National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing (RTMC) 2011
Proceedings published in International Journal of Computer Applications® (IJCA)

An approach Initiating Security Protocol towards Cloud Computing

Amit Joshi
Department of Computer Science & Engineering, Pacific University (PAHER), Pacific Hills, Udaipur (Rajasthan), India

Bhavesh Joshi
Department of Computer Science, Advent Institute of Management Studies, Udaipur (Rajasthan), India

Manuj Joshi
Department of Computer Science & Engineering, Sunrise Group of Institutions, Udaipur (Rajasthan), India

ABSTRACT
Cloud computing is a long awaited and now implemented dream of having interactive services and software applications, at reduced operational cost in the IT market, at highly automated and performance-based system, an on-demand services and these are just a few of the advantages that what cloud computing bring to us and what all features and services cloud computing provide us. It works on a Service Oriented Architecture (SOA) and delivers services as requested by the end users. Since cloud computing has a service oriented architecture, we rely on third party for our data and information are presented in the servers and data centers situated at different and hidden geographical locations all around the world. This reliance on third party shifts our attention to the security and standardization in cloud computing. The end users by no means, can determine data integrity and confidentiality of their data. Thus, our security protocol defines the standards to various cloud computing vendors and service providers, so that the problems such as data manipulation, data privacy and data consistency are minimized. This standardization will make data of end users more secure and safe and security areas may be resolved.

The paper proposes a security Model and also standards according to Monitor based security protocol for the security of the clouds vendors to efficiently store data on the clouds and to prevent data from threats.

Keywords
Utility Computing, End-to-End Quality of Service, Network Security, Internet Datacenters, Cloud computing.

1. INTRODUCTION
"Cloud" computing –is a very recent term, builds on decades of research orientation in virtualization, distributed computing, utility computing, and more recently with advance networking, web based technologies and software services. A next big leap in the Information Technology services and products; an evolution in the "Pay as You Go" or "On-Demand Services", will be addressed by Cloud Computing. Cloud computing relies to a large extent on the virtualization of the resources. The research in cloud computing is in the picture for some time now, by companies and in academia. The works from IBM [1], Amazon Elastic Compute Cloud [2], Hadoop [3], Globus [4], The Grid: Blueprint for a New Computing Infrastructure [5], Condor [6] have all contributed in the creation of cloud computing. Today various cloud computing providers exist and to highlight the big players, which offer the cloud services, are companies such as Amazon [7], Rackspace Cloud [8], Salesforce [9], Skytap [10], Microsoft [11] and Google [12].

The speed with which the clouds are forming and Multiplying strongly suggests that cloud computing will not only meet many of the needs of enterprise computing as we have come to know it, but also could form the digital platform for a shaping strategy guiding next generation enterprises in their migration to and participation in such ecosystems.

2. IMPORTANT AREAS OF CLOUD COMPUTING
Clouds do not have a complete definition in the literature and the web yet, which is an important task that will help to determine the areas of research and explore new application domains for the usage of the Clouds.

A number of definitions for cloud computing exists, but none of them can termed as an official standard definition. The cloud computing is termed as a paradigm that focuses on sharing data and computations over a scalable network of nodes. This organization of nodes is what we call a cloud, which could be a group of end user's computers, data centers, web servers etc. Let us head to the key concepts for understanding the fundamental of cloud computing:

2.1 Cyber infrastructure
For any business or major activity we rely in Information Technology services. Today companies are in use of various IT enabled services and products, which simplifies their work, resulting in a better productivity and throughput. A large number of firms uses IT services to ensure that their valuable amount of time is used in the research and novel implementation of their products and services. Thus, cyber infrastructure provides the means by which various applications and services are easy to develop and deploy in the global environment [13].

2.2 Service Oriented Architecture (SOA)
The SOA is not a recent term and a lot of work in development of this is taken place [14]. In a SOA scenario the end user requests for the particular service from an IT form, and on the return the IT firm facilitate the services during the time of request or at a later time. These services may include the various web based services, various software services or any other business related services that is meant for a desktop application.

2.3 Virtualization
Virtualization is an important concept in the cloud computing. It is an abstraction which hides the various lower layer

working, for example the various underlying hardware components that are required for the implementation of a task or functionalities. This results in sharing of various physical resources over the network and provides the feasibility to various functions of upper layers. Some of the examples of various virtualization products include: VMware, Xen – an open source product developed by XenSource, Microsoft Virtualization products [15].

In this way we can understand some of the important concepts in cloud computing. Now, as we have realized what cloud computing is all about, let us discusses the features and coin the pros and cons in using this, the so called highly anticipated research:

3. FEATURES OF CLOUD COMPUTING

- Cloud provides the resources which are on demand as there is isolation so no need to actual sharing.
- It is heterogeneous in nature.
- It adds the virtualization to the data and hardware resources too.
- It deals with end user security.
- Up-to-date Clouds are operated by single companies, but we envision federated Clouds facing similar problems as grids [16], [17].
- Clouds are easily usable hiding the deployment details from the user [18], [19].
- Cloud users are usually billed using a pay per-use model. More advanced payment models and SLA enforcement in a federated Cloud are just starting to be explored that will tear down one of the barriers to moving traditional applications to the Cloud: the loss of cost control [20].
- Clouds are also provides limited set of features exposed (i.e. they present a higher abstraction level to the user). For instance, the Simple Storage Service by Amazon can be regarded as a limited data Grid when compared to the CERN data Grid [21].

4. PROS AND CONS OF CLOUD COMPUTING

Pros of the cloud computing are:

- Very Highly Automated System.
- Reduced Cost: various other IT demands in a business firm are met because as we pay for the services we require.
- Mobility.
- Large Storage Capacity.

Various Cons and Limitations of the cloud computing are:

- Security?
- Reliance on the third party for our data?
- Availability?
- Migrating from current structure to the cloud is it optimal or feasible?

From the above points it is clear that cloud computing is a powerful concept, however we have to deal with the various problems it present in front of us. This paper focuses on the security issue of cloud computing. The security issue can be again divided in to two parts: First security concerns in the network when our data is transferred from one node to another that is an outside attacker can compromise our system. Second how can we be sure that our data is secured, as we have given our data to a third party?

Thus, this paper tries to find an optimal solution for the security parameter mainly to how we can feel safe, when we have given our important business data to a third party. A logical protocol is suggested and this paper then addresses a standard for various cloud computing providing vendors.

5. CLOUD COMPUTING PLAYERS IN INDIA

As a key player in the IT field, India is poised to be a Billion Dollar market in the next 5 years according to a study by an IT infrastructure firm. The study claims that this growth will be driven by the rapid increase in data such as text and media moving online. Some numbers shared in the study are quite interesting, it is expected that information stored online will reach a staggering 2.3 million petabytes (from 40,000 petabytes.)India's top IT firms, Infosys, TCS, Wipro and Tech Mahindra have cloud projects to their names. The competition is fierce as the market is nascent and big international names like Microsoft, IBM have dedicated resources as well. Support from the government to get basic infrastructure (cheaper and faster Internet) in place will go a long way in ensuring India's IT prominence [22]. The Cloud Computing players of India are shown in Table II. In year 2010 Microsoft and HP got into a strategic partnership to provide businesses with end-to-end cloud solutions. 2010 has also been dubbed as the "Year of the Cloud".

Table 1: Players of Cloud Computing in India

Company Name	Cloud Offering	Cloud Type	Location
Zenith Infotech	Proud	IaaS	Mumbai, India
Wolf Frameworks	Wolf PaaS	PaaS	Bangalore, India
OrangeSpace	OrangeSpace Cloud	PaaS	Chennai, India
TCS	ITaaS	IaaS+SaaS	India
Cynapse India	Cyn.in	IaaS+ On Demand SaaS	Mumbai, India
Wipro Technologies	Wipro w-SaaS	SaaS	India
Netmagic Solutions	CloudNet, CloudServe, Private Cloud	IaaS	Mumbai, India
Reliance Data Centre	Reliance Cloud Computing Services	IaaS+SaaS+PaaS	India
Infosys Technologies	Cloud Based Solution for Auto Sector	Saas	Bangalore, India
Synage	DeskAway	SaaS	Mumbai, India

6. RELATED AND PROPOSED WORK

The problem for cloud computing lies in the myth that cloud implementation is independent. However, in reality the cloud implementation is not independent and reliance on third party is even more dangerous for our data. There is a need for some transparency in between the cloud vendors and cloud users. Let us see the current works in the field of reliance of the information on the third party in case of the clouds, both public and private clouds.

Cloud service providers are making significant procedures and efforts to make their systems more secure; they are minimizing the threats on the internal cloud services and are trying to gain the customers trust. They are now substantially decreasing the number of staff members who have the access rights for the customers VM. They are providing high security measures and restricting the access on the numerous geographical facilities which consists of hardware implementation of the cloud. They are making various measures by which different, yet strong auditing protocols exists [23].

Terra [24] protocol tries to minimize the problem of interfering with the computations of the physical works on the process it also inspects with the problems for which it estimates whether the host can securely run the computation. This protocol works well within the single hosts and fails in case when computation is relied on various hosts.

SAS 70 [25] is another protocol which provides the guidelines for accessing the internal clouds. SOX [26] and HIPAA [27] are the regulations that work in congruent with the SAS 70 protocol.

Another area which requires focus is on the contracts by which the cloud vendors operate. They do not guarantee that the data with them is secure and asserts that cloud users cannot make any legal actions against them. Another concern is of the persistence of the data in the cloud vendors. How can we be sure that our data is been deleted when our work is finished with a particular vendor or in case of any shut down in the service. This transitive nature exists and could these contractors use various sub-contractors to perform their work can yield in new problems. Example of Nirvanix [28] and Carbonite [29], on these shut-downs caused loss of data for various cloud users.

The concern for Data Lock – in is another field which has come up in the recent cloud activity. How can we be sure that the cloud based services are not changing frequently by the cloud vendors [30]? The example from Coghead [31], when the services of them got shut down, it left various users to rewrite their application code. One solution to the Data Lock – in comes from the standard which is given by the GoGrid API [32].

7. PROPOSED SECURITY PROTOCOL

The concern for Data Lock – in is another field which has come up in the recent cloud activity. How can we be sure that the cloud based services are not changing frequently by the cloud vendors [30]? The example from Coghead [31], when the services of them got shut down, it left various users The companies which provide their business data to the various present cloud vendors in today's environment, whether maliciously or accidently illegal use and manipulation of data can severely damage the reputation of the company. After seeing the concerns in the area of security within the clouds, and to provide the cloud users a secure protocol by which we can ensure that the end users can feel confident in using both private and public clouds. The problems of data accessibility, data manipulation, data transparency all need to be addressed by a protocol, through which our reliance on third party is safe and secured. Obviously, when the data is under the privilege of a third party our concerns for the control and use of data is eminent. Hence, taking new approaches for ensuring security and reliability on various cloud vendors, this paper addresses the new concept of security by using the Monitor Based Security Protocol. The trusted cloud environment with new standards will surely minimize the problems of security in cloud computing paradigm.

7.1 Overview of Security Protocol for Cloud Computing Vendors

This approach is implemented with the help of special nodes called the "Monitors". These monitors are placed in between every cloud network end users and cloud vendors. These monitors will maintain a detail log of all the happening from both the cloud vendors and cloud users. These log files cannot be altered or manipulated nor by cloud vendors or cloud users, not even by any means. These log files are in the privileges of a special cloud standard committee. This committee should jointly work with the ISO standards and Legal Jurisdiction of the particular country specific government. By using monitors we can ensure that our data by no means can be illegally or maliciously used by the cloud vendor; as every point someone uses the particular cloud user's data the log based monitor initiates and maintains a log record for every transaction and usage.

7.2 Monitor Based Security Protocol

We assume that our entire cloud network is governed under the standard internet routing protocols. That is all the connection between the nodes from both the cloud vendors and cloud end users are interconnected by the internet. These special nodes can only have the "read only operations" for both the cloud vendors and cloud users. These information collecting nodes will monitor even the minimum detail of the activity in the cloud network, both by the cloud vendor or cloud user.

These monitors gather the information which is included in both the private as well as public clouds. These monitors are interconnected by a logical link which acts as a centralized server. This link is inter-connected to all the nodes of the users and the central administration of the cloud vendor. This centralized approach for both cloud vendor and cloud users will ensure that all the activities taking place between the cloud user and cloud vendor is under the privileges of the monitor. The monitor maintains its system log file which it constantly updates during any activity both from the cloud vendor and cloud user. The monitor creates the duplicate copy of the log file and keeps in the safe guard of the location where it is installed. This file can be retrieved by the authorizing agency (which is thought to be a joint venture between the ISO standard and the legal jurisdiction of the

particular government). The cloud monitors are in active state which holds the information based on the "time stamp", any activity that takes place is marked by the special reference number called the "SRN" and the official time stamp marked by the "OTS". This information is the means by which the agency that is monitoring or auditing the status of monitors within the specific cloud vendors and cloud users.

7.3 Working of Protocol

We make an assumption that all the nodes of the cloud are interconnected and are in working state; that is available for the usage of cloud services. Below we mention the working of the Monitor Based Security Protocol:

7.3.1 Assignment of Cloud Vendor Protocols

The monitor when initiated asks for the cloud vendor authentication number or special codes by which it successfully configures the cloud vendor provider and then configures the protocol stack implemented by the cloud vendor. This process assigns the logical link between the cloud vendor and cloud user and act as a centralized node. This monitor node now contains the centralized authority and waits for the cloud services to initiate.

7.3.2 Monitor Status Updating Routine for security protocol

The monitor now has the authority to monitor all the activities which it marks with the special dedicated log maintaining log messages the SRN and OTS. These messages are not working in constant time interval updating but on an efficient technique. This is triggered whenever the cloud user initiates the services and also triggers whenever the cloud vendor provides the services.

7.3.3 Monitor Log Entry for security Protocol

The cloud vendor's activity is constantly monitored as it is controlled by the authentic cloud service provider node and any activity within the frame of the particular data of a company that is using the monitor based security protocol. This activity, an internal activity within the cloud vendor is monitored and marked in the log based file held within the monitors and identified within the parameters of SRN and OTS.

7.3.4 Log File Auditing for security protocol

The monitored files are regularly been audited both by the cloud user and the agency which has the authority to take actions against the illegal activity of the particular user's data. These files are encoded for further security and other attacks from the agency providing the auditing facilities.

7.4 Standards defined for Security Protocol

Once the protocol is implemented we can write the standards for incorporating how the monitors will be used by both the cloud users and cloud vendors. The monitor implementation, which contains both the software and hardware parts should be made so that the Monitor Based Security Protocol is been implemented successfully. The standards for migrating current cloud structure within this protocol suite must be feasible. The agency which has the rights for which the end users trust must be of the highest of standards and should not hesitate to take any legal actions that are specified in the standards or laws for this protocol. Thus, these standards will ensure the services in the cloud computing paradigm to be successful and the use of technology will be for the good means.

By using the above standards and implementations we can broadly assure the Quality of Service (QoS) which the cloud user's expect from the cloud vendors and above all from the cloud paradigm. These standards will result in the better and secure environment for both private and public clouds.

8. CONCLUSION

This paper presents a monitor based security protocol for cloud Computing vendors, which ensures that, we can now to a large scale reduce the threat of our data from the various third party vendors. The clouds working in this procedure (using security protocol) will better result in the security demands with very few overheads as compared with the value of the business data on the cloud vendors. The proposed work provided in the paper would prove better, when the actual implementation of this protocol takes place. We still by no means can determine how effectively this security protocol works in the real time environment or can handle real time situations as the practical implementation is still a unreviewed benchmark. To a great extent the security problem would be controlled for the threats prevailing now on the clouds. But security problem in the cloud computing is still in a dubious condition as every day new security problem arises and is still an open question.

9. REFERENCES

[1] IBM, "North Carolina State University and IBM help bridge digital divide in North Carolina and beyond," May 7, 2007, http://www03.ibm.com/industries/education/doc/content/news/pressrelease/2494970110.html (Accessed on 10 Jan 2011).

[2] Amazon Elastic Compute Cloud (EC2): http://aws.amazon.com/ec2/ (Accessed on 10 Jan 2011).

[3] Hadoop: http://hadoop.apache.org/ (Accessed on 10 Jan 2011).

[4] Globus: http://www.globus.org/ (Accessed on 10 Jan 2011).

[5] The Grid: Blueprint for a New Computing Infrastructure, 2nd Edition, Morgan Kaufmann, 2004. ISBN: 1-55860-933-4.

[6] Condor: http://www.cs.wisc.edu/condor/ (Accessed on 10 Jan 2011).

[7] Amazon Elastic Compute Cloud (EC2): http://aws.amazon.com/ec2/ (Accessed on 10 Jan 2011).

[8] Rackspace Cloud: http://www.rackspacecloud.com (Accessed on 10 Jan 2011).

[9] Salesforce: www.salesforce.com (Accessed on 10 Jan 2011).

[10] Skytap: http://www.skytap.com (Accessed on 10 Jan 2011).

[11] Azure: http://www.microsoft.com/windowsazure/ - (Accessed on 10 Jan 2011).

[12] Google: http://code.google.com/appengine/ - (Accessed on 12 Mar 2011).

[13] .A. Vouk, "Virtualization of Information Technology Resources, in *Electronic Commerce: A Managerial Perspective 2008*, 5th Edition y Turban, and Prentice-Hall Business Publishing, to appear.

[14] The Grid: Blueprint for a New Computing Infrastructure, 2nd Edition, Morgan Kaufmann, 2004. ISBN: 1-55860-933-4.

[15] Microsoft Virtualization products: http://www.microsoft.com/virtualization/default.mspx - (Accessed on 12 Mar 2011).

[16] E. Hand. Head in the clouds. Nature, (449):963, Oct 2007.

[17] A break in the clouds: towards a cloud definition. Vaquero, Rodero-Merino, Caceres, Lindner. 2008.

[18] Gartner Says Cloud Computing Will Be As Influential As E-business. Gartner.com. http://www.gartner.com/it/page.jsp?id=707508. Retrieved 2010-08-22.

[19] Gruman, Galen What cloud computing really means. *InfoWorld*. http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031. Retrieved 2009-06-02.

[20] Cloud Computing: Clash of the clouds. The Economist. http://www.economist.com/displaystory.cfm?story_id=14637206. Retrieved 2009-11-03.

[21] NIST.gov - Computer Security Division - Computer Security Resource Center". Csrc.nist.gov.

[22] http://www.zdnet.com/blog/india/cloud-computings-latest-battlefield-india/179. Retrieved 2011-03-20.

[23] T. R. Peltier, J. Peltier, and J. Blackley. *Information Security Fundamentals*. Auerbach Publications, Boston, MA, USA, 2003.

[24] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh. Terra: A Virtual Machine-Based Platform for Trusted Computing. In *Proc. of SOSP'03*, 2003.

[25] SAS 70: http://sas70.com/sas70_overview.html - accessed Jan 2011.

[26] SOX (Sarbanes–Oxley Act of 2002): http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/content-detail.html - accessed Jan 2011.

[27] HIPAA - http://www.hipaa.org/ - Accessed 22 Mar 2011.

[28] Loss of customer data spurs closure of online storage service 'The Linkup'. http://www.networkworld.com/news/2008/081108-linkup-failure.html?page=1 – accessed Jan 2011.

[29] Latest cloud storage hiccups prompts data security questions. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9130682&source=NLT_PM – accessed Jan 2011.

[30] Cloud computing: Don't get caught without an exit strategy. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9128665&source=NLT_AM – accessed Jan 2011.

[31] Cloud Bursts as Coghead Calls It Quits. http://blogs.zdnet.com/collaboration/?p=349 – accessed Jan 2011.

[32] GoGrid API, http://www.gogrid.com/cloud-hosting/cloud-api.php – accessed Jan 2011.