Security Issues and Challenges – Cloud Computing

Daniyal M. Alghazzawi[1] Syed Hamid Hasan[2]

[1,2] Information Security Research Group
Faculty of Computing and Information Technology, Department of Information Systems
King Abdulaziz University, Kingdom of Saudi Arabia

Abstract

Cloud computing is in its preliminary stages when we respect to its implementation & usage. The reason for this is that the technology is heavily dependent on the high-tech resources that the academicians and researchers find it practically impossible to analyze & test the technology. The basis of the cloud computing process is a desire to have another layer added while information is processed. Cloud computing is generally understood as computing in grids and as a utility where the software is provided as a service and the storage is provided through the cloud via virtualization, which means that the client remotely uses a service provided by a provider commonly termed to be "in the cloud". It is being debated if the aforementioned components can be separated and can be individually dealt with, however there is a general agreement that they all come under the cloud computing collectively. There have been many discussions related to the Cloud computing from the actual providers of the Cloud computing, as there has been a lack of published work from the academicians. However, the researchers are also making their presence felt by addressing many of the issues related to cloud computing.

Keywords: *Cloud Computing, grid computing, Security Issues, Secure Architecture Model*

1. Introduction

The concept of Cloud computing should not be termed as an invention, but it is has its origins in the needs to provide an infrastructure, as a service, that is aimed for requirements of mega computing or big storage spaces. From the viewpoint of the provider it is a mechanism by which peripheral infrastructure is provided so as to mitigate any downtime in the network without the users being aware of it, in addition to the fact that the users' data is transferrable in-between clouds. Balding at [1] suggest that the front-end software, the middle ware and the backend be designed in the form of layers making it possible for each layer to be independently dealt with in implementation, testing and functionality. The following paper attempts to introduce cloud computing in its present state, along with the research efforts from the industry and the academicians and the challenges faces in its development. It goes on to describe the security issues and the benefits in cloud computing along with presenting a secure architecture model that can be used for implementing cloud computing.

2. Present Viewpoint

The Critics of cloud computing contend that it is not a secure mechanism as the data is no longer present within the safe confines of the Company's LAN. The security of the data is dependent on the level of commitment the vendor has in enforcing security policies and verification done by third party. The verification is being offered to the clients as an on-demand service by vendors such as Google, Salesforce and Amazon etc. Statistics at [3] show that 1/3 of the security breaches occur because of the unauthorized access to machines, whereas information being stolen by employees amounts to 16% of the breaches. The aforementioned breaches can be completely avoided if the data is stored in the cloud. Additionally, since vendors have high availability of resources they can update security patches for applications, Operating Systems and middleware much faster. As per the vendors offering cloud service, most cases of theft occurs when the data is not protected properly by users that have authorization to access data. In case of a session in a cloud we can configure the browser to delete

all sessions data and to maintain a log in the cloud that describes what data was access by which user. This approach is far secure than storing the data on the client side. For certain application the best option is cloud computing, like the NY Times that uses the cloud service provided by Amazon. It uses the service to convert its archive of articles into PDF format. If the servers at NY Times were put to use they would have taken about 14 years in completing the task, however the same task was achieved by the cloud in a matter of just a day at the expense of a few hundred dollars. [4]

Despite the advantages the technology is still only being used by small companies that want to reduce cost, or individual developers that want to offer their application as services on the cloud. The big names are only testing the cloud computing with small time applications. However, we cannot blame the fraternity for this cautious approach and we will discuss below the Continual Development, the research efforts of the academicians and the industry along with the challenges of cloud computing.

2.1 Development

New developments are continuously being added into the cloud computing technology with the aim of enhancing security. One such product is QualysGuard, which is meant for discovering the loopholes in a network. It has acquired considerable reputation after being used by almost 200 of the Forbes Global 2000 companies. The product functions by placing an apparatus behind the Firewalls where it monitors the network for any breaches or threats. All data is encrypted by the device and it has no access to the client's data, with just access to only specified IPs and the administrator for modification of script & credentials. The product provides a new mode of security where any possible threats or attacks are monitored and dealt with by a 3rd party. In case of an unauthorized access attempt or an attack on any of the services rendered by the cloud, the solution cuts off access to the service from the source of the threat and prevents it from affecting the service availability.

2.2 Research efforts by Academicians & Industry

A few IT companies and universities have partnered to further research in the field of cloud computing. They aim to explore methods to reduce the cost of computing and storage in the clouds. The group is named Open Cloud Consortium (OCC). It also aims to establish the standards of communication amongst various providers. The OCC was formed in the middle of 2008 making it a fairly new entity, and showing that the entire discipline is fairly young. Following are some of the aims of the OCC:

1. To develop the cloud computing standard & framework to be used for cloud interoperations
2. Development of benchmarks
3. Implementation of support references for cloud computing, if possible open source references.
4. Management of a cloud computing testbed called "Open Cloud Testbed".
5. Sponsoring workshop and event linked to cloud computing.

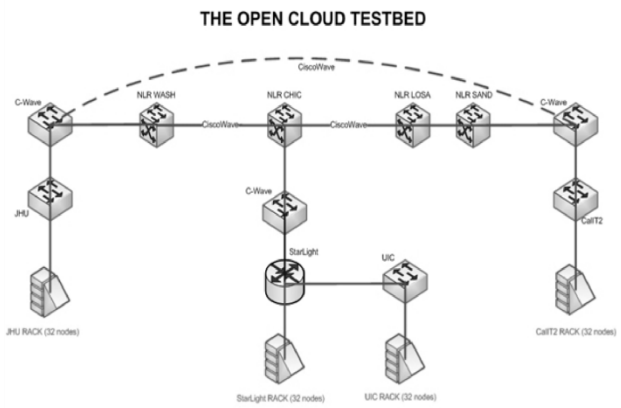

Fig. 1 OCC Network Layout

Figure-1 shows the network layout of the Open Cloud Consortium. The network is established between the servers at Universities of Illinois, John Hopkins, Calit2 and StarLight. Using the aforementioned architecture and the published network, the OCC has been working to implement a design and protocol for high traffic flow amongst various location[5].

2.3 Challenges

There are certain primary challenges that are faces by cloud computing in being deployed on a

large scale by the enterprises, some the challenges are:

a. High Availability – Whenever there is disruption of service by failure of Network, Storage or application the vendor must ensure that the service does not get affected, through a backup that must run at all times. The switch should also be seamless so as not to have a major impact on the users.
b. Service Level Agreements – The network is governed by the service level agreement that necessitate multiple instances of the application on different servers so if it is required a low priority application may have to be shut down or minimized.
c. Multi-Tenancy – There is a possibly a conflict of interests arising of the fact that the same application and hardware is being used by many customers at the same time.
d. Linear scalability – The cloud should be able to cope with the requirement of increasing the data processing capability linearly as the if we have x number of users requiring the resource y then the time for completing the request for resource should remain Y*1 rather than X*Y so the cloud should be capable of adding X number of devices.
e. Management of Data – When we have a large number of clients using the same resources like data storage then to distribute, partition, secure and synchronize the data is a challenge.

3. Security Challenges

The small companies, most of the times, do not have suitable protection available against the attacks as they lack hardware as well as software resources. Loopholes in the programing make the firewall ports vulnerable. This challenge compels the small companies to switch to cloud computing rather than option for maintaining their own hardware. Yet, cloud computing also has its share of drawbacks. For example, if the cloud fails than it becomes responsible for the failure of multiple clients connected to the cloud. Additionally, an optimal approach to Low power transmissions & high availability needs to be found despite the fact that major players like AT&T believes that distributed cloud architecture is the optimal mode of implementing the cloud. [2]. It is believed that due to the lack of an effective security policies would soon cause most of the major clients to shift away from the cloud computing approach. One more issue is the different methods and approaches in storing of data by the various cloud providers thus making is more difficult to establish the distributed cloud architecture between them.

3.1 Data Security

The term security encompasses various factors like confidentiality, integrity & availability. This a major concern for the providers. With Confidentiality we mean to decide who has the onus of storing of encryption keys used to encrypt the data of a company, The encrypted data stored with the vendor must be kept secured from the employees of the vendor. A possibility is that the client stores the encryption key.

With Integrity we mean absence of a common policy for approved data exchange; different protocols are being used by vendors to transfer various software image or job across the industry. We can work around this, for maintaining the security on the client's side, by using thin clients requiring the minimal possible resources and not storing any data on the client side so that there is no possibility of the data being stolen. The method is resistant to the attacks that aim on acquiring this data on the client side. Some, companies contend that by implementing a system with unpublished APIs we can provide better security, but it also have the danger of being reverse engineered. Additionally upgrading of firmware via DHCP & FTP is considered to be insecure for quite some time. However, the very same features being implemented through thin client products from Wyse are considered to be the safest available. [1]

Last but not the least is the most crucial problem of availability, as many of the companies that use the concept of cloud computing have suffered from downtime. E.g. a "denial of service" attack was experienced by the servers of Amazon.com. One more thing to consider is that contract policy exist between the client and the vendor implying that the data would belong only to the client and third party may not get involved

at any manner at any point of time. Authentication should also be proved by a combination of hardware and software means like a flash card or a finger print reader along with a password. This provides us with an advantage that the security of the client software may not be as stringent as earlier.

3.2 Cloud Computing Security Issues

A number of issues must be tackled before making it possible for the large companies to adopt the cloud computing architecture. The major ones are:

a. User access Privileges – Transmission of on the internet is prone to be attacked and is susceptible to risk owing to the issue of ownership of data. Thus companies should have ample knowledge of the policies of the provider. They may even test them by using a small application first.
b. Compliance to Regulations – The security of the solution and its accountability finally rests with the client as they have the option to choose between vendors who agree to be audited by 3rd parties for security and those who do not.
c. Location of Data – Some of the companies do not even have the knowledge of the location of their data, based on the contract type.
d. Segregation of Data – Mechanism for segregation of data need to be in place for as encrypted data for different clients is stored on the same storage.
e. Recovery – There should be a disaster recovery mechanism deployed by the vendor for protecting the user's data.
f. Investigative support – The Companies should have recourse to different legal means of investigation, if it is suspicious of any dubious activities by the vendor.
g. Viability for a Long term – The companies should have the option to cancel the contract and retrieve all the data if the vendor company is taken over by some other company.

Even though we understand that not all of the aforementioned points are relevant for all applications however, it is still critical that the concept is subjected to some sort of standardization if it needs to be accepted by the large enterprises.

3.3 Benefits

We know that we have a number of issues related to security that need to addressed when it comes to security, even then the concept brings forth a number of benefits related to security of Data. We now discuss some of such concepts like Incident Response, Centralized storage of data and logging.

The approach of Centralized Data is similar to putting all the eggs in a single place. Even though it presents a danger of being dependent on one resource, however it makes easier to monitor the data. The cloud data storage does away with many issues like misplacing the devices containing data, which is single largest reason of data loss by large companies or governments. In the cloud architecture only a small amount of data related to the thin client would be stored on device and even for connection the authorization is done at the cloud. Additionally when an access device is reported to be stolen the administrators can block all access attempts originating from the MAC address of the device. It is also easier to encrypt the data on the cloud then having to encrypt the data on each individual disk or backup tape.

The concept of Incident Response means the clients ability to have its hands on any required resources whenever required. This resource could be a processing capability, storage server or even a test environment. The concept circumvents the traditional and tedious process of securing resources in the traditional corporate environment. Additionally, in case of downtime of a server for maintenance the environment may be easily recreated by the client on an alternative machine with ease causing an improvement in the acquisition time. Hashes and checksum are provided for each file stored on the cloud by the vendors to evade the requirement of encryption of the files on the client side. However, it does not mean that the data is not encrypted before being sent on the internet, it simple means that the service is rendered from the cloud side.

Another feature available is the Password Assurance Testing which utilizes the processing capabilities available in the cloud to track and monitor the attempts made to break into the system of the company by use of password

breaking/guessing., in turn it helps in minimizing the required resources and time from the client. The concept of Logging is benefited by the fact that the client side does not need to worry about maintaining the logs of the transactions happening and the cloud searching facilities yield the results much faster. Moreover, the accessing of any resource by the user at any point of time can be easily identified.

4. Secured Architecture Model

OSA (Open Security Architecture) provide a free framework capable of being integrated easily into any application. The framework has its basis on plans that depict the flow of information for specific implementations, along with the policy being implemented in every phase for security reasons. In the following figure we propose the architecture of a cloud to enable envisioning of the constituents of a cloud architecture alongside description of the element that makes the architecture secure. End users, System Architects, developers, third party auditors along with the cloud are the important entities that are involved in the flow of data. We now look at the attributes and the mechanism existing for them.

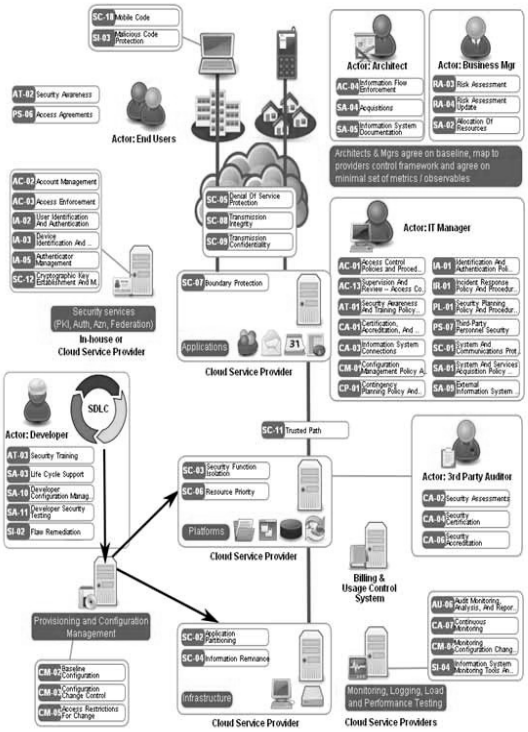

Fig. 2 Open Secure Architecture- Cloud Computing Model - [6]

4.1 End User

Access to certain resource, is required by end user, in the cloud and hence he must be conscious of the access agreement like the acceptable method of use / conflict of interests. Here, the commitment to the policy may be confirmed through the signature of the end user. All code and protocol on the client side devices such as the Server, Firewall or Mobile device, susceptible to attack must be detected and a patch uploaded to secure the local machine immediately upon detection. This ensures similar security for the cloud and the client. However, in case of the cloud there is a need of additional security from a user who tries to access the cloud with ulterior motives. Thus the denial of service (DOS) protection should be included in the cloud. One method of implementing denial of service protection is through improvement of infrastructure via increased bandwidths and higher processing capabilities which are in abundance in the cloud. From the traditional perspective, it involve filtration of specific packets that have analogous source IP addresses/server request. Once the security is catered to at the cloud level then we come across the issue of integrity of transmission between the cloud and the client. SSL/TSL (Secure Socket Layer/ Transport Layer Security) protocols can be utilized as one of the measured to ensure integrity of the transmission and preventing any attacks in the middle. IPsec (Secure Internet Protocol) can also alternatively be used to secure the network at the lower level. The last concern is to ensure that there is no eavesdropping on the session and the above mentioned measures can also be used to present unauthorized barging into the session.

4.2 System Architects

After the end users the system architect plays another role in flow of data. They write the policy pertaining to the configuration and installation of the HW component like firewall, server, router, & SWs like the OS and the thin client etc. System architects are also responsible for designating the control protocol that is to be used in directing the flow of data within the cloud e.g routers update/queuing protocol, proxy server's configuration or encryption of tunnels.

4.3 Developers

Next in line are the Developers who need access to the infrastructure of the development environment to build the applications in the cloud. Access to configuration servers is also required for testing of the applications designed from different viewpoints. Elasticity and availability of the resources offered by the cloud computing environment can be utilized to scale the SW environment and in turn help in the development E.g. if storage space is required by a developer he can get it instantly on demand from the cloud instead of going to the lengthy process to place a workorder & wait for long for the required permission. Additional virtual machiens may be prepared by the developers that can be used to obtain test data and for data analysis purposes all of which are time taking tasks. Additionally, the extra computing capabilities available at hand from the cloud can considerable cut down on the development time. The developers can also use the cloud for creating multiple evaluation environment to be used for the application, this will help to bypass the requirement of incorporating added security in the applications and burdening the cloud. However, the cloud computing environment is currently limited to Intel(x86) based architecture. Which proves to a be hurdle that the developers and the experts on the cloud computing need to be overcome. It is expected that the alternative architecture may also be available in the future. Call for server request from the API can be monitored to monitor Software. Thus Data centralization architecture makes is possible for focusing in a single direction making monitoring easier, even though it depends upon the clients and the developer about the amount of effort they want to put in this regards. The “Software as service” approach makes it easier for updating of the security patches on the cloud rather implementing the patches on each individual machines that have the SW on them.

4.4 Third Party Auditors

The security level of the cloud implementation need to be audited by a 3rd party auditor and this practice is supported both by the client companies as well as the Cloud vendors. Accreditation obtained by the vendor provides him the competitive edge and proves his level of commitment towards security. The process of accreditation is required to be carried out once in a three year cycle. So some companies may adopt an approach of continuous monitoring to lower the dependability on the cloud provider.

4.5 Overview

DMZ (demilitarized zone) approach of boundary protection is implemented by the cloud, like data centers, to ensure secure interaction among the various constituent entities like firewall, router gateways, storage & proxy server. Information that is most critical is stored on the other side of the demilitarized zone. Application partitioning and resource priorities are the other policies utilized to. Application partitioning uses a single server or storage for a number of client that have different forms of encryption used to encrypt data. The cloud must be able to distribute the view of the users of an application from the information stored on the backend. This can be achieved through may virtualization, multiple network adaptors or processors. Resource priority means allowing the processes or hardware requests to be queued in a queue on the basis of priority [6].

5. Conclusion

We can conclude that the concept of Cloud computing is yet to mature in to a full blown option that can be considered to be implemented by large conglomerates. And the challenge of making it so is being lead by the IT experts with the academicians nudging behind slowly. Formation of many groups like CSA and OCC have been done to find the offerings of cloud computing. They also aim at establishing a protocol for communication between various providers. In the present situation recognition is being gained by cloud computing however it faces many hurdles in doing so. However we need to carefully analyze the pros & cons, advantages & disadvantages of the concept in order to pass a judgment on the feasibility of Cloud computing being a major option of being implemented on a mass basis. Yet things look promising for the sphere as more and more researchers are option to pursue the task of analyzing and improving cloud computing.

References

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

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

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

[4] Neil-Wienberg, "Cloudy picture for cloud computing", 2008, http://www.networkworld.com/ news/2008/043008-interop-cloud-computing.html? p1 =rcb

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

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

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

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

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

[10] George-Reese, Cloud Application Architectures, O'Reilly-Media, April-2009.

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

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

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

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

Daniyal M. Alghazzawi has completed his PhD in Computer Science from University of Kansas in 2007, Master of Science in Teaching & Leadership in 2004 and Master of Science in Computer Science in 2003 from University of Kansas. He has worked as Web Programmer at ALTec (Advanced Learning Technologies). Dr. Daniyal is currently working as Associate Professor in the Information Systems Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, KSA. He has more than 20 publications to his credit. His research interest includes e-Security and Cryptography and Educational Technology. Dr. Daniyal is a member of IEEE (Education Transaction) and ACM-SIGCSE (Special Interest Group in Computer Science Education).

Syed Hamid Hasan has completed his PhD in Computer Science from JMI, India, MSc in Statistics and PGDCS from AMU, India. Dr Hamid has a teaching and research experience of more than 30 years and is currently working as a Professor at Information Systems department, faculty of Computing and Information Technology, King Abdulaziz University, Kingdom of Saudi Arabia. Prof. Hamid has worked as the Head of Computer Science department at AMU, India and also Head of IT department at the Musana College of Technology, Sultanate of Oman. He was Reviewer for NDT 2009, Ostrava, Czech Republic, 2009 Co Sponsored by IEEE Communications Society. He is included in the Panel of referees of "The Indian journal of community health", and was Chief Coordinator of the National Conference on "Vocationalization of Computer Education" held on 28-29 September-1996 at A.M.U. Aligarh, India. He is a life Member of Indian Society for Industrial and Applicable Mathematics (ISIAM), Computer Society of India (LMCSI), Fellow National Association of Computer Educators & Trainers (FNACET), India and a member of the IEEE. He has more than 25 research articles in conferences & journals to his credit. His research interest includes e-Security and Cryptography, administrative computing and software engineering.