Efficient Cloud Seeding On Cloud Storage Using Virtualization

E.Ravi kondal, 1, K.NIKITHA, 2,B.Mounika3,B.K.N.Priyanka4
COMPUTER SCIENCE & ENGINEERING Dept.
NOBLE COLLEGE OF ENGG &TECH FOR WOMEN, TG, HYD
easala_ravi@yahoo.com,nikitha.kakkula@gmail.com,mounika2241994@gmail.com,priyankasowji169@gmail.com

Abstract: In cloud computing files distribution and storage are handled by the cloud providers or physical storage devices provided by the third parties. The data which stored in the cloud is object based, we propose the index based cloud seeding (IBCS) on storage devices using Virtualization, and also balancing the workload on the server. To manage and optimize the client-server transmission status of the cloud seeding for optimal performance and offer suitable resources.

Index Terms: - cloud storage, cloud seeding, load balancing, Index based cloud seeding (IBCS).

……..

Introduction:

Cloud computing is a rapidly developing Information Technology and it rules the whole world. Cloud computing is not a totally new concept it is a new computing model. It will be a supervision technology and cloud computing is the third revolution in the IT industry. The core concept of cloud computing is reducing the processing burden on the users, constantly improves the handling ability of the cloud. The data in a storage environment are usually stored by the cloud providers automatically. In generally speaking the commonly seen storage protocols are NAS and SAN [1][5]. Due to the number of users the devices in the cloud network increase of the complexity of controlling the hardware and the network traffic are increasing, and the performance of the cloud network decrease .The cloud seeding of storage devices can increase the efficient accessing of the data from the users.

Cloud Definition:"CLOUD" is a virtualized pool of computing resources like PC, Desktop, Tablets, Ubiquitous devices [1][5] are connected through a network. The "cloud" itself is a network.

According to NIST[1][5] definition is that cloud computing is a model that early acquire on-demand access to a configurable computing resources, such as network servers, storage devices, applications and services of the public collection, these resources minimizing management costs.

Cloud model is composed of five Basic characteristics, three service models and four release models; to parse the cloud models of NIST's[1][5] definition we should know the basic characteristics.

Cloud Five Basic characteristics [2] are, as follows as shown in fig.1

On-demand self services: computer services such as email applications, network or server service can be provided without requiring human interaction with each revise provider. Cloud service providers providing on demand self services include Amazon Web Services (AWS), Microsoft, Google, IBM and Salesforce.com. New York Times and NASDAQ are examples of companies using AWS (NIST) [1] [5]. Gartner describes this characteristic as service based

Broad network access: Cloud Capabilities are available over the network and accessed Through standard mechanisms that promote use by heterogeneous thin or thick client platforms such as mobile phones, laptops and PDAs

Resource pooling: The provider's computing resources are pooled together to serve multiple consumers using multiple-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The resources include among other storage, processing, memory, network bandwidth, virtual machines and email services. The pooling together of the resource builds economies of scale.

Rapid elasticity: Cloud services can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. For the Consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured service: Cloud computing resource usage can be measured, controlled, and reported providing transparency for both the provider and consumer of the utilized service. Cloud computing services use a metering capability which enables to control and optimize resource use. This implies that just like air time, electricity or municipality water IT services are charged per usage metrics – **pay per use**. The more you utilize the higher the bill. Just as utility companies sell power to subscribers, and telephone companies sell voice and data services, IT services such as network security management, data center hosting or even departmental billing can now be easily delivered as a contractual service.

Multi Tenacity: Multi Tenacity is the 6th characteristics of cloud computing advocated by the Cloud Security Alliance. It refers to the need for policy-driven enforcement, segmentation, Isolation, governance, service levels, and chargeback/ billing models for different Consumer constituencies. Consumers might utilize a public cloud provider's service Offerings or actually be from the same organization, such as different business units rather than distinct organizational entities, but would still share infrastructure.

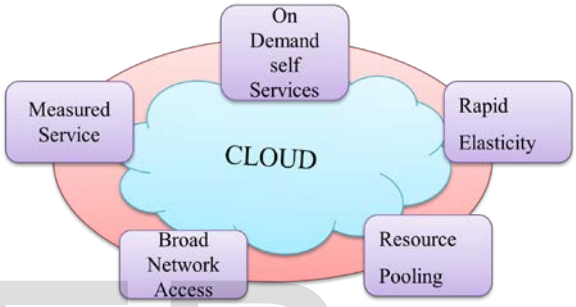


Fig.1

Cloud computing has been a paradigm shift in the IT. Third party providers are providing storage, software and Infrastructure resources to their customers through services. Cloud computing is providing different types of services among them the best Three services are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-Service (IaaS) [2][5] as shown in fig.2

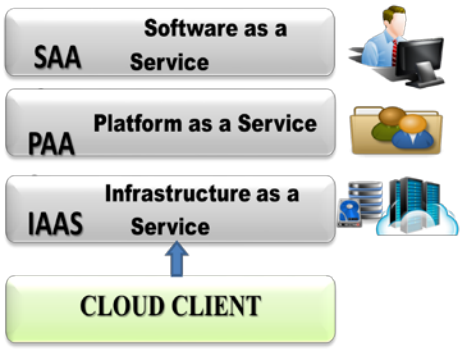


Fig.2

Software as a service (SaaS)

In the business model using software as a service (SaaS) [2], users are provided access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. SaaS is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis. SaaS providers generally price applications using a subscription fee.

In the SaaS [5] model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. Cloud users do not manage the cloud infrastructure and platform where the application runs. This eliminates the need to install and run the application on the cloud users' own computers, which simplifies maintenance and support. Cloud applications are different from other applications in their scalable which can be achieved by cloning tasks onto multiple virtual machines at run-time to meet changing work demand.

Load balancers [6] distribute the work over the set of virtual machines. This process is transparent to the cloud user, who sees only a single access point. To accommodate a large number of cloud users, cloud applications can be multitenant, that is, any machine serves more than one cloud user organization. It is common to refer to special types of cloud-based application software with a similar naming convention: desktop as a service, business process as a service, test environment as a service, communication as a service.

Platform as a service (PaaS)

In the PaaS[2] models, cloud providers deliver a computing platform, typically including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers.

With some PaaS offers like Microsoft Azure and Google App Engine, the underlying computer and storage resources scale automatically to match application demand so that the cloud user does not have to allocate resources manually. The latter has also been proposed by an architecture aiming to facilitate real-time in cloud environments.

Infrastructure as a service (IaaS)

In the most basic cloud-service model, providers of IaaS [2][5] offer computers physical or (more often) virtual machines and other resources. (A hypervisor, such as Xen, Oracle Virtual Box, KVM, VMware ESX/ESXi, or Hyper-V runs the virtual machines as guests. Pools of hypervisors within the cloud operational support-system can support large numbers of virtual machines and the ability to scale services up and down according to customers' varying requirements.)

IaaS clouds often offer additional resources such as a virtual-machine disk image library, raw block storage, and file or object storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles. IaaS cloud providers supply these resources on-demand from their large pools installed in data centers. For wide-area connectivity, customers can use either the Internet or carrier clouds (dedicated virtual private networks). Recently, this paradigm has been extended towards sensing and actuation resources, aiming at providing virtual sensors and actuators as services SaaS [2].

To deploy their applications, cloud users install operating-system images and their

application software on the cloud infrastructure. In this model, the cloud user patches and maintains the operating systems and the application software. Cloud providers typically bill IaaS services on a utility computing basis cost reflect the amount of resources allocated and consumed.

Deployment Models in Cloud Computing

Cloud services can be deployed in different ways, depending on the organizational structure and the provisioning location. Four deployment models [3] are usually distinguished, namely public, private, community and hybrid cloud service usage.

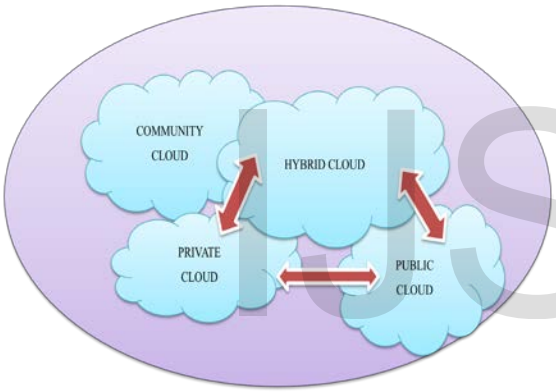


Fig.3a

Public Cloud

The deployment of a public cloud computing system is characterized on the one hand by the public availability of the cloud service offering and on the other hand by the public network that is used to communicate with the cloud service. The cloud services and cloud resources are procured from very large resource pools that are shared by all end users. These IT factories, which tend to be specifically built for running cloud computing systems, provision the resources precisely according to required quantities. By optimizing operation, support, and maintenance, the cloud provider can achieve significant economies of scale, leading to low prices for cloud resources. In addition, public cloud portfolios employ techniques for resource optimization as shown in ,fig.3,3a; however, these are transparent for end users and represent a potential threat to the security of the system. If a cloud provider runs several data centers, for instance, resources can be assigned in such a way that the load is uniformly distributed between all centers.

Some of the best-known examples of public cloud systems are Amazon Web Services (AWS) containing the Elastic Compute Cloud (EC2) and the Simple Storage Service (S3) which form an IaaS cloud offering and the Google App Engine with provides a PaaS [3] to its customers. The customer relationship management (CRM) solution Salesforce.com is the best-known example in the area of SaaS cloud offerings.

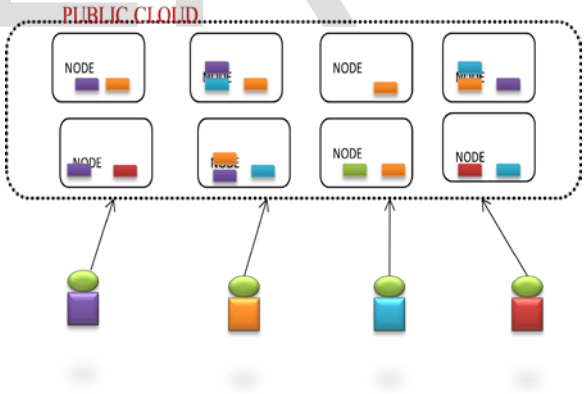


Fig.3

Private Cloud

Private cloud computing fig.3a [3] systems emulate public cloud service offerings within an organization's boundary to make services accessible for one designated organization. Private cloud computing systems make use of

Virtualization solutions and focus on consolidating distributed IT services often within data centers belonging to the company. The chief advantage of these systems is that the enterprise retains full control over corporate data, security guidelines, and system performance. In contrast, private cloud offerings are usually not as large-scale as public cloud offerings resulting in worse economies of scale, as shown in fig.4

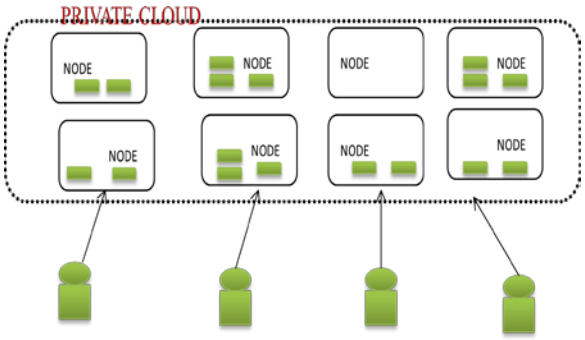


Fig.4

Community Cloud

In a community cloud [8], organizations fig.3a,fig.5 with similar requirements shares a cloud infrastructure. It may be understood as a generalization of a private cloud, a private cloud being an infrastructure which is only accessible by one certain organization.

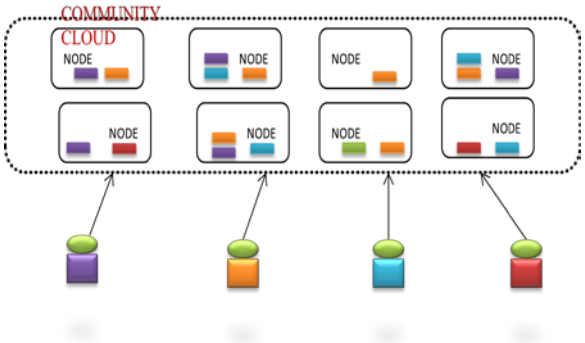
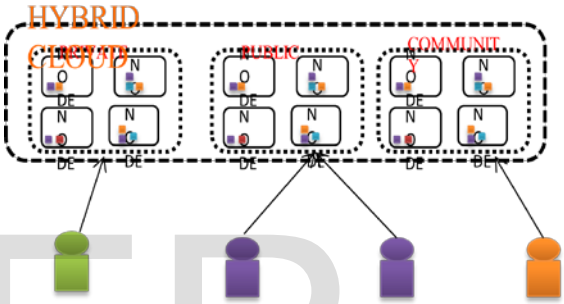


Fig.5

Hybrid Cloud:

A hybrid cloud service [8] deployment model implements the required processes by combining the cloud services of different cloud computing systems, e.g. fig.3a, fig.6 private and public cloud services. The hybrid model is also suitable for enterprises in which the transition to full outsourcing has already been completed, for instance, to combine community cloud services with public cloud services.

Fig.6



Virtualization:

Virtualization, in computing, refers to the act of creating a virtual (rather than actual) version of something, including but not limited to a virtual computer hardware platform, operating system (OS), storage device, or computer network resources. The term "Virtualization" traces its roots to 1960s mainframes, during which it was a method of logically dividing the mainframes' resources for different applications fig.7.

Hardware virtualization

Hardware Virtualization or platform Virtualization refers to the creation of a virtual machine [10] that acts like a real computer with an operating system. Software executed on these

virtual machines is separated from the underlying hardware resources. For example, a computer that is running Microsoft Windows may host a virtual machine that looks like a computer with the Ubuntu Linux operating system; Ubuntu-based software can be run on the virtual machine

In hardware virtualization [7], the host machine is the actual machine on which the virtualization takes place, and the guest machine is the virtual machine. The words host and guest are used to distinguish the software that runs on the physical machine from the software that runs on the virtual machine. The software or firmware that creates a virtual machine on the host hardware is called a hypervisor or Virtual Machine Manager.

Different types of hardware virtualization include:

1. Full Virtualization: Almost complete simulation of the actual hardware to allow software, which typically consists of a guest operating system, to run unmodified.
2. Partial Virtualization: Some but not all of the target environment is simulated. Some guest programs, therefore, may need modifications to run in this virtual environment.
3. Para Virtualization: A hardware environment is not simulated; however, the guest programs are executed in their own isolated domains, as if they are running on a separate system. Guest program needs to be specifically modified to run in this environment.

Hardware-assisted Virtualization [10] is a way of improving the efficiency of hardware Virtualization. It involves employing specially designed CPUs and hardware components that help improve the performance of a guest environment.

Hardware Virtualization can be viewed as part of an overall trend in enterprise IT that includes autonomic computing, a scenario in which the IT environment will be able to manage itself based on perceived activity, and utility computing, in which computer processing power is seen as a utility that clients can pay for only as needed. The usual goal of Virtualization is to centralize administrative tasks while improving scalability and overall hardware-resource utilization. With Virtualization, several operating systems can be run in parallel on a single central processing unit (CPU).

This parallelism tends to reduce overhead costs and differs from multitasking, which involves running several programs on the same OS. Using Virtualization, an enterprise can better manage updates and rapid changes to the operating system and applications without disrupting the user. "Ultimately, Virtualization dramatically improves the efficiency and availability of resources and applications in an organization. Instead of relying on the old model of “one server, one application” that leads to underutilized resources, virtual resources are dynamically applied to meet business needs without any excess fat"

Desktop virtualization

Desktop Virtualization is the concept of separating the logical desktop from the physical machine as shown in fig.7

One form of desktop Virtualization, virtual desktop infrastructure (VDI), can be thought as a more advanced form of hardware Virtualization. Rather than interacting with a host computer directly via a keyboard, mouse, and monitor, the user interacts with the host computer using another desktop computer or a mobile device by means of a network connection, such as a LAN, Wireless LAN or even the Internet. In addition, the host computer in this scenario

becomes a server computer capable of hosting multiple virtual machines at the same time for multiple users.

Another form, session Virtualization, allows multiple users to connect and log into a shared but powerful computer over the network and use it simultaneously. Each is given a desktop and a personal folder in which they store their files. With Multi seat configuration, session Virtualization can be accomplished using a single PC with multiple monitors keyboards and mice connected.

Moving Virtualized desktops into the cloud creates hosted virtual desktops (HVD), where the desktop images are centrally managed and maintained by a specialist hosting firm. Benefits include scalability and the reduction of capital expenditure, which is replaced by a monthly operational cost.

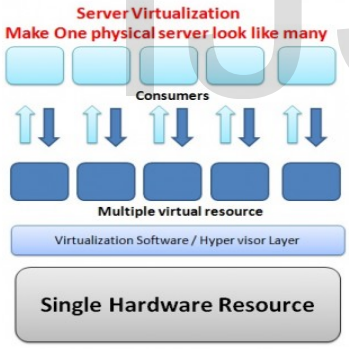


Fig.7

Cloud computing and seeding:

Access control is generally a policy or procedure that allows, denies or restricts access to a system. It may, as well, monitor and record all attempts made to access a system. Access Control may also identify users attempting to access a system unauthorized. It is a mechanism which is very much important for protection in computer security [7]. Various access control models are in use, including the most common Mandatory Access Control [13] (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC) [4]. All these models are known as identity based cloud seeding (IBCS) control models. In all these access control models, user (subjects) and resources (objects) are identified by unique names. Identification may be done directly or through roles assigned to the subjects. These IBCS access control methods are effective in the Unchangeable distributed system, where there is only a set of Users with a known set of services.

Nowadays, very large distributed open systems are developing very rapidly. These include Grid Computing and Cloud Computing. These systems are like virtual organizations with various autonomous domains. The relationship between users and resources is dynamic and more ad-hoc in cloud and inter cloud systems. In these systems, users and resource providers are not in the same security domain [6]. Users are normally identified by their attributes or characteristics and not by predefined identities. In such cases, the traditional identity based access control models are not very much effective and therefore, access to the system must be done on decisions based on certain attributes. In addition, in the cloud system, autonomous Domains have a separate set of security policies. Hence, the access control Mechanism must be flexible to support various kinds of domains and policies. With the development of large distributed systems attributes based access control (ABAC) has become increasingly important.

SEEDIND CONTROL METHODS

The way a system provides security to its resources and data, is by controlling access [13] to the resources and the system itself. However, access control is more than just controlling which users (subjects) can access which computing and network resources. In addition, IBCS access control manages users, files and other resources. It

controls the user's privileges to files or resources (objects). In access control systems various steps like, identification, authentication, authorization and accountability are taken before actually accessing the resources or the object in general.

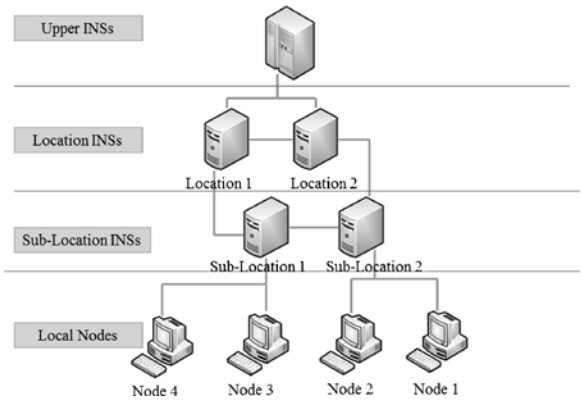


Fig.8

In the early stages of computing and information technology, researchers and technologists realized the importance of preventing users from interfering each other on shared systems in fig 8. Various access control models [6] were developed. User's identity was the main index to allow users to use the system or its resources. This approach was called Identification Based Access Control (IBAC) [6]. However, with the growth of the networks and the number of users, IBAC was found to be weak to defend such a large growth. Advanced concepts in access control were introduced which included owner/ group/ public. IBAC proved to be problematic for distributed systems as well.

Cloud Manage [CM]: Cloud Manager has also have same function File Splitting Function [FSM], Create Metadata [CMM] [23] function and Search function [SFM] [16] and have same working. The Cloud manager can assign a cloud even without using these functions. Cloud Interface [CLI] act as a communicator between Cloud managers and different cloud

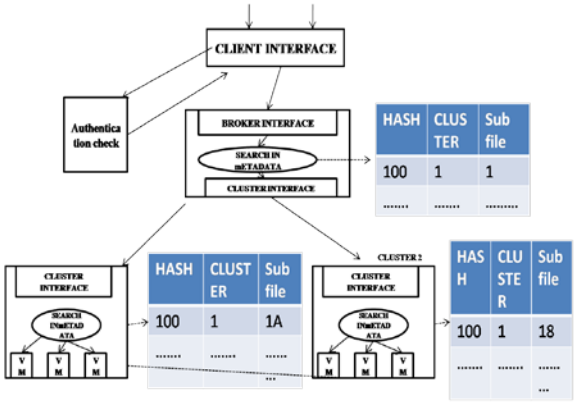


Fig.9

Data Retrieval from Cloud:

The metadata [8] is created at the CM level then when any request come it will search on which CL, the Fi is stored. The CL having the Fi, response to the CM and again all intra-cloud search operation is performed and required virtual machines are found and mount. Now the splitting of files can be done in various ways.

So this model can operate on inter-cloud operation or intra cloud operation. As whole data is not in single cloud it will increase security, reliability to some extents [14]. The division of file into multiple sub files can also be done by fixing the minimum size of sub files so a small file would not be broken into two smaller sub files which unnecessarily increase the processing. One another aspect is also to introduce the security attribute which refer to the importance of security required for particular files. If this attribute is NULL means files is not so important and no need to break the file. If the attribute value is 50% then broke it into half of the maximum no. of possible sub files according to attribute value divide the file into sub file.

Managing access to the system and resources became hard and vulnerable to errors. A new method known as Role Based Access Control (RBAC) [4] was introduced. Role based Access

Control (RBAC) determines user's access to the system based on the Job role. The role a user is assigned to be basically based on the least privilege concept . The role is defined with the least amount of permissions or functionalities that is necessary for the job to be done. Permissions can be added or deleted if the privileges for a role change. However, problems became apparent when RBAC was extended across administrative domains. And, it proved difficult to reach an agreement on what privileges associate with a role. Accordingly, a policy based access control known as Attribute Based

Access Control (ABAC) [15] came into existence in fig.9. In ABAC, access is granted on attributes that the user could prove to have such as date of birth or national number. However, reaching to an agreement on a set of attributes is very hard, especially across multiple agencies [12] or domains and organizations. All access control methods rely on authentication of the user on the site, as well as, at the time of request. Sometimes they are labeled as authentication based access control. In all these methods, tight coupling [11] among domains is required. This is done to merge identities or define the meaning of attributes or roles. Furthermore, all these approaches make it difficult to assign subsets of privileges of an administrator.

ABAC Characteristics

- Hierarchical policy structure based on the concept of abstraction and encapsulation
- Policy set is composed of various policies that need to be supported
- Police have their own decision and decision making algorithms
- Does not use a unified method to describe each policy
- Effective supports of multiple policies
- Model is more flexible and scalable

CONCLUSIONS

In this paper we propose the efficient access of the data from the cloud storage, the complexity of access of the data with Identity based access control increases the efficiency of data in cloud seeding from cloud storage. The role is defined with the least amount of permissions or functionalities that is necessary for the job to be done.

REFERENCES:

[1]. P. Mell and T.Grance, "Draft NIST working definition of cloud computingv15," 21.Aug2009, 2009.

[2]. Y.-M. Huo, H.-Y. Wang, L.-A. Hu, and H.-G.Yang, "A cloud storage architecture model for data-intensive applications," in Proc. Int. Conf.Comput. Manage., May 2011, pp. 1–4.

[3] L. B. Costa and M. Ripeanu, "Towards automating the configuration of a distributed storage system," in Proc. 11th IEEE/ACM Int. Conf. Grid Compute Oct. 2010, pp. 201–208.

[4] G. Ahn and H. Hu, "Towards Realizing a Formal RBAC Model in Real Systems," Proc. 12th ACM Symp. Access Control Models and Technologies, pp. 215-224, 2007.

[5] P. Mell and T.Grance, "Draft NIST working definition of cloud computingv15," 21.Aug2009, 2009.

[6] S. Pearson, Y. Shen, and M. Mowbray. "A privacy manager for cloud computing". In The First International Conference on Cloud Computing, pages 90–106, 2009.

[7] L. Kaufman. "Data security in the world of cloud computing". IEEE SECURITY & PRIVACY, 7(4), July-August 2009.
[8] S. Creese, P. Hopkins, S. Pearson, and Y. Shen. "Data protection-aware design for cloud services". In The First International Conference on Cloud Computing, pages 119–130, 2009.
[9] Access control in a cloud computing environment ARPN Journal of Engineering and Applied Sciences
[10] L. Kaufman. "Data security in the world of cloud computing". IEEE SECURITY & PRIVACY, 7(4), July-August 2009.
[11] S. Creese, P. Hopkins, S. Pearson, and Y. Shen. "Data protection-aware design for cloud services". In The First International Conference on Cloud Computing, pages 119–130, 2009.
[12] L. Hu, S. Ying, X. Jia, and K. Zhao. "Towards an approach of semantic access control for cloud computing". In The First International Conference on
Cloud Computing, pages 145–156, 2009.
[13] D. Chen, X. Huang, and X. Ren. "Access control of cloud service based on acron ". of The First International Conference on Cloud Computing, pages 559–564, 2009.
[14] T. Uemura, T. Dohi, and N. Kaio. "Availability analysis of a scalable intrusion tolerant architecture with two detection modes". In The First International Conference on Cloud Computing, pages 178–189, 2009.
[15] L. M. Vaquero, L. Rodero-Merino, J. Caceres and M. Lindner, "A break in the clouds: towards a cloud definition," SIGCOMM Comput. Commune. Rev. 39, 1, pp. 50-55, Dec. 2008.