never know what country or what jurisdiction their data is located

. data segregation - encrypted information from multiple companies may be stored on the same hard disk, so a mechanism to separate data should be deployed by the provider.

. recovery - every provider should have a disaster recovery protocol to protect user data

. investigative support - if a client suspects faulty activity from the provider, it may not have many legal ways pursue an investigation

. long-term viability - refers to the ability to retract a contract and all data if the current provider is bought out by another firm

Given that not all of the above need to be improved depending on the application at hand, it is still paramount that consensus is reached on the issues regarding standardization.

3.3 Security Benefits

There are definitely plenty of concerns regarding the inability to trust cloud computing due to its security issues. However, cloud computing comes with several benefits that address data security. The following sections looks into addressing concepts such as centralized data, incident response or logging.

Centralized Data refers to the approach of placing all eggs in one basket. It might be dangerous to think that if the cloud goes down, so does the service they provide, but at the same time, it is easier to monitor. Storing data in the cloud voids many issues related to losing laptops or flash drives, which has been the most common way of loosing data for large enterprises or government organizations. The laptop would only store a small cache to interface with the thin client, but the authentication is done through the network, in the cloud. In addition to this, when a laptop is known to be stolen, administrators can block its attempted access based on its identifier or MAC address. Moreover, it is easier and cheaper to store data encrypted in the cloud that to perform disk encryption on every piece of hardware or backup tape.

Incident Response refers to the ability to procure a resource such as a database server or supercomputing power or use a testing environment whenever needed. This bypasses the supplemental red tape associated with traditional requesting of resources within the corporate world. Also, if a server is down for re-imaging or disk clean-up, the client may easily create similar instances of their environment on other machines, improving the acquisition time. From a security standpoint, cloud providers already provide algorithms for generating hashes or checksums whenever a file is stored in the cloud, which bypasses the local/client need for encrypting. This does not imply that clients should not encrypt the data before sending it, but merely that the service is already in place for them.

Password Assurance Testing is a service that can be used to harness the computational power of the cloud in attempts to break into a company's system by guessing passwords. This approach minimizes resources and time spent on the client side. Logging benefits come from the idea that the client need not worry about storage space for log files and enjoys a faster way of searching through them. Moreover, it allows for a convenient way to observe which user accessed certain resources at any given time.

Improvement of Secure Software refers to several aspects in the development lifecycle of a product. Initially, a company that is thinking of placing their application in the cloud knows that the cost of running the application are directly proportional with the number of processing cycles, thus creating an incentive for an optimal implementation. Secondly, it becomes easier to monitor the effects of various security policies implemented in the software, without the overhead of traditional switching environments from development to production or to testing. Creating a new environment simply means creating a clone of the extant one. Thirdly, software run behind an architecture that is build for secure transactions at a physical, data link, network and transport layer, making it easier to design the application without the outspoken need of a security software engineer. Moreover, some cloud providers may use code scanning to detect vulnerabilities in the application code. [Balding08]

4. Secure Architecture Models

Open Security Architecture (OSA) provides free frameworks that are easily integrated in applications, for the security architecture community. Its patterns are based on schematics that show the information traffic flow for a particular implementation as well as policies implemented at each step for security reasons. The following description of a proposed cloud computing architecture, also shown in fig. 2, should help the reader envision the components of cloud computing architectures along with descriptions of elements that make it secure. The important entities involved in the data flow are end users, developers, system architect, 3rd party auditors and the cloud itself. The following summary looks at their attributions and mechanisms available for them.

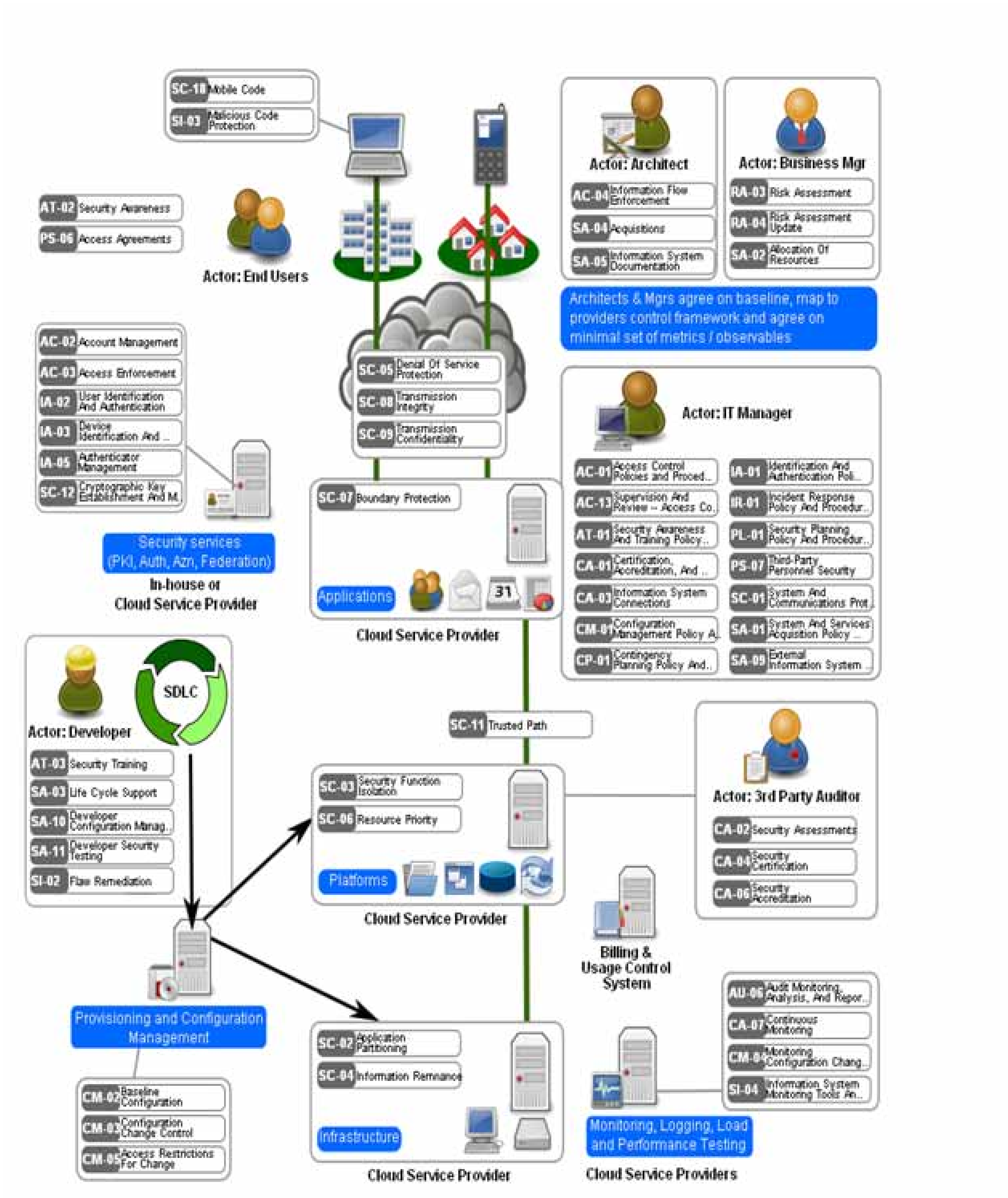
SC-18 Mobile Code
SI-03 Malicious Code Protection
AT-02 Security Awareness
PS-06 Access Agreements
Actor: End Users
Actor: Architect
AC-04 Information Flow Enforcement
SA-04 Acquisitions
SA-05 Information System Documentation
Actor: Business Mgr
RA-03 Risk Assessment
RA-04 Risk Assessment Update
SA-02 Allocation Of Resources
Architects & Mgrs agree on baseline, map to providers control framework and agree on minimal set of metrics / observables
AC-02 Account Management
AC-03 Access Enforcement
IA-02 User Identification And Authentication
IA-03 Device Identification And ...
IA-05 Authenticator Management
SC-12 Cryptographic Key Establishment And M..
SC-05 Denial Of Service Protection
SC-08 Transmission Integrity
SC-09 Transmission Confidentiality
Security services (PKI, Auth, Azn, Federation)
In-house or Cloud Service Provider
SC-07 Boundary Protection
Applications
31
Cloud Service Provider
Actor: IT Manager
AC-01 Access Control Policies and Proced..
AC-13 Supervision And Review – Access Co..
AT-01 Security Awareness And Training Policy..
CA-01 Certification, Accreditation, And ..
CA-03 Information System Connections
CM-01 Configuration Management Policy A..
CP-01 Contingency Planning Policy And..
IA-01 Identification And Authentication Poli..
IR-01 Incident Response Policy And Procedur..
PL-01 Security Planning Policy And Procedur..
PS-07 Third-Party Personnel Security
SC-01 System And Communications Prot..
SA-01 System And Services Acquisition Policy ...
SA-09 External Information System ..
Actor: Developer
SDLC
AT-03 Security Training
SA-03 Life Cycle Support
SA-10 Developer Configuration Manag..
SA-11 Developer Security Testing
SI-02 Flaw Remediation
SC-11 Trusted Path
SC-03 Security Function Isolation
SC-06 Resource Priority
Platforms
Cloud Service Provider
Actor: 3rd Party Auditor
CA-02 Security Assessments
CA-04 Security Certification
CA-06 Security Accreditation
Billing & Usage Control System
Provisioning and Configuration Management
CM-02 Baseline Configuration
CM-03 Configuration Change Control
CM-05 Access Restrictions For Change
SC-02 Application Partitioning
SC-04 Information Remnance
Infrastructure
Cloud Service Provider
AU-06 Audit Monitoring, Analysis, And Repor..
CA-07 Continuous Monitoring
CM-04 Monitoring Configuration Chang..
SI-04 Information System Monitoring Tools An..
Monitoring, Logging, Load and Performance Testing
Cloud Service Providers

Figure 2. Cloud Computing Model - Open Secure Architecture[OSA09]

4.1 End Users

End Users need to access certain resources in the cloud and should be aware of access agreements such as acceptable use or conflict of interest. In this model, end user signatures may be used to confirm someone is committed to such policies. The client organization should run mechanisms to detect vulnerable code or protocols at entry points such as firewalls, servers, or mobile devices and upload patches on the local systems as soon as they are found. Thus, this approach ensures security on the end users and on the cloud alike. However, the cloud needs to be secure from any user with malicious intent that may attempt to gain access to information or shut down a service. For this reason, the cloud should include a denial of service (DOS) protection. One way of enforcing DOS protection is done by improving the infrastructure with more bandwidth and better computational power which the cloud has abundantly. However, in the more traditional sense, it involves filtering certain packets that have similar IP source addresses or server requests. The next issue concerning the cloud provider to end users is transmission integrity. One way of implementing integrity is by using secure socket layer (SSL) or transport layer security (TLS) to ensure that the sessions are not being altered by a man in the middle attack. At a lower level, the network can be made secure by the use of secure internet protocol (IPsec). Lastly, the final middle point between end users and the cloud is transmission confidentiality or the guarantee that no one is listening on the conversation between authenticated users and the cloud. The same mechanisms mentioned above can also guarantee confidentiality.

4.2 System Architects

System architects are employed with writing the policies that pertain to the installation and configuration of hardware components such as firewalls, servers, routers, and software such as operating systems, thin clients, etc. They designate control protocols to direct the information flow within the cloud such as router update/queuing protocols, proxy server configurations or encrypted tunnels.

4.3 Developers

Developers building an application in the cloud need to access the infrastructure where the development environment is located. They also need to access some configuration server that allows them to test applications from various views. Cloud computing can improve software development by scaling the software environment through elasticity of resources. For example, one developer can get extra hard space as an on-demand resource, instead of placing a work order and wait for several days for the permission. Developers may desire extra virtual machines to either generate test data or to perform data analysis, processes which take significant time. Also, using more processing power from the cloud can help in catching up with the development schedule. The cloud also helps developers create multiple evaluation versions environments for their applications, bypassing the need to incorporate additional security within the application and placing the burden on the cloud provider. One significant drawback of cloud computing at the moment is its limitations to Intel x86 processor architecture. Even if this may very well change in the future, it is another stumbling block that developers and cloud computing experts need to overcome. Software monitoring may be done by monitoring API calls for server requests. With an architectural model where data is centralized, all eyes are focused in one direction, which implies better monitoring, although ultimately the issue rests with the developers/clients on how much effort will be directed in this regard. As far as security patches for the software as service approach, updating a patch is easier done in the cloud and shared with everyone seamlessly, rather than finding every machine that has the software installed locally.

4.4 Third Party Auditors

Third party auditors are used by clients and providers alike to determine the security of the cloud implementation. Depending on the level of commitment to security and usefulness in obtaining a competitive edge, a cloud vendor may choose to submit itself to regular security assessments in an attempt to obtain accreditation. The accreditation process needs to be undertaken every three years. Thus, in order to lower the constraints on the cloud vendor, some organizations may implement continuous monitoring of the cloud system.

4.5 Overview

The cloud is the resource that incorporates routers, firewalls, gateway, proxy and storage servers. The interaction among these entities needs to occur in a secure fashion. For this reason, the cloud, just like any data center, implements a boundary protection also known as the demilitarized zone (DMZ). The most sensitive information is stored behind the DMZ. Other policies that run in the cloud are resource priority and application partitioning. Resource priority allows processes or hardware requests in a higher priority queue to be serviced first. Application partitioning refers to the usage of one server or storage device for various clients that may have data encrypted differently. The cloud should have policies that divide the users' view of one application from the backend information storage. This may be solved by using virtualization, multiple processors or network adaptors. [OSA09]

5. Conclusion

Cloud computing is still struggling in its infancy, with positive and negative comments made on its possible implementation for a large-sized enterprise. IT technicians are spearheading the challenge, while academia is bit slower to react. Several groups have recently been formed, such as the Cloud Security Alliance or the Open Cloud Consortium, with the goal of exploring the possibilities offered by cloud computing and to establish a common language among different providers. In this boiling pot, cloud computing is facing several issues in gaining recognition for its merits. Its security deficiencies and benefits need to be carefully weighed before making a decision to implement it. However, the future looks less cloudy as far as more people being attracted by the topic and pursuing research to improve on its drawbacks.

6. Acronyms

- OCC - Open Cloud Consortium
- IP - Internet Protocol
- SLA - Service Level Agreement(s)
- PHP - PHP Hypertext Preprocessor
- API - Application Programming Interface
- DHCP - Dynamic Host Configuration Protocol
- FTP - File Transfer Protocol
- MAC - Media Access Control
- OSA - Open Secure Architecture
- DOS - Denial of Service
- SSL - Secure Socket Layer
- TLS - Transport Layer Security
- LAN - Local Area Network
- IPsec - Secure Internet Protocol
- DMZ - Demilitarized Zone

7. References

[Balding08] Craig Balding, "ITG2008 World Cloud Computing Summit", 2008
http://cloudsecurity.org/

[Croll08] Alistair Croll, "Why Cloud Computing Needs Security", 2008
http://gigaom.com/2008/06/10/the-amazon-outage-fortresses-in-the-clouds/

[Erickson08]Jonothan Erickson, "Best Practices for Protecting Data in the Cloud", 2008
http://www.ddj.com/security/210602698

[Brodkin08] Jon Brodkin, "Seven Cloud-Computing Security Risks", 2008
http://www.networkworld.com/news/2008/070208-cloud.html

[Mills09] Elinor Mills, "Cloud Computing Security Forecast: Clear Skies", 2009
http://news.zdnet.com/2100-9595_22-264312.html

[Perry08] Geva Perry, "How Cloud & Utility Computing Are Different", 2008
http://gigaom.com/2008/02/28/how-cloud-utility-computing-are-different/

[Weinberg08] Neil Wienberg, "Cloudy picture for cloud computing", 2008
http://www.networkworld.com/news/2008/043008-interop-cloud-computing.html?ap1=rcb

[Schwartz08] Ephraim Schwartz, "Hybrid model brings security to the cloud", 2008
http://www.infoworld.com/d/cloud-computing/hybrid-model-brings-security-cloud-364

[OCC08] The Open Cloud Consortium, 2008
http://www.opencloudconsortium.org/index.html

[OSA09] Open Security Architecture, 2009
http://www.opensecurityarchitecture.org/cms/

[Jager08]Paul Jaeger, Jimmy Lin, Justin Grimes, "Cloud Computing and Information Policy", March 2008

[Rittinghouse09] John Rittinghouse, "Cloud Computing: Implementation, Management, and Security", 2009

[Armrust09] Michael Armbrust, Armando Fox, ... , "Above the Clouds: A Berkley View of Cloud Computing", February 10, 2009

[Reese09] George Reese, "Cloud Application Architectures", April 2009, O'Reilly Media

[Miller08] Michael Miller, "Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online", August 2008

[Lamb09] John Lamb, "The Greening of IT: How Companies Can Make a Difference for the Environment", April 2009, IBM Press

[Gu08] Yunhong Gu, Robert L. Grossman: Sector and Sphere: The Design and Implementation of a High Performance Data Cloud, UK, 2008.

Last Modified: April 30, 2009
This and other papers on latest advances in network security are available on line at http://www.cse.wustl.edu/~jain/cse571-09/index.html
SHARE Back to Raj Jain's Home Page