Research Article Impact Factor: 0.621 ISSN: 2319-507X
SY Gawali, IJPRET, 2014; Volume 2 (8): 827-841 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SECURITY MANAGEMENT AND FUTURE CLOUD DATA CENTER IN CLOUD COMPUTING

PROF. S. Y. GAWALI[1], MISS DIPTI V. JILHARE[2]

1. Assistance Professor, Dept. of CSE, Babasaheb Naik college Of Engg., Pusad (India)
2. M. E. Student, Dept. of CSE, Babasaheb Naik college Of Engg., Pusad (India)

Accepted Date: 15/02/2014 ; Published Date: 01/04/2014

Abstract: This Paper discusses in first section There is a risk of data theft from machines in the cloud, by rogue employees of cloud service providers or by data thieves breaking into service providers' machines. Our contribution to addressing these problems is a Privacy Manager, which helps the user manage the privacy of their data in the cloud. As a first line of defence, the privacy manager uses a feature called obfuscation, First section of this paper provide solution for this insecurity is privacy manager for cloud computing, which reduces the risk Encryption prevents unwanted individuals from being able to access, tamper with or vindictively change files to cause harm to you personally or to your business. Also This Paper discusses the current complexity challenges facing large-scale data centers and how the Internet, Web, and especially Web services are not only creating those challenges, but also offering the solution to those challenges during the next 5-10 years. The central focus of second section is to describe the evolution of the data center of the future (DCFuture), the forces driving that evolution, and its impact on products and markets.

Keywords: Cloud computing, Data center, Virtualization Commoditization Innovation, integration, privacy manager, obfuscation**.**

PAPER-QR CODE

Corresponding Author: PROF. S. Y. GAWALI

Access Online On:

www.ijpret.com

How to Cite This Article:

SY Gawali, IJPRET, 2014; Volume 2 (8): 827-841

INTRODUCTION

Cloud computing is a disruptive technology with profound implications not only for Internet services but also for the IT sector as a whole. The cloud is the internet where files are uploaded to and downloaded from.A data center may be concerned with just operations architecture or it may provide other services as well.The main purpose of a data center is running the applications that handle the core business and operational data of the organization.Data centers are also used for off site backups. Companies may subscribe to backup services provided by a data center. This is often used in conjunction with backup tapes . Cipher Cloud eliminates the inherent security and privacy risks of cloud computing. Your business never loses control of its sensitive data, yet you can achieve the full benefits of cloud computing. TPM (Trusted Platform Module) is a computer chip that can securely store artifacts used to authenticate the platform (your PC or laptop). Trusted Gateway takes a revolutionary approach to protecting sensitive data before it leaves an organization's secure enterprise network. Second section of this paper provide solution for this insecurity is privacy manager for cloud computing, which reduces the risk. the privacy manager uses a feature called obfuscation, The obfuscation method uses a key which is chosen by the user and known by the privacy manager, but which is not communicated to the service provider. Thus the service provider is not able to de-obfuscate the user's data, during the next five years, the DCFuture will contain ever larger numbers of ever smaller components offered by diverse vendors, but based on common standards. Although the complexity of the basic building blocks will decrease, the complexity of integrating them into services and solutions the Internet, Web, and especially Web services are not only creating those challenges, but also offering the solution to those challenges during the next 5-10 years. The central focus of this Paper is to describe the evolution of the data center of the future (DCFuture), the forces driving that evolution, and its impact on produce Four fundamental economic forces have shaped the data center up until now and will continue to

• **Commoditization:**: The standardization and specialization of function, with the progressive shift in focus toward quality, complementary products and services, and price.

• **Virtualization:** The systems are composed of increasing numbers of functionally identical subsystems of decreasing size and complexity to increase utilization.

• **Integration**: The network-centric is interconnection of the systems is far greater the data center becomes the network.

• **Innovation**: The rate of change of the integrated systems and their interconnections is accelerating from network topology changes, to software configuration changes, to application integration changes and markets.

II.TYPES OF CLOD IN CLOUD COMPITING

A. PRIVATE CLOUD

A private cloud is a particular model of cloud computing that involves a distinct and secure cloud based environment in which only the specified client can operate. As with other cloud models, private clouds will provide computing power as a service within a virtualized environment using an underlying pool of physical computing resource. However, under the private cloud model, the cloud (the pool of resource) is only accessible by a single organization providing that organization with greater control and privacy.

A. PUBLIC CLOUD

A cloud is called a "public cloud" when the services are rendered over a network that is open for public use. Made available by a service provider for a public audience and when communication is effected over a non-trusted network. Generally, public cloud service providers like Amazon AWS, Microsoft and Google own and operate the infrastructure and offer access only via Internet.

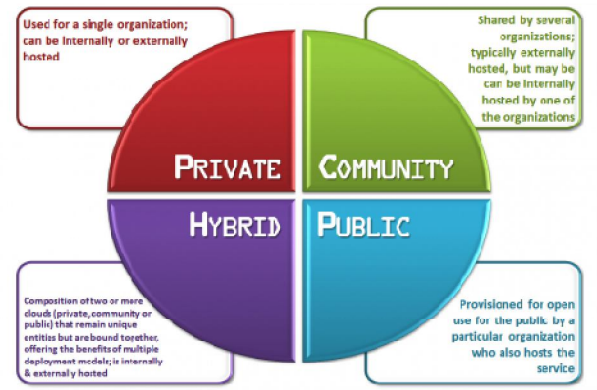

fig 1: **types of cloud**

C. HYBRID CLOUD

Hybrid cloud can also mean the ability to connect allocation, managed and/or dedicated services with cloud resources. It allows one to extend either the capacity or the capability of a cloud service, by aggregation, integration or customization with another cloud service.

D. COMMUNITY CLOUD

community cloud is a is a multi-tenant cloud service model that is shared among several or organizations and that is governed, managed and secured commonly by all the participating organizations or a third party managed service provider. Community clouds are a hybrid form of private clouds built and operated specifically for a targeted group.

III. CLOUD MANAGEMENT STRATEGIES

Public clouds are managed by public cloud service providers, which include the public cloud environment's servers, storage, networking and data center operations. Users of public cloud services can generally select from three basic categories:

User self-provisioning: Customers purchase cloud services directly from the provider, typically through a web form or console interface. The customer pays on a per-transaction basis.

Advance provisioning: Customers contract in advance a predetermined amount of resources, which are prepared in advance of service. The customer pays a flat fee or a monthly fee.

Dynamic provisioning: The provider allocates resources when the customer needs them, then decommissions them when they are no longer needed. The customer is charged on a pay-per-use basis.

Managing a private cloud requires software tools to help create a virtualized pool of compute resources, provide a self-service portal for end users and handle security, resource allocation, tracking and billing. Management tools for private clouds tend to be service driven, as opposed to resource driven, because cloud environments are typically highly virtualized and organized in terms of portable workloads. Estimates vary widely on possible cost savings •"If you move your data center to a cloud provider, it will cost a tenth of the cost."Use of cloud applications can reduce costs from 50% to 90% " .In hybrid cloud environments, compute, network and storage resources must be managed across multiple domains, so a good management strategy should start by defining what needs to be managed, and where and how to do it. Policies to help govern these domains should include configuration and installation of images, access control, and budgeting and reporting. Access control often includes the use of Single sign-on (SSO), in

which a user logs in once and gains access to all systems without being prompted to log in again at each of them.

IV.CLOUD SECURITY

Public and private cloud services, also known as multi-tenant infrastructure, are used increasingly in the enterprise and by government agencies. With their popularity come security issues that are now high priority. A number of technologies and standards, including the Trusted Platform Module (TPM), network security, and self-encrypting drives can be used to provide security for systems, networks, and data.TPM (Trusted Platform Module) is a computer chip (microcontroller) that can securely store artifacts used to authenticate the platform (your PC or laptop). These artifacts can include passwords, certificates, or encryption keys. A TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy. TPM maintains thrice of all (CIA) properties:

Confidentiality: The nature of hardware-based cryptography ensures that the information stored in hardware is better protected from external software attacks.

Authentication: It also acts as a secure vault for certificates, keys and passwords, negating the need for costly tokens.

Platform Integrity: Measures and reports on the integrity of platform, including the BIOS, disk MBR, boot sector, operating system and application software, to ensure no unauthorized changes have occurred. The TPM, a secure cryptographic integrated circuit (IC), provides a hardware-based approach to manage user authentication, network access, data protection and more that takes security to higher level than software-based security[1].

V. PRIVACY MANAGER

Privacy manager for cloud computing, which reduces the risk to the cloud computing user of their private data being stolen or misused, and also assists the cloud computing provider to conform to privacy law. There is a risk of data theft from machines in the cloud, by rogue employees of cloud service providers or by data thieves breaking into service providers' machines, or even by other customers of the same service if there is inadequate separation of different customers' data in a machine that they share in the cloud. Privacy Manager, which helps the user manage the privacy of their data in the cloud. As a first line of defence, the privacy manager uses a feature called *obfuscation*, where this is possible. The idea is that instead of being present unencrypted in the cloud. The user's private data is sent to the cloud in

an encrypted form, and the processing is done on the encrypted data. The result of the processing is de-obfuscated by the privacy manager to reveal the correct result.

VI. OBFUSCATION

In this paper is only that it is difficult for the service provider to determine *x* given the obfuscated data. It may be that the service provider can easily obtain some information about *x*, but not enough to determine *x*. As a different example of obfuscation methods that allow some but not all information about the input data to be learned from the obfuscated data, Narayanan and Shmatikov describe an obfuscation method which allows individual records to be retrieved from an obfuscated database by anyone who can specify them precisely, while making "mass harvesting" queries matching a large number of records computationally infeasible. As remarked in , there is a tension between the strict security definitions and loose notions of efficiency used by the cryptography community, and the strict efficiency requirements but loose security requirements of the database community. Like the database community we prioritize efficiency over strength of the security definition, as it is essential for us that the privacy manager be practical and scalable to implement.

VII. FUTURE TRUSTED CLOUD STORAGE ARCHITECTURE

Cloud data storage under the aforementioned model, our protocol design should achieve the following security and performance guarantee:

A) **Public auditability**: To allow TPA to verify the correctness of the cloud data on demand without retrieving

a copy of the whole data or introducing additional on-line burden to the cloud users;

B) **Storage correctness**: To ensure that there exists no cheating cloud server that can pass the audit from TPA without indeed storing users' data intact;

C) **Privacy-preserving**: To ensure that there exists no way for TPA to derive users' data content from the information collected during the auditing process;

D) **Batch auditing**: to enable TPA with secure and efficient auditing capability to

cope with multiple auditing delegations from possibly large number of different users simultaneously;

E) **Lightweight:** To allow TPA to perform auditing with minimum communication and computation overhead. For the vast majority of cloud storage, the security and privacy options provided are perfectly acceptable. The fact is that most people just don't care about privacy. For those of us that do, however, there is a relatively easy solution that can allow you to continue using cloud storage and keep your data secure, Using Trusted Cloud; you can create encrypted folders within your cloud storage, which gets synched like any other file from the Trusted Cloud. You probably have data stored in multiple clouds - Salesforce, Box.net, Gmail, Amazon, and many others. Trusted Cloud provides you with the ability to create a unified data protection policy across all clouds. As an in-line security gateway that sits between your users and your cloud applications, Trusted Cloud applies encryption on the fly before sensitive data leaves the enterprise. By applying encryption in a cloud security gateway, Cipher Cloud eliminates the inherent security and privacy risks of cloud computing. Your business never loses control of its sensitive data, yet you can achieve the full benefits of cloud computing. Mostly data stored in cloud are not in protected format. There

is a big concern of security in cloud storage. The Trusted Gateway provides a way to encrypt sensitive information to the enterprises as it moves to any cloud application and then decrypt it again as data is delivered to end users. This protects

the data from being accessed by others. This revolutionary technology maintains the cloud application user experience,

with near zero latency, and without making any changes to the cloud application itself. Trusted Gateway takes a revolutionary approach to protecting sensitive data before it leaves an organization's secure enterprise network. the Trusted Gateway examines all outgoing cloud requests, in real time, to identify sensitive data, encrypt that data using TPM, and then forward the modified request to the cloud application. Similarly, encrypted data returning from the cloud application is converted, again in real time, into clear text prior to being displayed to the end user[3]. The entities of the authentication service are as follows:

End User (U): User, who aims to stores encrypted credentials to the cloud storage. So to encrypt data user should authenticate itself to the Trusted Gateway.

Remote User: Remote User, who access the cloud storage outside the internal enterprise network.

Trusted Gateway (TG): Trusted gateway is the work station having TPM which maintains the data to be encrypted comes from end users and encrypt them and store to the cloud storage and vice versa.

Authentication Server (AS): Authentication Server verifies user's access right in database; create ticket granting ticket and session key.

Ticket Granting Server (TGS): Ticket Granting Server issues ticket to request the Trusted Gateway.

Database: The Kerberos service must have a database to store user id (ID) and hashed passwords[1].

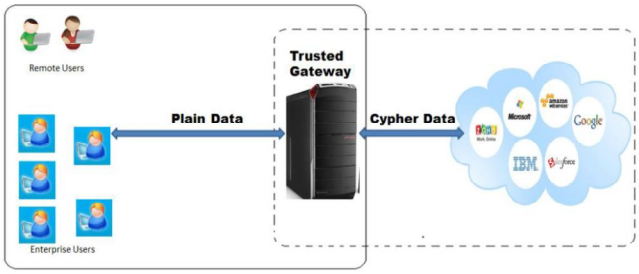

Fig. 2 Trusted Cloud Storage Architecture

VIII. TRUSTED COMPUTING

Encryption is one of the major reasons why online backup is the preferred choice for computer storage. Encryption prevents malicious parties from attempting to access, change or damage files by storing them in a why which is inaccessible without the key. Trusted Computing based on hardware root of trust has been developed by industry to protect computing infrastructure and billions of end points. Encryption prevents unwanted individuals from being able to access, tamper with or vindictively change files to cause harm to you personally or to your business. Encryption is the process whereby you use a program to scramble data in a way which can only be rectified by using a key. This protects the files while they are on our

data servers, by simply storing them away from your PC. TCG[2] created the Trusted Platform Module cryptographic capability, which enforces specific behaviours and protects the system against unauthorized changes and attacks such as malware and root kits. As computing has expanded to different devices and infrastructure has evolved, so too has TCG extended the concept of trusted systems well beyond the computer-with-a-TPM to other devices, ranging

from hard disk drives and mobile phones. Standards-based Trusted Computing technologies developed by TCG members now are deployed in enterprise systems, storage systems, networks, embedded systems, and mobile devices and can secure cloud computing and virtualized systems.

IX. CHARACTERISTICS OF FUTURE DATA CENTER

We propose a new data center architecture with following properties:

• **Isolation**: The architecture provides effective isolation between different customer networks. This includes supporting their private IP address spaces, which may potentially be overlapping, and isolating their traffic. Resource allocation should be managed so that customers cannot impact each other's resource usage in an uncontrolled manner.

• **Transparency**: The underlying data center infrastructure and hardware should be transparent to the customers. Each customer should have a logical view of its own network, independent of the actual implementation. This simplifies the administration for the customer and improves security.

• **Location independence**: The virtual machines (VM) and networks of customers should be "location independent",

i.e., can be physically allocated anywhere in the data center. This can greatly improve resource utilization and simplify provisioning.

• **Easy policy control**: Each customer may have its own policy and security requirements. The architecture should allow customers to configure their individual policy settings on the fly, and enforce such settings in the network.

• **Scalability**: The number of customers that can be supported should be restricted only by the resources available in the data center, not by design artifacts.

• **Low cost.** :The solution must mostly rely on off he- shelf devices, so that new investment for cloud

service providers can be reduced.

X. NETWORK VIRTUALIZATION TECHNIQUES

In this paper, we exploit recent advances in technologies amenable to network virtualization. Network virtualization techniques can logically separate different networks on the same hardware and partition resources accordingly. This feature is useful for providing good isolation as well as network-resource sharing among different users. Furthermore, recently proposed mechanisms simplify packet-forwarding elements and make control functions more flexible and managable by using centralized control. Given the high density of physical resources and demand for high manage ability of devices, the centralized control architecture suits data center networks very well. However, unlike in typical network virtualization solutions, our design does not require deploying specialized routers or switches across the entire data center network. Instead, conventional off-the-shelf Ethernet switches can be used in most parts of the network. Enhanced layer 2 switches, which we refer as Forwarding Elements (FE), are deployed only at certain aggregation points to provide the required virtualization functions. In this architecture, each customer has its own isolated virtual network in the data center, to which access is tightly controlled. But physically, such virtual network may be distributed at anywhere in the data center. This architecture intends to offer a more secured elastic cloud computing (SEC2) service. But the design can also naturally support virtual private cloud (VPC) service, where each user's private network in cloud is connected to its on-site network via VPN.___ __

XI. SECURE ELASTIC CLOUD COMPUTING (SEC2)

Based on the above observations, we propose a new design based on network virtualization. In this design, network virtualization is accomplished by two entities:

Forwarding Elements (FEs) and Central Controller (CC). FEs are basically Ethernet switches with enhanced APIs that allow them to be controlled from a remote CC. Packet handling actions such as address mapping, policy checking and enforcement, and forwarding are done in FEs. CC stores control information such as addresses, location, and policy. Such information is distributed to different FEs as needed[7,8,9].

A.Central Controller (CC)

CC controls the operation of FEs. It maintains both address mapping and policy databases.CC also maintains policy rules..Although CC is conceptually one entity in this architecture, it can be implemented in a distributed way. For example, different customers can be assigned to different CCs by using Distributed Hash Table (DHT). Since the management and policy control

of different customer networks are relatively independent, such partition does not affect the functionality of CC[6].

B.Forwarding Elements (FE)

FEs are gateways between the core domain and the edge domains. Each edge domain may have more than one FEs for redundancy purpose. Functions of FE include the following:

• **Address lookup and mapping**. When a packet is originated from its edge domain to other domains, it looks up the FE MAC of the destination domain and VLAN ID in destination domain. This is done by first checking its local cache, and if there is no hit, it inquires the CC[8,9].

• **Policy enforcement**. FEs enforce policy by applying filtering, QoS treatment, or redirecting to middle boxes that are attached to them. By default, packets designated to a different customer are dropped.

• **Tunnelling.** FE tunnels the packet across the core domain to the destination FE via MAC-in-MAC.

The source FE adds another MAC header to the original Ethernet frame. The destination FE strips off the outer layer header upon receiving the packet. Most modern Ethernet switches allow larger frame sizes (jumbo frames) to be used so the extra few bytes of MAC header is not a problem. This is especially true for the core domain since we expect high-end Ethernet switches to be deployed to meet capacity needs in the core. experienced by products and vendors are merely a symptom of more fundamental long-term changes.

Four fundamental economic forces have shaped the data center up until now and will continue to shape the systems inhabiting the data center .

The data center of the future will be shaped by four forces: commoditization, virtualization, integration, and innovation. We are witnessing a long-term shift in scope from assembling and configuring standard client/server systems out of standard components based on standard designs, to assembling and configuring standard data centers out of virtual components based on standard designs. As a result, automated, virtualized, operational services (e.g., design, assembly, provisioning, monitoring, change management) become essential for managing the complex dynamic relationships among the components[6].

XII. COMMODITIZING THE DATA CENTER OF THE FUTURE

Commoditization depends on a vast underlying network infrastructure of buyers, distributors, suppliers, and assemblers. Commoditization can be broken down into two complementary forces: standardization and specialization. Twenty years ago, in the inframe/minicomputer era, users were essentially required to buy their servers, terminals, storage, and networks from one vendor. Today, users have the flexibility to mix and match networks from one vendor with servers from another vendor, with storage from a third vendor, and with clients from yet another. All this is due to the emergence of standards and the increasing use of networks among the various tiers. While the shift from the mainframe to the client/server era during the past 20 years certainly changed many aspects of the data center, it did not fundamentally change the proprietary nature of the data center resources.

A.Network: The data network layer is clearly standardized on TCP/IP. The DCFuture will increase standardization of the network stack up through the middleware layers..

B.Storage: In storage, the trend is toward storage-area networks (SANs), clearly standardized on SCSI as the interface between servers and SANs. In the DCFuture the SAN technology will begin to significantly converge with IP-network technology.

C.Server Hardware: After many years of diverging standards, the server market is standardizing on IA-32 running Linux, and Windows. IA-32 dominates the DCFuture by 2007.

E.Server OS: With distributed n-tier server hardware standardizing on IA-32, proprietary Unix (Solaris,HP-UX, AIX) will recede, joining z/OS and iOS (OS/400) as high-end, low-unit-volume, legacy-platform status by 2005/06, displaced by commodity OSs designed for commodity hardware.J2EE and .Net application servers will be key business application implementation platforms through 2007.

Open Source: Just as the evolution of software portability has virtualized and commoditized hardware during the past 20 years, the evolution of XML Web services network interoperability will virtualized and commoditize software during the next 20 years. This is one of the reasons that open source software. Bottom Line on Commoditization: The DCFuture will be populated by storage, server, and network elements from diverse vendors, defined by increasingly standardized interoperable interfaces. This benefits the end user due to the competitive landscape of hardware and software vendors[5].

XIII. VIRTUALIZING THE DATA CENTER OF THE FUTURE

Another unmistakable DC Future architectural trend is systems composed of increasing numbers of functionally identical subsystems of decreasing size. Virtualization can be broken down into two complementary forces:

Miniaturization: The system's size and complexity, relative to its performance, decreases over time whether the system is at the chip, disk, or port level, the board level, or even the server level.

Massification: The number of subsystems composing a system's instances grows over time thousands of processors, servers, spindles.

Virtualization is the answer to the question on the minds of every CIO: One of the primary benefits of virtualization is that it can increase utilization beyond the traditionally low utilization rates (<25%) for Unix and Windows servers. By more dynamically distributing workloads across server, storage, and communications resources, utilization rates can begin to increase to 50%-75%, slowing the need to buy additional resources. However, the benefits of virtualization go far beyond increased utilization. Other benefits include[5]:

Increased performance

Increased availability (rolling upgrades and shared/spared resource pools)

Increased innovation

Increased commoditization of underlying resources

Increased commoditization of management skills

In short, virtualization is the key to providing utility- or carrier-grade IT services as those capabilities

become mainstream.

XIV. INTEGRATING THE DATA CENTER OF THE FUTURE

Although the forces of commoditization and virtualization will dramatically drive down the costs of the individual components inhabiting the DCFuture, the explosion in the number of components in the largest data centers from thousands (2003-05) to tens of thousands (2005+) could drive coordination costs of integrating so many components so high that they completely

overwhelm such cost savings. Fundamentally new approaches to integrating such components must be found. The various approaches to loosely coupling within and among the various domains (middleware, storage, servers) are unified by one relentless trend — integration via asynchronous, message-based, routable, hotpluggable, standard networks. The DCFuture is in transition from a proprietary-platform-centric world to a standard-network-centric world. Clearly, traditional approaches to integrating systems parallel buses, server partitioning, clustering, distributed objects, TP monitors will not suffice. The only proven approach to successfully integrating millions of servers on a global scale is the worldwide Web[5].

XV. INNOVATING THE DATA CENTER OF THE FUTURE

The exploding complexity of the DCFuture is not only driven by the degree of integration among all systems, but also compounded by the fact that the rate of change of those integrated systems and their interconnections is far faster from network topology changes, to software configuration changes, to application integration changes. One strategy is simply to slow the pace of data center change to reduce the complexity. Unfortunately, slowing the pace of data center change has one potentially catastrophic side effect: it could slow the pace of the business. In those businesses in which IT innovation is essential to business innovation, which includes more businesses every day, some other way of managing the complexity of rapid innovation must be found. To prevent the data center from eventually consuming the entire IT budget, increased manageability and resource utilization through standardization and automation are essential. However, while virtualizing the use of diverse resources is straightforward virtualizing their management is not[5].

XVI. CONCLUSION

The data center of the future will be a simplified, commoditized, virtualized set of computational, storage, and network resources that is enabled by ubiquitous, interoperable standards. Such standardization of components and interfaces will enable the transformation of what is essentially a craft industry for manufacturing hand-crafted infrastructure configurations for one or a few applications, into a standardized industry for assembling machine-generated infrastructure configurations for many applications.

The path of the four forces that has shaped the data center throughout its history is not that of a pendulum that reverses direction periodically; rather, it is the path of a ratchet that is inexorably evolving the data center in a single direction: toward larger numbers of smaller, simpler, more specialized component systems that are more dynamically composed into solution systems via increasingly powerful networks. This is the data center of the future.

REFERENCES

1. Abhishek Patel, Mayank Kumar A Proposed Model for Data Security of Cloud Storage Using Trusted Platform Module, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3,April 2013.

2. Trusted Computing Group.[Online].Available: https://www.trustedcomputinggroup.org/

3. William Stallings, *Cryptography and Network Security- Principles and Practices*, 3rd Edition, Prentice Hall of India, 2003.

4. K.Valli Madhavi, R. Tamilkodi and R.Bala Dinakar, "Data Storage Security in Cloud Computing for Ensuring Effective and Flexible Distributed System," *International Journal of Electronics Communication and Computer Engineering,* Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X.

5. Nick Gall The Data Center of the Future, Integration & Development Strategies, *A META Group White Paper* March 2003.

6. Fang Hao, T.V. Lakshman, Sarit Mukherjee, Haoyu Song, Bell Labs, Alcatel-Lucent, Secure Cloud Computing with a Virtualized Network.

7. Global Environment for Network Innovations. *http://www.geni.net*, 2006.

8. T. Lakshman, T. Nandagopal, R. Ramjee, K. Sabnani, and T. Woo, The SoftRouter Architecture. In *ACM HOTNETS*, 2004.

9. N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, Openflow: Enabling innovation in campus networks. *http://www.openflowswitch.org*, 2008.

10. Juniper Networks, Logical Router Overview.*Systems Design and Implementation*, 2005.

11. M. Armbrust et al, Above the Clouds: A Berkeley View of Cloud Computing. *http://www.eecs.berkeley.edu*, 2009.

12. Dark Reading, Security is chief obstacle to cloud computing adoption, study says, *http://www.darkreading.com*.

13. Network World, Are security issues delaying adoption of cloud computing?, *http://www.networkworld.com*.