Harpreet Singh

CS 4960 – Senior Seminar

Dr. Martin

Research Paper

November 03, 2010

CLOUD COMPUTING : ISSUES

Introduction

Cloud computing is a technology in which data and different applications are kept on storage networks and servers which are located in a remote place and accessed by the users via the Internet. It has two parts in it that is the access via the internet using the Web browser to the resources which are administered remotely and allocated and de-allocated basing on the requirements of the users. While the other one is paying for the actual use of the computing resources. This technology of cloud computing allows businesses and consumers to get access to applications without the need of installing them on their own on-site servers. As mentioned by, the applications are installed on remote servers. In the normal way of applications use, consumers purchase licenses for application software from their software provider and install them on their on-site servers. In cloud computing case, it is On Demand basis where consumers pay a subscription fee for the service. The use of this technology increases efficiency because the storage, memory and processing are centralized. There are challenges that are experienced when cloud computing are deployed on a large scale. They are discussed as follows:”

Self-healing is a challenge that is experienced in cloud computing such that whenever there is a failure in network, or application, there will be timely backups and this will seem to be nothing to the end-users. This has not been achieved. Another challenge is that of service level agreements. The cloud computing developers have not been able to create several instances of an application on many computers. This has been the desire of these developers from time immemorial. This is still a challenge and there is striving in this field to realize this goal. When this is achieved, the power shutdown will be minimized. There is another challenge in the use of hardware where the users may be using one hardware resource even without their understanding of what is happening behind the scene. This has in most times brought about conflict of interests amnion the users. The issue of virtualization is still thorny in the world of cloud computing. This is a case where applications are not specific on what hardware they are using. This has brought about conflict of interest in the programs.

Another problem of cloud computing is linear scalability. It is projected that a cloud should e able to handle an increase in data processing in a linear proportion. This has not been achieved also and still remains a challenge in the world of computing. There is still a challenge in the portioning and management of data. Although there are technologies that have been introduced to counter this problem, there are many things that are still to be desired.

Security challenges

Companies which are still n their infancy stages often lack the measures for protection to counter the attacks that are directed at their servers. This is due to lack of resources and poor programming in the cloud computing systems that they deploy. Programming languages like PHP and JavaScript have ports to firewalls. These ports are more often susceptible to denial of service problems. For this reason, there are campaigns that companies should opt for cloud computing as opposed to supporting their own hardware backbones in the company premises. Although there is a lot of hype in use of cloud computing, there are pitfalls that come with this technology. First, it has been seen, at least with new starters that it presents a scenario where it acts as a source of failure for many resources in the network. Although implementers and network carriers like AT&T insist that it is the best technology to be used in distribute computing, they lack the technology they can use to transmit in low power network. There is a notion that companies will shy away from implementing cloud computing due to the fact tat there is no security policy that has been laid exclusive for cloud computing. It is like every company and cloud providers come with their own security policies. What is more, there is no security measure that has been implemented and to be followed globally. The main problem here is the fact that the different providers of the cloud come up with their own ways of storing data; this has brought about the challenge that the cloud computing challenges are to be solved by the vendors.

Data security

Security of data refers to confidentiality and availability of data; this has been a major issue for vendors. Confidentially entail issues like who owns the encryption keys of the data and which employees should be allowed to access of these encryption keys. One of the problems that can be seen here is the fact that there is no universal policy to be followed when it comes to implementing security in the cloud. Every vendor come with their own security policy and this becomes erratic in the whole security implementation process. One the ways that have been adopted to maintain security on the client side is the use of thin client. One advantage of this is the fact that minimal resources and information are stored on the server. Passwords are not stored here either this eliminating the issue of stealing passwords. This concept, however good it may seem, is impervious to data theft. There is, however, the implementation of unpublished APIs (Andrei, T. 2010).

The last problem of cloud computing is the availability of data. There have been claims that the data are not available when the cloud computing providers are experiencing downtime. There is need to make sure that the agreement between the client and the vendor is such that the data belongs to the client at all times.

Secure architecture models

Open Security Architecture (OSA) is known to provide frameworks that are integrated to applications for the sake of security implementation in these applications. The pattern is based in a schematic way; the implementation is shown in reach step so that security is assured. The model that is described here help the reader and the researcher to envision the element that makes it secure.

End users

The end users are the people who are going to use the system. They should be aware of the issues that entail the security of the system. They should be provided with security mechanisms that will ensure the security.

Systems architects

These are the people who are entrusted with the development the system. They are also tasked with the design issues of the system. They look at the security protocol in the system.

Overview

The cloud computing incorporates network appliances like routers, proxy and storage servers. The interaction of all these devices and entities should be in a secure manner. For this case, the cloud implements a boundary that is used for protection that is called the demilitarized zone (DMZ). The information that is deemed sensitive is stored behind the DMZ. The other applications that re stored in the cloud are used for partitioning and application data grid. The cloud should be in a position to divide the view of the users from the view of the back-end users. This issue could be resolved by using virtualization (Andrei, T. 2010).

Cloud computing has been met by high percentage of acceptance. One of the reasons for this acceptance is the economic benefits of this technology; it has been found that there is reduced capital expenditure (CapEx) and also the reduction of operational expenditure (OpEx). Also this is the case; there are still some issues that are to be solved with the use of this technology. Among the challenges that are common in the world cloud computing include the fact that the data is trusted to third-parties. The owner sends the data to remote sites thus bringing the issue of security into fore. Most of the issues that come up when discussing cloud computing issues come into fore due to issues related to organizational means. Some sections of the paper will talk about the technical issues that arise from cloud computing.

Security is becoming a major issue of concern for most of the clients. Before committing to a cloud computing vendor, many clients will want to know what measures are there for the vendors so that they are sure that their data are secure. The security details should be comprehensive enough so that the clients have the minds of the coders, security officers and operators. It is also desirable that the vendors are in a position to identify vulnerabilities which are hard to come by.

There are many security issues that are associated with cloud computing. One of the security issues is that of privileged access of the data. The fact that data are processed outside the premises of the organization brings with it a lot of risks. The data that are processed bypass the control of the personnel and physical security measures. The clients should garner all the information they need about who really handles their data in the cloud. They should get the information on how the data is managed, the personnel's they manage and their qualifications.

Another very vital issue on cloud computing is the fact that customers are responsible for their own data even if the data is held by another party. This should be put into consideration and the customers should be concerned about this.

There is another issue on the location of the data. Most of the times, the customers are not in a position to get the location of the data in the cloud. They may not even be in a position to locate the country in which the data is stored. It is advisable that the clients request that their data be stored within a given jurisdiction. They should also demand to know if they will need to sign to different policies if their data are stored overseas.

Data segregation is also of paramount importance with the use of cloud computing. This is so because the data in the cloud are from different clients that have also signed for the same services. The data in the cloud can mix with these from the other vendors. This should be taken care of by the company. They should have a provision where the data from the company is autonomous. The customer should ask such questions like, what are the methods that the company uses to have data segregation. An accident which makes data to mix with the rest can e make the data unusable and can even cause the encryption techniques complicate the availability of the data.

Data recovery should be taken care of by the cloud computing provider. Even if the user does not have ka clue of where the data is stored, there should be a well-explained plan that shows the way the data is to be recovered. The tome it will take to get the data back should be clearly labeled.

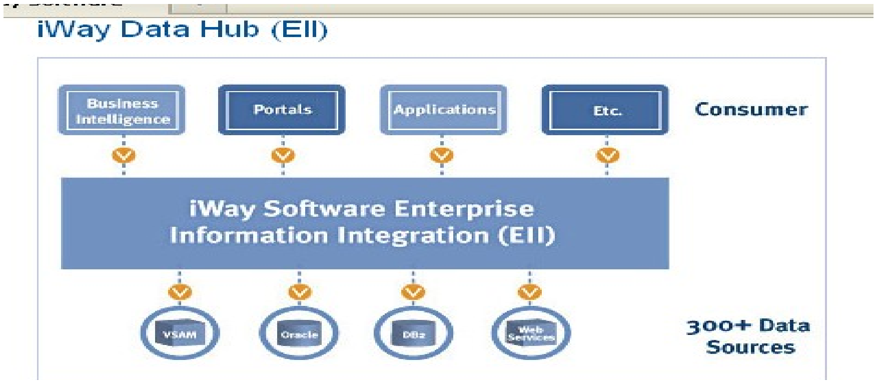
Data that is stored in the cloud usually need well authenticating mechanisms. In the traditional way of data security, the authentication is usually through passwords and tokens; on the other hand, encryption on the cloud is through Transport Layer Security (TLS) which are enforced through cloud computing applications and services. Using a secure client in authenticating information in the cloud is a hacker's worst nightmare.

Most organization store large volume of information in a cloud computing storage, most of those data or information is so sensitive that requires frequent access monitoring and protection. This information is very vital for the organization, in that the loss will not be anticipated by any organization. The whole markets are created to protect the stored information and data for enterprises. Data is the raw material of information economy in any organization thus data governance should be a strategic tool in success of any organization. The information access by right people at right time is important in any organization.

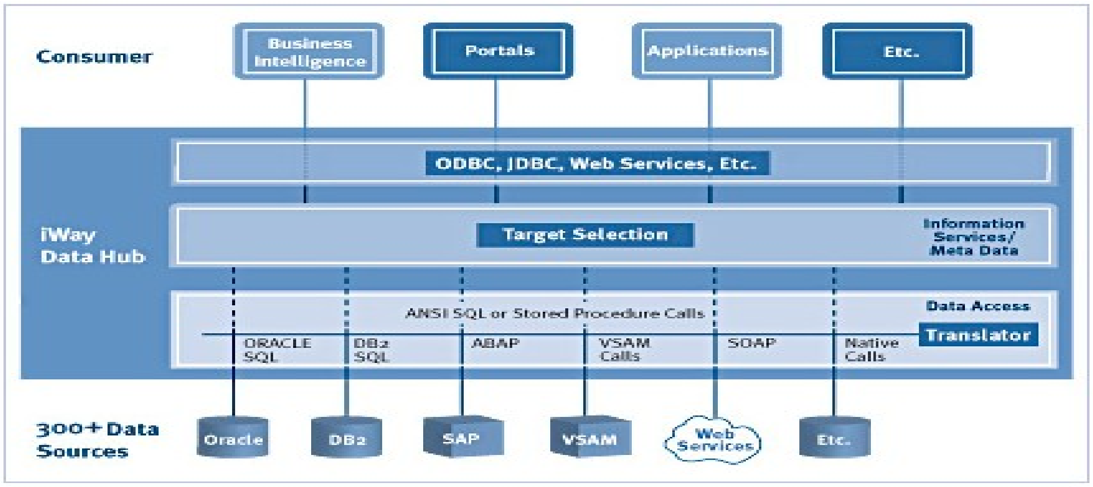
Cloud computing apply virtualization technology to assist organization in breaking the physical bonds the Information technology infrastructure and the users. Because the cloud organization is given the responsibility by business enterprises to control over the asset security, it's their duty to provide a strong security model. Cloud model make the clients to lose control on physical security. In public cloud computing where service are dynamically on self-service basis over the internet, in this model organizations organization will be sharing resources with other organization. The shared pool which is external to the organization, an organization will not have the insight knowledge or the control on the running resources and its location. The exposure of organization information to external world will enable the government to seize the company asset by other company breaching the law of information sharing, this occurs because of shared environment, public cloud.

System integration is another problem faced by cloud competing organization; an example is storage device provided a certain cloud vendor may be incompatible with another vendor's service. This result to end users switching from one cloud vendor to another, this is inefficient mode, especially on business people who need a reliable and efficient system. The vendor create this service which make end user difficult to transport from one cloud vendor to other (example is Amazon's "simple storage services' [S3] which incompatible with IBM's Blue Cloud (Google), and Dell. To solve this situation scholars have come with software's which will provide platform compatibility, an example is iWay Software's Enterprise information Integration (EII) which creates a federal view of all data source with the real-time access (Rittinghouse, & Ransome, 2009).

Figure below is iWay Data hub (EII)



The iWay Software Enterprise Data hub with iWay universal Adapter enable the Implementers to develop a federated view of more than 70 data sources, this include relational databases, files, databases and some selected application packages. iWay data hub is integrated with real-time visibility and access to a multiple, information source in and outside enterprise, the hub will aggregates the information from different sources into a single unified logical view to enable developer work with heterogeneous environment, when developing an application such as end-to-end business process transaction system ("iWay Data Hub").



The iWay Data Hub aggregates information from over 300 sources on more than 35 platforms, These platform include; relational databases, transaction systems, applications, e-business documents, ERP and CRM packages. To access data they use; SQL to non-Sql, Standard SQL to proprietary SQL transformation, SQL pass-through, Join processing, and resource governing (“iWay Data Hub”).

Insecure Interfaces and APIs is one of security issue on cloud computing, when front end user request for service the cloud computing exposes a set of software’s interfaces that a user uses to manage and interact with cloud service, Since the security and the availability of cloud services will dependent on security basic of APIs, authentication and access control , and encryption will require the interfaces to designed so as to prevent malicious attempt of altering the policies of cloud computing vendor.

Virtualization makes the cloud computing operate effectively, the virtual machines enable diverse organization to be located on central place on the same physical resource, the physical segregation and security of hardware-based can not protect attacks between virtual machine on the same server. This expose organization with security risks, the dynamic feature of virtual machine will make hard to maintain the consistency of security. Locating insecure virtual machine is very difficult on cloud computing, to solve this problem; it will force the vendor to have intrusion detection to detect malicious activity at the virtual machine level (Rittinghouse, & Ransome, 2009). To address this issue there is need for analyzed security model of the cloud provider interfaces; strong authentication and access control are implemented with encrypted transmission.

In virtualized environment operating systems and applications are shared on physical infrastructure and requires system, file, and activity monitoring to provide a confidence on customer on their resources, on cloud computing platform, enterprises are one to subscribe to cloud computing resources, with responsibility of patching taken care by subscriber.

Service/ account hijacking is another challenge which threaten the development of cloud computing, account and service hijacking involve , fraud and exploitation of software vulnerability, since passwords and credential are been used frequently, make easier for this attack to take place. When an attackers gain access to someone credential, they can eavesdrop on transaction, alter some information, and send falsified information redirect a front end user to wrong sites. To solve this situation should be no sharing of account credentials among the users and services, embrace the proactive monitoring to detect unauthorized activity.

Data loss or leakage is another issue which is frequently faced by cloud computing vendors, deletion of record or information without backup result to data loss, unlinking a record from larger context will caused it not recovered at all since the storage media is not a reliable source. When encoding keys are not embraced while storing information it can lead to destruction. The threats of data in cloud computation happen because of interaction between risks and challenge which unique issues in cloud computing. To avert this problem the vendors should implement a strong API access control ,encryption and data integrity protection in transit, analyzes data at design and run time level and provide backup and retention strategies.

Challenges for developers

There are many issues that come with cloud computing for the developers. One of the issues that come up when designing cloud infrastructure and architecture is the way the cloud is partitioned. There are algorithms that should be followed when designing the partitions in the cloud.

The number of objects that are to be in the cloud have to be partitioned into a number of clusters. The number of clusters, for this case, is *K.* The basic algorithm for partitioning the cloud includes the following steps:

1. Get the objects for each group in the cluster
2. Find the nearest centroid
3. Add p to C(p) group
4. Update the centroids

The algorithm itself is as follows:

```
Randomly initialize groups
Iterate
     For each point p:
          Find nearest centroid C(p)
          Add p to the C(p) group
Update centroids
```

The above algorithm uses Windows Azure cloud-compouting platform and is written in C#. The framework that is used is .NET. The design of the architecture has three levels which include Tables, Queue, and Worker. The tables include Tasks, Status, Cluster, and EntityCluster. The Queue level includes Queue, and Blob. The last level, Worker includes ClusterJob and EntityJob.

The builder is the one which initializes the storage in the tables makes sure that the entities are uploaded. This is the same area where the remote files are aligned so that they are compatible with is there on the ground. The tester is the one which is tasked with starting the algorithm. The evaluator is the one tasked with computing the score of the algorithm. A remote Web Interface unifies the CLI tools so that there is one single interface.

<u>Challenges with the algorithm</u>

There are challenges that are common in the algorithm. There are improvements that should be done to the algorithm. The challenges are stated in the sections that follow:

i. There are no techniques that are available that can be used to unify the network. In any distributed system, the sections are distributed within the space and there is no tool that can be used to unify the objects in the cloud (Scheier, 2009).

ii. There are poor strategies that have been employed to have an efficient storage within the Blob system. In this regards, the entities have no specific area where they are assigned in the cloud. The arbitrary assignment of the groups is wanting. There should be a method devised that will help in the storage within the system. What is more, there is also the issue of cache within the entities; it should be improved for efficient storage. In this algorithm, there are cases where multiple entities may occur. When there are such occurrences, there should be a provision so that the entities are handled well (Fowler, & Worthen, 2009).

iii. The users lack the capabilities of adding and removing entities. In this case, there is difficulty when the users are supposed to have some entities on the fly. They have to request for the addition of these. With this, it brings the efficient execution of entities abit complicated for many users. There is also no repair tool in this algorithm. There is no tool that can be used to repair tables.

Improvements

There are ways in which the issues that have been listed above be improved so that the storage in the cloud gain optimality. For the first case of unification, this can be achieved by use of reflection so that unification of all the tools involved can be achieved. The handling of the entities can be improved by making sure that each worker is assigned specific entity. This way there will be assured handling of entities in the cloud. It will also help and be easier when handling the entities that will be stored in the cloud. For the multiple entities, each blob should store each multiple entity (Mahmood, 2000).

Another viable solution for the algorithm that can greatly improve it is making user that dedicated threads be used when dealing with split computations and storage queries. The users should also be allowed to add or remove entities. This way, the issue of user inconveniencies is removed.

Computing encrypted data

There are difficulties in the security of the cloud now that they are open for access by anybody interested in the data (Dodani, 2009). There are efforts that are being developed in leading laboratories to make sure that the data in the cloud are encrypted. The main problem here is the fact that when the data is encrypted, it will prove to be difficult to gain free access to the same data that should have been used by the people interested. The security of the data is also of paramount importance. One issue in the data which are stored in a remote place is the fact that there is no way that the data can be manipulated without exposing the same data. For this case, they are to be secured when they are being accessed. One problem that has thwarted efforts to solve this problem is the fact that spam is encrypted every time data is encrypted. This is a problem of major concern given the fact that the spam is also sent over the network to the cloud, in the event the cloud is also affected by the injection (Ramiler, & Swanson, 2004). One of the most annoying things about encryption is the fact the data that has been encrypted will not be accessed not until the encryption is opened with the secret decryption key. This will therefore mean that there are two things which will be involved in the handling of this. In either case, the data will be attacked; if the cloud has infection, the data that is decrypted will be infected and also if the data that has been encrypted are infected, they will infect the cloud (Martin, & Hoover, 2008).

Solution

There is a solution that has been developed that allows one to analyze data or make a computation of a function while the data are still being encrypted. An example is that if one wants to store a file in a server they don’t trust, they will be forced to leave the data as they are because if they open the data, they will expose it (Beweley, 2009). The issue is that the server should not gain any form of access to the data. On the other hand, the user may be interested in accessing the data intelligently. This will be possible by making sure that the data are not exposed and at the same time, they are accessed.

The idea of accessing encrypted data intelligently can be expressed in an algorithm. If the data are encrypted in a full homomorphic scheme, the query for the encryption can be sent to the server and should be expressed as a function f; the server will in turn compute, in a homomorphic way an encryption of f (m_1, …, m_t)----, in this case f(m_1, ….., m_t) gives the files that are relevant and then will send the text that is in cipher text back to you. In this algorithm, it is very possible to encrypt the query also. This will make the data and information that is being sent to be secure as well.

The solution above will help improve and strengthen cloud computing model in the fact that the vendors can be able to compute the data of their clients without exposing the data. Of course they will compute the data under the request of their clients. This solution will also help to solve the problem of email spam which has been there for decades.

References:

Andrei, T. (2010). Cloud computing challenges. Retrieved on 14th September, 2010, from http://www.cse.wustl.edu/~jain/cse571-09/ftp/cloud/index.html

Ramiler, N., &Swanson, B.(2004). *Innovating mindfully with Information Technology.* MIS Quarterly, Vol. 28, No. 4, pp. 553-583, retrieved on 14th September, 2010 from http://www.misq.org/archivist/bestpaper/Swanson.pdf

Dodani, Mahesh (2009). “Cloud computing architecture”. Journal of Object Technology, Vol. 8, No. 6, pp. 35-44 retrieved on 14th September, 2010 from http://www.jot.fm/issues/issue_2009_11/column3/index.html

Beweley, Alex (2009). *What the cloud means for the data center.* The Data center journal, retrieved on 19th September, 2010 from http://datacenterjournal.com/content/view/3344/40/

Fowler, G., & Worthen, B.(2009). *The Internet is on the cloud.* World street journal, pp A1

Martin, R., & Hoover, N.(2008). *Guide to cloud computing.* Information Week journal. Issue No. 23, pp. 21-23, retrieved on 19th September, 2010 from http://www.informationweek.com/news/services/hosted_apps/showArticle.jhtml?articleID=208700713

Scheier, R. (2009). *Can IT manage the cloud? These CTOs can.* InfoWorld online journal, retrieved on 19th Septmeber, 2010 from http://www.infoworld.com/d/cloud-computing/can-it-manage-cloud-these-ctos-can-784

Mahmood, Mo A. (2000). *Impacts of Information technology investment on organizational performance.* JIMS, Vol. 16 Issue 4, pp. 1-16, retrieved on 18th September, 2010 from http://www.jmis-web.org/articles/v16_n4_p3/index.html

“iWay Data Hub.” iWay Software. Retrived on 20th September, 2010 from http://www.iwaysoftware.com/products/eii.html

Rittinghouse, John W. & Ransome, James (2009). “Cloud Security Challenges”. Information Systems Security. Retrived on 20th September, 2010 from

http://www.infosectoday.com/Articles/Cloud_Security_Challenges.htm