International Journal of Scientific Research in Computer Science and Engineering
Review Paper Vol-1, Issue-6 ISSN: 2320-7639

Study of Services and Privacy Usage in Cloud Computing

Rakesh Prasad Sarang[1*], Rajesh Kumar Bunkar[2]

[1*] *Computer Science & Application, IPS College Gwalior, India, sarang.snit@gmail.com*
[2] *Computer Science, IGN Tribal University, Amarkantak, India, bunkar.rajesh@gmail.com*

Available online at www.isroset.org

Received: 16 Nov 2013 Revised: 20 Nov 2013 Accepted: 12 Dec 2013 Published: 30 Dec 2013

***Abstract*—** In last decade, there are several survey point out over privacy and services has risen and increasingly becoming central point for IT industries. Almost every day, IT sector, network security and sensitive data are being broken. This uses more advanced techniques to protect their information. Privacy is a very essential issue for cloud computing. Hence there is a need of an effective privacy and security that protect data, information and technology resources adequately. This survey focus on cloud computing, its architecture, services and identifies the cloud computing privacy. In this paper, we are presenting a service models to deal with the privacy and security problems in cloud computing environment. We elaborate privacy and service models as considered in cloud computing resources and the proper preventing their data. There are multifarious security and privacy that need to be understood. The paper includes some privacy and techniques that show the motivation for the adoption of cloud computing.

Keywords- Cloud Computing,Service Models, Vulnerability Privacy and Cloud Usage

I. INTRODUCTION

Cloud computing emerges as a computing platform for the next generation of the new computing technology. Cloud computing is a technology which provided you as a service with users can access all the database resources and software through the internet from anywhere in the world, as long as they need. But actually the system resource doesn't install on your system, it is provided only for services by another company and accessed using a browser over the internet [1].

In this paper privacy & services issues of cloud computing are reviewed. The cloud computing techniques has several applications and components in different areas including client's datacenter, and distributed servers. Through cloud computing we can design and carryout implementation of security applications. However it is mandatory that the service models need to be inbuilt and enabled for the desired objectives. Cloud computing is a system, where the resources of a data center is shared using virtualization technology, which also provides elastic, on demand and instant services to its customers and associate customer usage as grid computing [2].

Cloud computing technique is also advantageous in control of datacenter information security policy, information security infrastructure, security of third party. Cloud computing aids virtualization and Grid Technology analysis for security activities. Virtualization and grid technology analysis are some of the techniques which are especially useful in diverse fields such as IT Technologies, Services Provider Applications, Information security, Control network segment and sharing resources etc.

In this paper we present, the privacy and service issues in cloud computing environment. We would also investigate challenges in cloud computing, and the uses of cloud computing. Vulnerability: According to the Open Group's risk taxonomy "Vulnerability is the possibility that a quality will be unable to resist the actions of a threat agent. Vulnerability exists when there is a differentiation between the energy being applied by the threat agent, and an object's capability to resist that force." So, vulnerability must always be described in terms of conflict to a certain type of attack.

In this works, we provides an overview of the most important privacy regulations in the cloud-computing environment, cloud providers, in traditional IT environments, clients connect to multiple servers located on company site. Clients need to connect to each of the servers separately. In cloud computing clients connect to the cloud, the cloud contains all of the applications and infrastructure and appears as a single entity. Cloud computing allows for dynamically reconfigurable resources to supply for changes in demand for load, more efficient use of the resources. This exclusive aspects, however poses many tangible and intangible security challenges like accessibility vulnerabilities, virtualization vulnerabilities, and web applications. All challenges relate to cloud server having physical control of data and manage documentation [3] [4].

This paper is organized as follows: in Section 1 present Introduction of privacy and security issues in cloud computing environments. Section 2 presented architecture and addressing in cloud computing. Section 3 present better service models. Section 4 presents cloud vulnerabilities security. Section 5 presents privacy and security in cloud computing. Section 6 presents cloud security usage. Finally section 7 presents conclusions.

II. ARCHITECTURE OF CLOUD COMPUTING

In this cloud computing we used to define five major architectural modules and their associations, show in fig 1

Corresponding Author: R.P.Sarang

the architecture of cloud computing is a huge network of "server cloud" interrelated as in a grid. The virtualization could be used to maximize the process of the computing power available on server to improve the overall workload. A front end interface such as a gateway allows a user to select a service from a grid. This request gets passed to the system management which finds the correct resources and then calls the provisioning services which allocates resources in the cloud. The provisioning service may deploy the requested control server or software application through authorization on-demand.

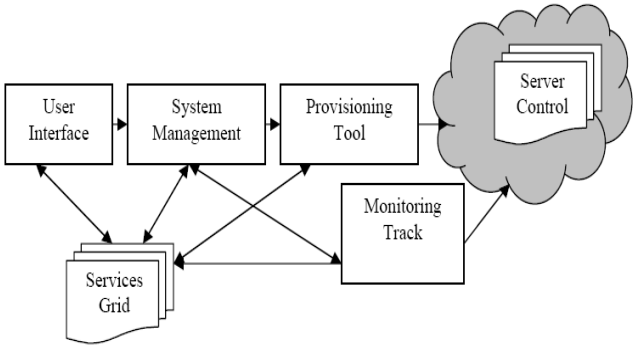

Fig. 1 General Cloud Computing Architecture

- User Interface - A user interface is the system by which users interact with a machine. The user interface includes hardware (physical) and software (logical) components. The term user interface is generally assumed to the graphical user interface, while industrial control panel and control server. The cloud user interface with the underlying Grid to request services.
- System Management - System management refers to enterprise-wide administration of distributed computer system. That is related to the provisioning service, which manages the computer resources available on grid. System management may involve one or more tasks like server availability monitoring, software installation and hardware inventory, network capacity and security management.
- Provisioning Tool - Provisioning tool is the process of preparing and equipping a network to allow it to new services to users. This tool allocates the systems from the Grid to deliver on the requested grid service. It may also deploy the required software
- Server Control - control server that hosts the supervisory control system management. They can be either virtual machine or authentic. Control server rights is equivalent to system admin permission except the fact that logins. Also that logins with control server permission will have implicit access to the databases linked service grid.
- Service Grid - A grid is the list of services that an organization provides, often to its employees or customers. Service grids enable aggregation of distributed resources and transparently access to web services-based protocols that allow distributed resources to be accessed, user interface, system management, provisioning and monitoring track.
- Monitoring Track - monitoring track system is the optional part that usage of the grid so the resources used can be attributed to a certain user. The monitoring are also pass through system by linked control server area [5].

III. CLOUD COMPUTING SERVICE MODELS

A. Software as a service(SaaS)

SaaS is a model of software deployment where an application is hosted as a service to client's access via the internet. SaaS has been around since early 2001. It refers to the computing resources as a service and Application Service Provider (ASP). Where applications are hosted and delivered online via a web browser offering traditional desktop functionality. SaaS consist of software running on the cloud infrastructure. It provides storage that the consumer is used including bandwidth requirements for the storage. The client contains a multiple browser to access the application (on-demand) via thin client over the internet. Examples of SaaS are Google, Docs and Salesforce.com [6].

B. Platform as a service(PaaS)

PaaS is another application model, where supplies all the resources required to build (develops, test and deploy). It also includes operating system and required services for particular applications. PaaS providers offer a predefined combination of OS, development tools, Integrated Development Environment (IDE) and application servers, such as LAMP platform (Linux, Apache, MySql and PHP). These platforms include data security, backup, recovery, application hosting, and scalable architecture. Examples of PaaS are Microsoft Azure, Google App Eng and Force.com [7].

C. Infrastructure as a service(IaaS)

Iaas is a service which provides an access to hardware resources for executing services, such as CPU processing, memory, data storage and network connectivity. The vendor may share their hardware among multiple customers referred to as multiple tenants, using virtualization software resource. IaaS allow customers to run operating systems and software applications.

Fig 2 shows the basic cloud architecture provides the various common deployment service models with related different elements of cloud computing. The above mentioned service models, where the three cloud service models can be deployed on top of the four deployment models depending on the clients' requirements.

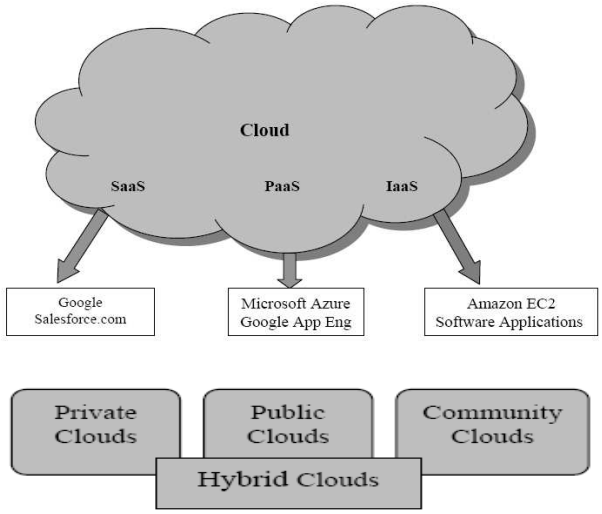

Fig. 2 Cloud Computing deployment Service Models

IV. CLOUD VULNERABILITIES

1) Securely fortrnsfarring data: Securely transferring data: Our data can be vulnerable to prying eyes as we hand on it and from the cloud. Therefore we should not shift important or confidential data in an open wireless network, in a random public Wi-Fi network. It is better to use our home network, and ensure encrypting our data. We should make sure that our wireless router is password-protected. We should ensure that the Web addresses of sites we are visiting are HTTPS rather than simply HTTP. HTTPS sites are encrypted to transfer information safely.

2) Data backup: Our data isn't floating around in the clouds; it's stored on a physical server somewhere. So what happens when there is a hurricane or a flood or a power failure? Take the time to evaluate our cloud provider's disaster recovery plan when we use the cloud to store critical data then have our own backup as well. "In the confidentiality world, they talk about organizations being 'custodians of data,' and that's a good way to look at it". We should be careful as we are handing critical information over to someone else. Ensuring that our data exists elsewhere whether on an external hard drive, on our laptop's hard drive or on a USB drive will give us peace of mind.

3) Accessing Data: There is nothing worse than trying to recover our information and finding it's not available. "Customers want to know that their data is available when they need it".. Before we delegate a cloud provider with our data, we should evaluate what sort of guarantee they have about uptime when our data is accessible and consider their track record. Generally better off sticking with honest, big-name providers.

4) Privacy: Privacy is important consideration about the information we distribute. For example, why provide a phone number to sign up for an email news letter? Take the time to irregularly review which mobile applications and third party services have access to key accounts such as Facebook and Twitter. Reviewing the admission grants will remind we to sever that relationship, removing any possibility of abuse or exploit [8].

5) Using Password: Multiple instance of hacks and data breach has exposed the passwords of users of well-known websites and companies. These attacks also lean-to light on what a miserable job most of us do in using strong, unique passwords. We should try not to use the identical password for all our activities in the cloud. If we use the similar password for a gaming site as we do for our bank account, we place our finances at risk, if that gaming password is compromised. It is good practice to use a password manager such as Last Pass.

V. CLOUD SECURITY AND PRIVACY

This paper looks at the main privacy and security an issue relevant to cloud computing, as they relate to outsourcing portions of the organizational computing environment. It point out areas of concern with public clouds that require special attention and data protection provides the necessary on Security and privacy in cloud computing.

We have multiple security issues that need to be protected data and Information. Here we comparison private and public cloud computing scenario. A public cloud works as a host of a number of virtual machines, virtual machine monitors, supporting middleware. But in a public cloud enabling a shared multi-tenant environment, as the number of users is increasing, security risks are getting more intensified and diverse. So it is necessary to identify the attack surfaces which are security attacks and mechanisms ensuring successful client-side and server-side protection. Because different security issues in a public cloud, adopting a private cloud solution is more secure with an option to move to public cloud in future if needed. Hence, security is very essential at different levels in order to manage and proper implementation of cloud computing such as: server access security, internet access security, database access security, data privacy security and program access security. Some security concerns are listed and discussed below.

A. Network Level Security

There are several types of securities are into Network level that are, shared and non-shared, public or private, small area

or large area networks and each of them have a number of security threats to deal with. To ensure network security following points such as: privacy and integrity in the network, proper access control and maintaining security against the external third party threats should be considered while providing network level security [9].

B. Application Level Security

Application level security refers to the usage of software and hardware resources to provide security and applications such as the attackers are not able to get control over these applications and make desirable changes to their format. That is the outdated network level security policies allow only the authorized users to access the specific IP address. The recent technological advancement, these have higher level of security policies with high performance [10].

C. Information Level Security

Information Level security, which is approved by the management, published and communicated as appropriate to all employees. It conditions the management commitment and set out the organizational approach to managing information security. Like Information security infrastructure, security of third party access, Virtualization and Grid Technologies, identity and access management, secure development lifecycle and secure activities on cloud computing [11].

D. Client-Side Protection

Client-Side Protection, a successful defense both client side and web side infrastructures both are required for protection against attacks. For the former to be overlooked typical emphasis are placed on the latter. For many cloud computing services web browser act as a key element, and the various plug-ins and extensions which are available for their security problems.

E. Server-Side Protection

Server-Side Protection, an IaaS clouds, virtual servers and applications, much like their non-virtualized counterparts, are needed to be secured. For the occurrence of VM images for deployment following organizational policies and procedures for hardening of the operating system and applications are launched. Proper care should be taken to make adjustments for the virtualized environments so that images can run [12].

VI. USAGE OF CLOUD SECURITY

Your cloud computing is a new business model wrapped around new technologies like virtualization, SaaS and broadband internet. Recent interests offered new applications and IT educational usage of cloud computing. The Cloud delivers computing and storage resources to its users. It works as a service on demand scalability with higher computing parameters for ICT. So, these have continuing IT management of the resources.

A. ICT Capability of Cloud Usage

This section includes survey conducted by international data corporation (IDC). It shows the strength of cloud computing to be implemented in IT industry and gives the potential inspiration to CSP. The fig 3 shows the graph that is collected by IDC. It shows today's and future usage of cloud in different areas [13].

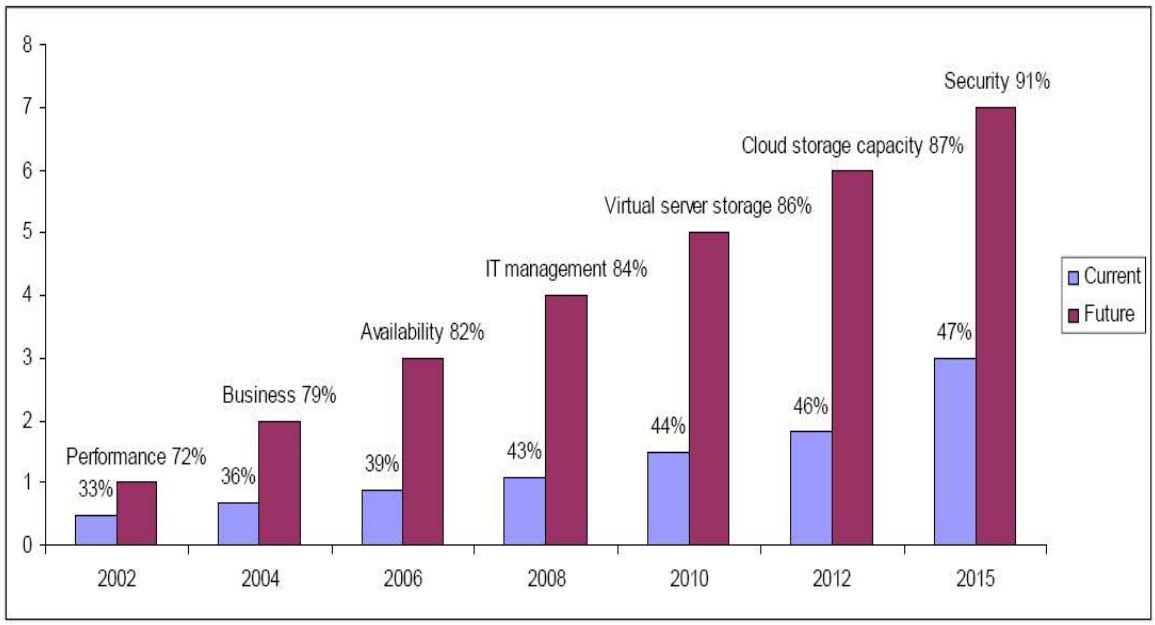

Fig. 3 Current usage of cloud

In fig 4 shows the IT trends for future (especially cloud computing) that it is being used more in the areas of IT industries and business when compared to other sectors. The results are shown as a pie chart and the labels on each different slice represent different industrial sectors and services. Here the percentages of cloud usage in different IT industrial sectors, business, media and security, schools and education, government, and professional services [14] [15].

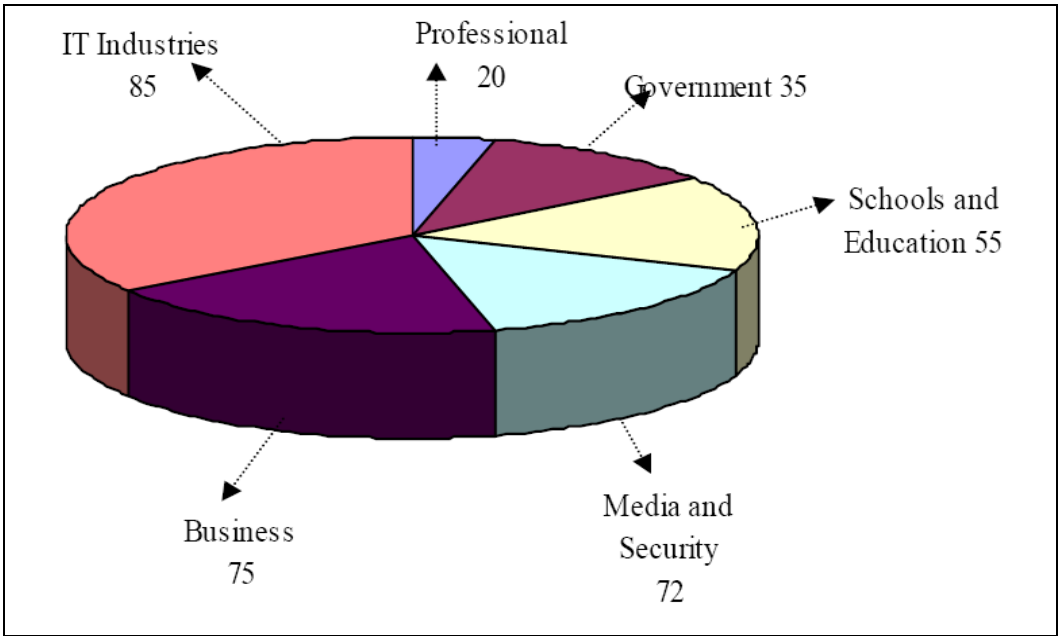

Fig.4 Cloud usage of future

B. Data Security on Use

The data use requires the insurance of data availability in cloud and their use (visualization, processing, and access) by the authorized people. Access management occupies an important part inside this phase. The human rights and permissions related to individuals, devices or positions allow the controlled and authorized access to data use. The use and safe transfer of network data can also be achieved through separation, using different strategies, such as multiprotocol label switching (MPLS), virtual private networks (VPNs) and virtual local-area networks. In the MPLS-VPN process, isolation is performed through routing network devices to a virtual routing and forwarding system [16].

Public cloud not only increases the privacy issue but also security concern. Information security is a main issue current cloud offerings are essentially public exposing the system to more attacks. In this cause there are potentially additional challenges to make cloud computing environments as secure in IT industries. Security and privacy affect the entire cloud computing stack, since Information requiring standard security and various privacy challenges with the specific steps to be taken in the cloud computing [17].

VII. CONCLUSION

Cloud computing is latest development that provides easy access to high performance computing resources and storage infrastructure through web services. This paper mainly discusses privacy and security importance of system behavior and challenges in the cloud computing, including services model. This services the theoretical foundation and practical cloud computing application. We also identity challenges and opportunities in cloud computing. The paper addresses the issues that can arise during the deployment of cloud services model.

This paper has presented the cloud computing can provide resources in IT industries and can also help to reduce computing costs within organizations, and also new business opportunities for service-oriented models. This is particularly useful during organizational sustainability. However it can provide the basis for the deeper research on security deployment of cloud computing.

REFERENCES

[1] Rao, Srinivasa, and V Nageswara Rao, "Cloud Computing: an Overview", (JATIT) Journal of Theoretical and Applied Information Technology, 71-76, 2009.

[2] Khorshed, Tanzim, A B M Shawkat Ali, and Saleh A Wasimi, "A Survey on Gaps, Threat Remediation Challenges and Some Thoughts for Proactive Attack Detection in Cloud Computing", Future Generation Computer Systems, 833-851, 2012.

[3] Ruiter, Joep, and Martijn Warnier, "Privacy Regulations for Cloud Computing", 1-16.

[4] Sun D, Chang G, Sun L, Wang X, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud computing Environment", Elsevier Procedia Engineering, 2852-2856, 2011.

[5] Metri, Priya, Sarote, Geeta,"Privacy Issues and Challenges in Cloud Computing", (IJAEST) International Journal of Advanced Engineering Sciences and Technologies, vol. 5, 1-6, 2011.

[6] Sultan, Nabil, "Cloud Computing for Education: A New Dawn", (IJIM) International Journal of Information Management, 30 109-116, 2010.

[7] San Francisco, CA Chappell and Associates Chappell, D. A. "Short introduction to Cloud platforms: An Enterprise-Oriented view", Aug. 2008.

[8] Bhadauria, Rohit, Chaki, Rituparna, Nabendu, Sanyal, Sugata, "A Survey on Security Issues in Cloud Computing", Electronics and Communications.

[9] Jens, F. Jones, M. T. "Cloud computing with Linux Defining Cloud services and cloud computing", Sept. 2008.

[10] Scalable Security Solutions, Check Point Open Performance Architecture, Quad Core Intel Xeon Processors, "Delivering Application-Level Security at Data Centre Performance Levels", IntelCorporation,2008.http://download.intel.com/netcomms/technologies/security.

[11] Kumar, Pardeep, Sehgal, Vivek, Chauhan, Durg, Singh, Gupta, P K, and Diwakar, Manoj "Effective Ways of Secure, Private and Trusted Cloud Computing", (IJCSI) International Journal of Computer Science Issues, vol.8, 412-421, May. 2011.

[12] Jansen, Wayne A, "Cloud Hooks: Security and Privacy Issues in Cloud Computing", 44th Hawaii International Conference on System Sciences, 1-10, Oct. 2011.

[13] Alvi, F. A., Choudary, B. S., & Jaferry, N., "A review on cloud computing security issues & challenges".

[14] Ercan, T., "Effective use of cloud computing in educational institutions", Sciences-New York, 2, 938-942.sbspro, 130, 2010.

[15] Open Grid Forum. "Cloud Storage for Cloud Computing Storage Networking Industry Association", http://www.snia.org/cloud/ Cloud Storage for Cloud Computing, 2009.

[16] Mircea, M., "Addressing Data Security in the Cloud", Intelligence World Academy of Science, Engineering and Technology 6, 539-546, 2012.

[17] S. Jordan, and A. Bruno, "CCDA 640-864 Official Cert Guide, 4th Edition", Indianapolis: Cisco Press. 2011.

