International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 2, February - 2014

Analytical Survey of Cloud Computing as a Service and Representation of its Life Cycle.

[1]Ayushi Prakash, [2]Ravi Kant Yadav, [3]Bhawana Malik, [4]Vineet Kr. Singh
[1]Asstt. Prof, Department of C.S.E., Dr. K.N.Modi Foudation, Ghaziabad, India
[2]Sales & Application Manager, BWMT, Ghaziabad, India
[3]Lecturer, Department of I.T., Dr. K.N.Modi Foudation, Ghaziabad, India
[4]Lecturer, Department of I.T., I.E.T. Faizabad, India

***Abstract*— The cloud is basically metonymy for the internet, cloud computing is a significant advancement in the delivery of information technology and services .It leverages its low cost and simplicity to both providers and users .But the security is the prime concern as it involves lot of sensitivity data. This paper describes cloud computing, its service models, security and privacy issues, benefits and representation of cloud computing management life cycle.**

Keywords*— *Cloud, Data security, Life Cycle, Service.

I. INTRODUCTION

Today security is a major challenge of any internet user. Data security is the means of ensuring that data is safe from corruption and the access to it is suitability control, and privacy is ensured by both data security.

Cloud computing technology uses the internet and central remote servers to maintain data and applications. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth [1].Cloud computing is an extension of old mainframe concepts of sharing with the addition of networking and application runs. It has advantages like costs, capacity addition, availability security, experimentation with new technologies, management, minimal use of resources etc [1].

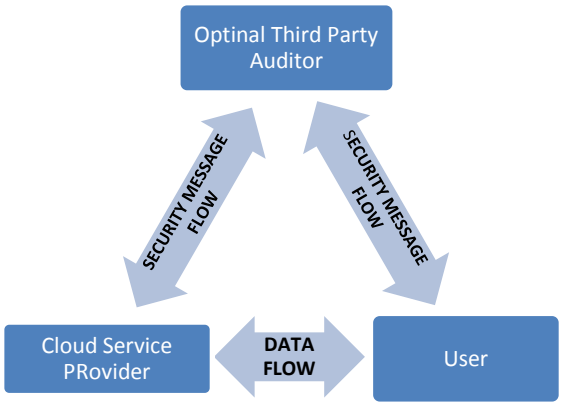

Fig.1: Cloud data storage architecture

Cloud succeeds or fails depends on the system management and its quality. In this paper we proposed security as a service by cloud computing. The remaining sections are organized as follows: In section 2, cloud service models. Section 3 is its security and privacy issues. Section 4, then benefits and challenges of cloud computing .Then section 5, represents the cloud computing management life cycle and finally in section 6, future work and results are discussed.

II. CLOUD COMPUTING SERVICE MODELS

In this section we describe the service model. Each service has its own security issues. Cloud computing providers offer their services according to several fundamental model SaaS, IaaS, PaaS. In 2012 networking as a service (Naas) and communication as a service (Caas) were officially included by ITU (International Telecommunication Union).

Software as a Service Model

In this SaaS, users are provided access to application software and database. In this model, application could run entirely on the network, with the user interface living on a thin client .Degree of control by providers is high and they are responsible for confidentiality, integrity and availability of their services. One drawback of SaaS is that users' data are stored on cloud provider's server. So as result, there could be unauthorized access to the data. [4]

CLOUD CLIENTS (Web browsers, Mobile app, Thin client, Terminal Emulator)	
Application	**SaaS (Email, CRM, Games….)**
Platform	**PaaS (Executon runtime, Database, Web server..)**
Infrastructure	**IaaS (Virtual Machine, Server, Network….)**

Fig 2: A model for data security in cloud computing

Platform as a Service Model

In this model cloud providers deliver a computing platform, including operating System, programming language, execution runtime, database, and web server. The user does not manage the underlying cloud infrastructure. A downfall to PaaS is a lack of interoperability and portability among providers is

medium and they are responsible for confidentiality and data privacy.

Infrastructure as a Service Model

In the most basic cloud service model, providers of IaaS offer computers physical or virtual machine and other hardware resources. Degree of control by providers is low and they are only responsible for availability of their services .But users' responsibility is high and they are responsible of confidentiality, data privacy and integrity. [5]

Network as a Service

A model ensure the capability provided to the cloud service user is to use network/transport connectivity service or/and intercloud network connectivity services. [2]

III. Cloud Computing Security and Privacy

Issues

IT Governance: It include the techniques, policies, standards, design, implementation, testing, as well as monitoring of services that measure and control how systems are managed. With the wide availability of cloud computing services, lack of organizational control over employees such services arbitrarily can be source of problem.

Compliances: It involves conformance with an established specification, standards, regulation, or law. Various types of security and privacy laws and regulations exits within different countries, making compliances a complicated issue for cloud computing.

Legal: Certain legal issues arise with cloud computing, including trademark infringement, security concern and sharing proprietary data resources. These legal issues are not confined to the time period in which the cloud based application is actively being used. However in case like bankruptcy the state of data may become blurred.

Trust: Under the cloud computing model, an organization hand over direct control over many aspects of security, in doing so, confers an unprecedented level of trust onto the cloud provider.

Vendor Lock-in: Many cloud platforms and services are proprietary, meaning that they are built on the specific standards, tools, and protocols developed by a particular vendor for its particular cloud offering. This can make migrating off a proprietary cloud platform prohibitively complicated and expensive.

Data Protection: Data stored in the cloud typically resides in a shared environment collocated with data from other customers. Organizations moving sensitive and regulated data into the cloud, must account for the means by which access to the data is controlled and the data is kept secure. [1]

Abuse: As with privately purchased hardware, customer can purchase the services of cloud computing to cheat people out of their money. This includes password cracking and launching attacks using this purchased services.

Availability: Availability is the extent to which an organization's full set of computational resources is accessible and usable. Availability can be affected temporarily or permanently, and a loss can be partial or complete. [1]

IV. Security Benefits

Effectiveness: The cloud focuses on maximizing the effectiveness of the shared resources.

Availability: The scalability of cloud computing facilities allows for greater availability especially for disaster recovery for better resilience when facing denial of service attacks and for quick recovery from serious incidents.

Platform Strength: Greater uniformity and homogeneity facilitate platform hardening and enable better automation of security management activities.

Coherence and economic of scale: Cloud Computing relies on sharing of resources to achieve coherence and economic of scale.

Backup and Recovery: The backup and recovery policies and procedures of a cloud service may be superior to those of the organization.

Data Concentration: Data maintained and processed in the cloud can present less of a risk to an organization.

Cloud Oriented: Cloud services are available to improve the security of other cloud environments.

V. Challenges [6]

- Loss of Control
- Data Protection
- User Authentication
- Attraction to Hackers
- Cracking
- System complexity
- Privacy law on International standard

VI. Life Cycle of Clouding Computing

In this section a cloud life cycle approach is introduced and it is shown how such an approach can be used for both the migration and ongoing management of public and cloud based services. The cloud life cycle is like a documented project management policy that is the requirement of most IT and business managers in this era. The cloud life cycle is broadly categorized in four broad phases and then further divided in to nine steps as illustrated in fig. (3).Each step is essential and important for next step and for successful result.

Following are the four phases of Cloud Computing:

- **Analysis and Discovery**

  The very first phase begins with the investigation and planning of cloud project. The planning stage turns requirement in to design and deployment options. The design includes alignment to the enterprise architecture, mapping cloud computing providers against requirements, ranking tools for each solution, assisting the organization in SLAs with cloud providers and developing a cost.

- **Selection**

- The second phase selects service providers that can provide the required services by providing clouds.

- **Implementation**

The most important phase is the operation phase where service providers operates the cloud services and take care of the management issues.

- **Review**

The last but not least important phase is refresh phase in which the service providers reviews the requirements.

A. Clearly the above lifecycle is an over simplification of real process, but illustrative of the basic 9 steps. [3]

Step 1: Investigate
Investigate a vision into and understanding of what an organization wants to achieve by moving to the cloud, their goal, expectations are to be met and that is based on analysis of industrial segment.

Step 2: Identify
To determine what services will be outsourced to the cloud, what type of cloud outsourcing model will be used and documentation of current and future state of IT infrastructure.

Step 3: Implementation Strategy
This step defines the strategy to roll out the cloud services that are to be outsourced, the details of how the program will be staffed and reported and how the risk will be managed.

Step 4: Designing
This step defines the SLA (Service Level Agreement), pricing model, negotiable and non negotiable issues and all the details of the services. It provides the clear definition of the existing and desired interfaces.

Step 5: Deployment
In deployment, we offer an effective and efficient set of cloud infrastructure and application that run in the cloud. It supports a variety of mechanism for deploying cloning, fresh install and template based creations.

Step 6: Install and Active
Activation is the activity of starting up the executable component of software cloud computing deployment considering fees, licensing, SLA, guidelines, security, performance, maintenance, and operational monitoring.

Step 7: Monitor
It is important to manage the new cloud services as efficiently and effectively as possible. The organization will need to adapt to the new setup, particularly at IT management level. This will provide require effective monitoring and control so that issues or disputed can be resolved to the satisfaction of both parties.

Step 8: Maintenance
This phase provides comprehensive patching capabilities that include understanding the customer configuration, advising customer configuration on what patches are available and should be applied, planning patch deployment and testing.

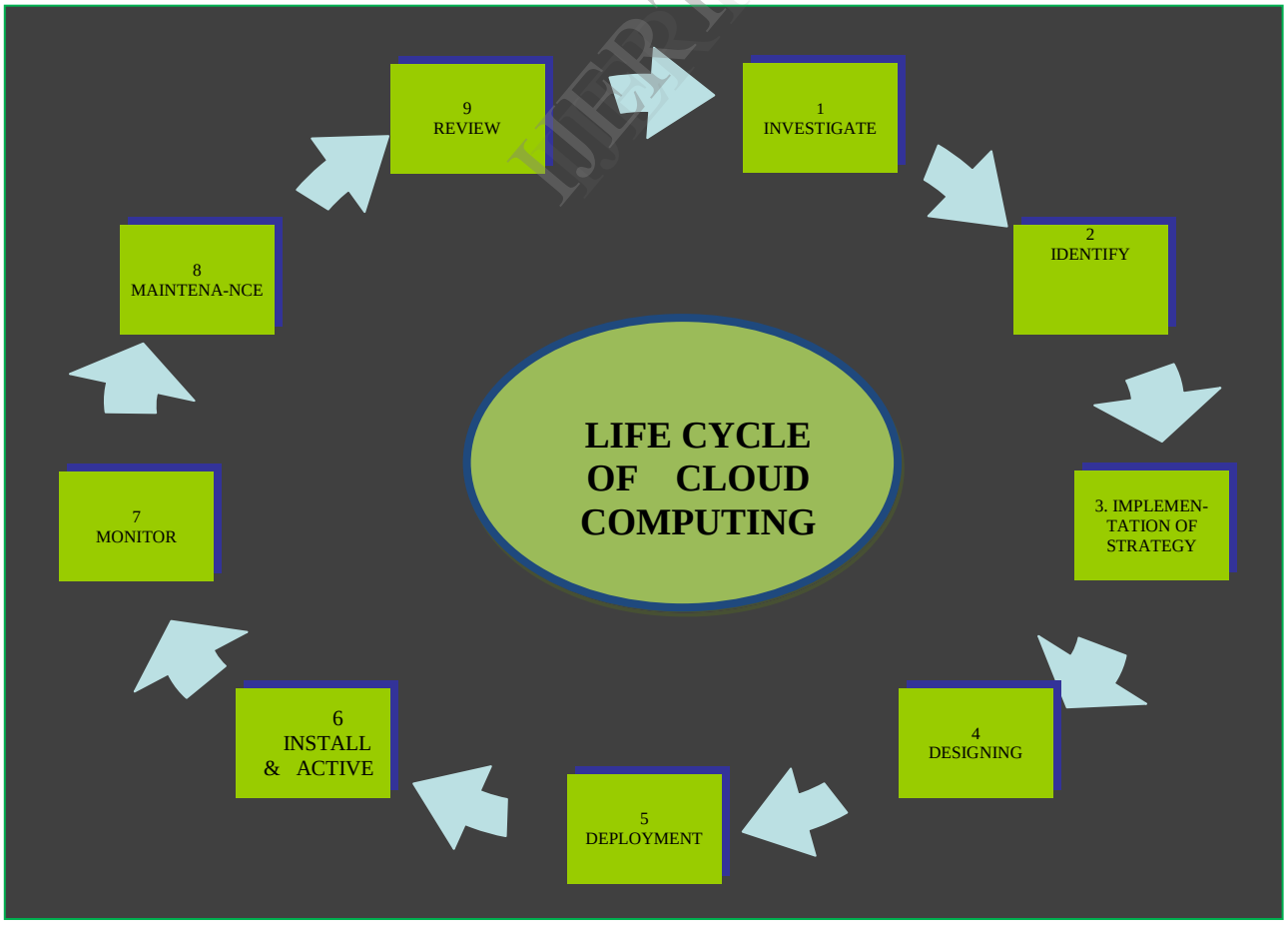

Fig 3: Life cycle of the cloud computing in nine simple steps.

In this we go for the update process replaces an earlier version of all or part of software system with new release.

Step 9: Review

Finally, once an application is not being used any longer, enterprise manager can be uninstall the application so that the resources can be used for other purposes, to prioritize and get approval to start a new cloud service project life cycle.

VII. CONCLUSION

As computing takes a step forward to cloud computing, we must pay attention to security issues of it. Because of security concerns, cloud computing is not concerned with some users. In this paper, security concern about data in cloud computing is categorized and discussed. This paper provides the complete open and unified portfolio of products to build, use and manage public and private cloud can make cloud computing fully enterprise – grade and support cloud computing to give versatility to users.

We believe that cloud computing is disruptive change for few enterprises and it can proved as feasible option for IT companies.

REFERENCES:

[1] D.L.G.FILHO and P.S.L.M.BARRETO, "Demonstrating Data Transfer," Cryptology Print Archive, Report 2006/150,2006,http://eprint.iacr.org.

[2] Cloud Computing Security, May 2010.

[3] Wikipedia,http://en.wikipedia.org/wiki/cloud_computing [accessed july 20,2009].

[4] A. Costanzo, M. Assuncao, and R. Buyya, "Harnessing Cloud Technologies for a virtualized Distributed Computing Infrastructure", IEEE Internet computing, Sept, 2009.

[5] J. Viega, Mcafee, "Cloud Computingand tha common Man";Published by IEEE Computer Society 0018-9162/09/$26.00 copyright 2009 IEEE.

Julia Allie et al., Security for information Technology Services Contracts, CMU/SEISIM-03, Software Engineering Institute, Carnegie Mellon University, January 1988, <URL: http