ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 9, September 2016

A Detailed Survey on Cloud Computing

[1] P.Smitha [2] G.P. Arvind Kumar [3] V.Ganesh Kumar
[1] Assistant Professor [2][3] Student
[1][2][3] Department of CSE, Velammal Engineering College, Chennai
[1] smithaps.ap@gmail.com [2] arvindkumargp21@gmail.com [3] maliksalim506@gmail.com

***Abstract:* — the theme underneath this paper is based on a survey of cloud computing, the way how it is, the way how it can be and finally, the way how it should be. Cloud computing is one of the fastest growing computer and network related sectors whose usage can cause much benefit .It totally depends on internet to deliver its services to the users. It also includes security, privacy, and internet dependency and availability as avoidance issues. This paper puts forth some of the suggestions that may arise in future for a more secured environment of cloud computing resources.**

I. INTRODUCTION

Cloud computing **[1]** uses internet and central remote servers to maintain data and applications. Next generation networks and service infrastructures should overcome the scalability, flexibility, resilience and security bottlenecks of current network and service architectures, in order to provide a large variety of services and opportunities, adoptable by business models capable of dynamic and seamless utilization of IT resources based on user- demand.The cloud model provides three types of services**[2]:**

Software as a Service (SaaS) - SaaS reassign programs to millions of users all the way through browser. For user, this can save some cost on software and servers. For Service provider's, they only need to maintain one program, this can also saves space and cost.

Platform as a Service (PaaS) – PaaS is an application development and deployment platform provided as a service to developers over the Web.

Infrastructure as a Service (IaaS) - IaaS is the delivery of associated software and hardware as a service. Hardware like server, storage, network, and associated software like operating systems, virtualization technology and file system are associated.

Public Cloud: The Public Cloud allows systems and services to be easily accessible to the general public. Public cloud may be less secure because of its openness, e.g., e-mail.

Private Cloud*:* The Private Cloud allows systems and services to be accessible within an organization. It offers increased security because of its private nature.

Community Cloud*:* The Community Cloud allows systems and services to be accessible by group of organizations.

Hybrid Cloud: The Hybrid Cloudis mixture of public and private cloud. However, the critical activities are performed using private cloud while the non-critical activities are performed using public cloud. The Cloud Computing architecture comprises of many cloud components, each of them is loosely coupled.**[3]**

Advantages: These include access to completely different levels of scale and economicsin terms of the ability to scale very rapidly andto operate IT systems more cheaplythat previously possible.By 2020 we can expect communications in the datacenter to be "running at a speed in the low hundreds of gigabits per second".

Disadvantages*:* Requires a constant Internet connection. A dead Internet connection means no work, when you're offline, cloud computing simply doesn't work. Stored data might not be secure. With cloud computing, all your data is stored on the cloud. Theoretically, data stored in the cloud is unusually safe, replicated across multiple machines.

II. CHALLENGES

The current adoption of cloud computing is associated

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 9, September 2016

with numerous challenges because users are still skeptical about its authenticity. The major challenges are

***A. Security*:** It is clear that the security issue has played the most important role. There exists no doubt that putting your data, running your software on someone else's hard disk using someone else's CPU appears daunting to many. Well known security issues such as data loss, phishing, botnet pose serious threats to organization's data and software.

B. Costing Model: Cloud consumers must consider the tradeoffs amongst computation, communication, and integration. While migrating to the cloud can significantly reduce the infrastructure cost, it does raise the cost of data communication.

***C. Charging Model*:** The elastic resource pool has made the cost analysis a lot more complicated than regular data centers, which often calculates their cost based on consumptions of static computing.

D. Service Level Agreement (SLA): Although cloud consumers do not have control over the underlying computing resources, they do need to ensure the quality, availability, reliability, and performance of these resources.

E. Cloud Interoperability Issue: Currently, each cloud offering has its own way on how cloud clients/applications/users interact with the cloud, leading to the "Hazy Cloud" phenomenon.

III. METHODS FOR SOLVING SECURITY ISSUES

Asymmetric cryptography uses public and private keys to authenticate to the system or encrypt/decrypt the data in transit. The public key can always be shared with the public as it is used for the data encryption, while only the private key can decrypt the data.

Use password protected keys It's important to select a strong password when generating a private key to protect it from unlawful use.

Back up keys: Creating backups is a good idea when you rely on a number of public/private key-pairs to authenticate to the cloud-based services. It's advisable to choose at least a 4096-bit key, which is currently considered secure as it contains enough possibilities to prevent the attacker to brute-force the passwords in real time.

***Fragmentation-redundancy-scattering (FRS) technique*:** It aims to provide intrusion tolerance and, in consequence, secure storage. This technique consists in first breaking down sensitive data into insignificant fragments, so any fragment does not have any significant information by itself.

***Homomorphism encryption*:** Encryption techniques can be used to secure data while it is being transferred in and out of the cloud or stored in the provider's premises. Cloud providers have to decrypt cipher data in order to process it, which raises privacy concerns. Fully homomorphism encryption allows performing arbitrary computation on cipher texts without being decrypted. Current homomorphism encryption schemes support limited number of homomorphism operations such as addition and multiplication.

Message Digest Algorithm: Message digest functions which are also called as hash functions, used to generate Digital Signature of the information which is known as message digest. MD5 algorithm is used to implement integrity of the message which produce message digest of size 128 bits. Message digest algorithm yields two advantages. Identical messages always generate the same message digest and even if one of the bits of the message changes, then it produce different message digest. The other advantage is that message digests are much shorter than the document from which digests are generated. It processes the message and generates 128- bits message digest.

RSA Algorithm [6] RSA is Public-Key algorithm. It has been developed by Ron Rivest, Adi Shamir and Len Adleman in 1977. We use RSA algorithm to encrypt the data so that no unauthorized user access it. User data is first encrypted and then it is stored in the Cloud. RSA is like a block cipher, where every message is mapped to an integer.

IV. SECURITY ISSUES[7]

The economic case for cloud computing has gained widespread acceptance .Cloud computing providers can build large datacenters at low cost due to their expertise in organizing and provisioning computational resources. First, data and software are not

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 9, September 2016

the only assets worth protecting. Activity patterns also need to be protected. Sharing of resources means that the activity of one cloud user might appear visible to other cloud users using the same resources potentially leading to the construction of covert and side channels. Activity patterns may also themselves constitute confidential business information, if divulging them could lead to reverse-engineering of customer base, revenue size, and the like.To alleviate these concerns, a cloud solution provider must ensure that customers will continue to have the same security and privacy controls over their applications and services. Some of these vulnerabilities are the following:
Security of enterprise data that stored in the cloud, risk of lock-in to cloud platform vendors, loss of control over cloud resources run and managed by someone else, and reliability.

Lack of security education - people continues to be a weak point in information security. This is true in any type of organization; however, in the cloud, it has a bigger impact because there are more people that interact with the cloud: cloud providers, third-party providers, suppliers, organizational customers, and end-users. Data can also be moved from one location to another, therefore cloud provider should ensure security of information.

V. CONCLUSION AND FUTURE WORKS:

The main reason for possible success of cloud computing and vast interest from organizations throughout the world is due to the broad category of services provided with cloud. There are many challenges to be addressed by the researchers for making cloud computing work well in reality. Some of the suggestions that could be worked upon in future for improved security and protection of data are:

(i) Two rational numbers can be used instead of prime numbers in case of generating the 4096 bit key. Rational numbers doesn't end easily and it becomes a tedious process in identifying them.

(ii) Clouds can be limited in the sense based on the type of data and same kind of data need to be identified and gathered under a main cloud which in turn must be given a special protection. This helps in a way that if one kind of cloud gets attacked, the others can be made cautious and protected.

(iii) There must be an intermediate software between the data and cloud which could analyze the kind of data need to be boarded onto the cloud.

(iv) Clouds with personal data should be localized to regions and must be given a limited space to move across the internet. So that even if gets attacked by someone, it will be easy enough to locate the attacker. There is a need to focus on privacy and on solutions of various security problems to maintain the trust level of organization for deploying the cloud computing without any hesitation and also need of technical support for elastic scalability to serve by vertical scaling approach which is currently restricted to only horizontal scaling. However, new security techniques are needed as well as redesigned traditional solutions that can work with cloud architectures.

REFERENCES

1. Thomas Erl , Cloud Computing: Concepts, Technology & Architecture, Published May 2013

2. Michael J. Kavis , Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, & IaaS), Published January 2014

3. Raghuram Yeluri, Building the Infrastructure for Cloud Security, Published March 2014

4. Hongwei Li, Yuanshun Dai, Ling Tian, and Haomiao Yang, Identity-Based Authentication for Cloud Computing

5. Sudhansu Ranjan Lenka, Biswaranjan Nayak , Enhancing Data Security in Cloud Computing Using RSA Encryption andMD5 Algorithm, Trident Academy of Technology.

6. Suruchee V.Nandgaonkar, Prof. A. B. Raut, A Comprehensive Study on Cloud Computing

7. M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, On Technical Security Issues in Cloud Computing. IEEE, 2009