COPY RIGHT

IJIEMR Transactions, online available on 15th JUN 2018. Link :

http://www.ijiemr.org/main/index.php?vol=Volume-07&issue=ISSUE-06

Title: **AN INTRODUCTION TO CLOUD COMPUTING**

Volume 07, Issue 06, Pages: 155–162.

Paper Authors

K.SRINIVAS, DR. JOSEPH PRAKASH MOSIGANTI

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

AN INTRODUCTION TO CLOUD COMPUTING

[1]K.SRINIVAS, [2]DR. JOSEPH PRAKASH MOSIGANTI

[1]Assistant Professor Holy Mary Institute of Technology & Science

[2]Professor, CSE Department MCET, Hyderabad

ABSTRACT

Nowadays, access control and data security are two most critical problems with cloud computing. Access control can be defined as a procedure by which users can access data from the cloud server. At the time of accessing data, there are many problems, such as data security, high data accessing time, data lost, overhead, data redundancy, etc. In the first part of this paper, a brief discussion of fundamentals of cloud computing are presented. Moreover, all the issues of cloud computing are also discussed in this paper. Finally, future work directions have been identified for the cloud computing environment.

1. INTRODUCTION

Cloud computing has been an important issue in recent years , is a term of a high performance computing , cloud computing make internet as a big storage to store a data and resources , users can access to resources by using internet , the main aims of cloud computing is reducing costs and proceed a complex tasks , cloud computing is providing users multi benefit consist of high performance processing , sharing resources , scalability, ease of use ,fault tolerance , cloud computing having disadvantages including availability ,dependability and security and privacy issues .

1.1. Cloud computing

The services can provide by service providers are consist of software as a service, platform as a service and infrastructure as a service , users can access to the internet and use cloud services [13],[6],[3]. The deployment models of cloud computing Private cloud user can create an own private cloud to interconnection with their data and other resources, while a Public cloud defined as resources are provided a according to the basis of service, for example: internet sales, Community cloud enable multiple environments for sharing the cloud infrastructure and resources And Hybrid cloud is more than cloud that connected together, and that will create a large community cloud to provide service for environment.

1.2. Cloud computing characteristics

Broad Network Access: users can access to cloud computing from anywhere and at any time using less disk device,

Rapid Elasticity: It is very easy to scale up or down the resources at anytime, 3.3 Shared Resource Pooling : users can share the cloud resources,

International Journal for Innovative Engineering and Management Research
A Peer Reviewed Open Access International Journal

www.ijiemr.org

On demand services : uses of cloud resources at anytime from users ,

Multi-tenancy : users can access to multiple services provide by multiple service providers

Maintenance : cloud service providers maintenance cloud system and services

measured service : cloud computing resources usage controlled by cloud service provider and can be measured and monitoring [10] , [9] ,[7].

Cloud computing is emerged as a modern technology which developed in last few years and considered as next big thing in years to come. In recent years it has grown up from just being a concept to major part of IT industry. Cloud computing provides a distributed computing environment comprises of heterogeneous components like hardware, software, firmware, networking as well as services. It changed the entire process that distributed computing used to present e.g Grid computing, server-client computing. Cloud computing describes recent developments in many existing IT technologies and separates application and information resources from underlying infrastructure.

Cloud computing generally works on three type architecture namely

1. SaaS (Software as a Service).
2. PaaS (Platform as a Service).
3. IaaS (Infrastructure as a Service).

There are different issues and concerns with each of the cloud computing technology

SaaS (Software as a Service):

- Hosts and manages a given application in their data Centre and makes it available to multiple users over the web.
- Examples of SaaS are Oracle CRM on Demand and salesforce.com.

PaaS (Platform as a Service):

- Application development and deployment platform which delivere over the web to developers.
- Facilitates development and deployment of applications without the cost and complexity of buying and managing the underlying infrastructure.
- All of the facilities required to support the complete lifecycle of building and delivering web applications and services entirely available through internet.
- Includes database, middleware, development tools and infrastructure software.
- Paas service providers include Google App engine and Engine Yard.

IaaS (Infrastructure as a Service):

- Delivery of software and hardware as a service.
- It is a traditional hosting that does not require any log term commitment and allows users to provision resources on demand.
- Amazon web services elastic compute cloud (EC2) and secure storage service (S3) are examples.
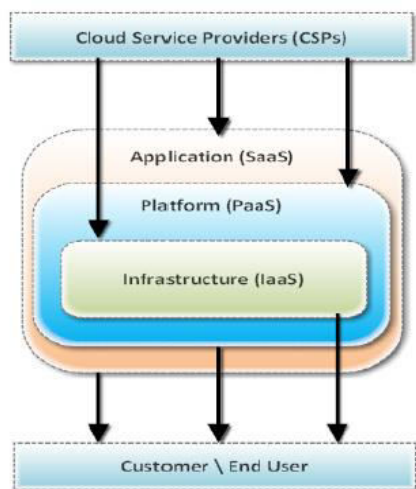
Cloud computing faces a lot of different challenges. Security is one of the key challenges. Security problems can cause great loss, even devastating blow. Therefore to make the enterprise and the organization accept cloud computing services, it is necessary to solve security peoblems.

Advantages of cloud computing

☐ **Lower computer costs:** As the cloud computing are web based, and are run in the cloud desktop PC, lap-tops, tablets does not need the processing power or hard disk space .

☐ **Improved performance**: Computers in a cloud compu-ting system boot and run faster because they have fewer programs and processes loaded into memory.

☐ **Reduced software costs**: Instead of purchasing licensed software applications, it can be accessed for free.

☐ **Unlimited data storage capacity and increased data reliability:** A computer in the cloud can store hundreds of Petabytes of data in the cloud and crashing in the cloud does not affect the storage of data.

☐ **Universal document access**: Document stay in the cloud, and can be accessed through an Internet connec-tion

☐ **Device independence**: Changes to computers, applica-tions and documents follow you through the cloud.

2. RECENT WORKS:

Various authors proposed different frameworks to detect and stop large number of attacks which are discussed below

- Authors proposed a generic management framework which allows the providers to enforce complex security policies. They designed a expressive policy description language to be easily interfaced with various data management systems. They efficiently protected a data storage system by evaluating their security framework on top of BlobSeer data management platform.

- Other work investigated the problem of assuring customer integrity. In order to provide a way for the user to check his integrity the authors provided a scheme. This proof can be agreed up on by both the cloud provider and customer and can be in corporated in the service level agreement.

- Authors suggested four methods for cloud security and privacy which are
  1. Access control method which is an application of Role Based Access Control (RBAC).
  2. Policy integration method which is a dynamic policy control mechanism.

3. Identity management method which prevents the un authorizes secondary usage of data.

4. User control method which solves the problem of cloud users losing control of their data.

- Authors focused on technical security issues such as VM-Level attacks, isolation failure, management interface, compromise and compliance risks. They proposed a cloud security architecture using which organizations can protect themselves against threats and attacks. The key points for architecture are single-sign on, increased availability, single management console and virtual machine protection.

3. ATTACKS ON CLOUD COMPUTING:

- **Zombie attack**
  Mitigation: Better authentication and authorization and IDS/IPS can provide protection against such attack.

- **Service injection attack**
  Mitigation: Service integrity checking module should be implemented. Strong isolation between VMs may disable the attacker from injecting malicious code in the neighbor's VM.

- **Attacks on virtualization**
  Mitigation: By monitoring through IDS (Instruction Detection System)/IPS (Intrusion Prevention System) and by implementing firewall.

- **Man in the middle attack**

**Mitigation:** Proper SSL configuration and data communication tests between authorized parties.

- **Metadata spoofing attack**
  Mitigation: Information about services and applications should be kept in encrypted form. Strong authentication should be enforced for accessing such critical information.

- **Back door channel attack**
  Mitigation: Better isolation and authentication between VMs can provide protection against such attacks.

4. PROPOSED SECURITY MODEL:
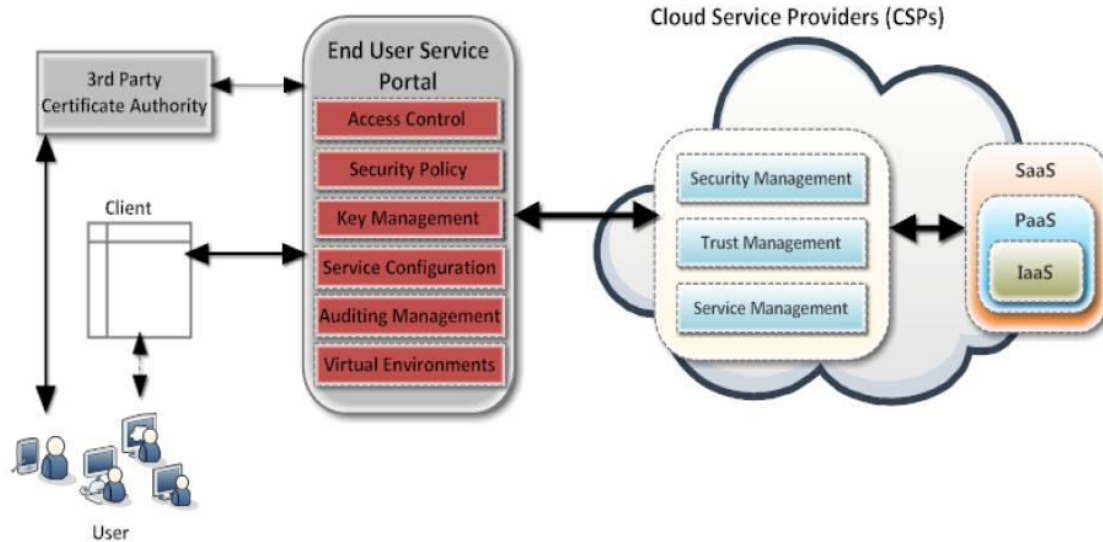
Based on all the threats described above this security model is constructed. User can be certificated by the 3rd party certificate authority, then can be issued token for service by End User Service Portal. After joining service portal, user can purchase and use cloud services which are provided by single service provider. End User Service Portal which is composed access control, security policy, key management, service configuration, auditing management, and virtual environments provides secure access control using Virtual Private Network (VPN) and cloud service managing and configuration.

5. FRAMEWORK FOR SECURE CLOUD COMPUTING

Framework for secure cloud computing is based on the security model shown above which describes the details of each component and apply the needed security technologies for implementation between components in cloud computing. Access control process on each component is as follows:

- **Client:** users could access the client side with multi factors authentication provided by End-User Service Portal. Multi factors authentication based on certification issued by 3rd party certification authority.

- **End-User Service Portal:** when clearance is granted, a single Sign-on access token (SSAT) could be issued using certification of user. Then the access control component share the user information related with security policy and verification with each other components in end-user service portal and cloud service providers by using XACML and KIMP.
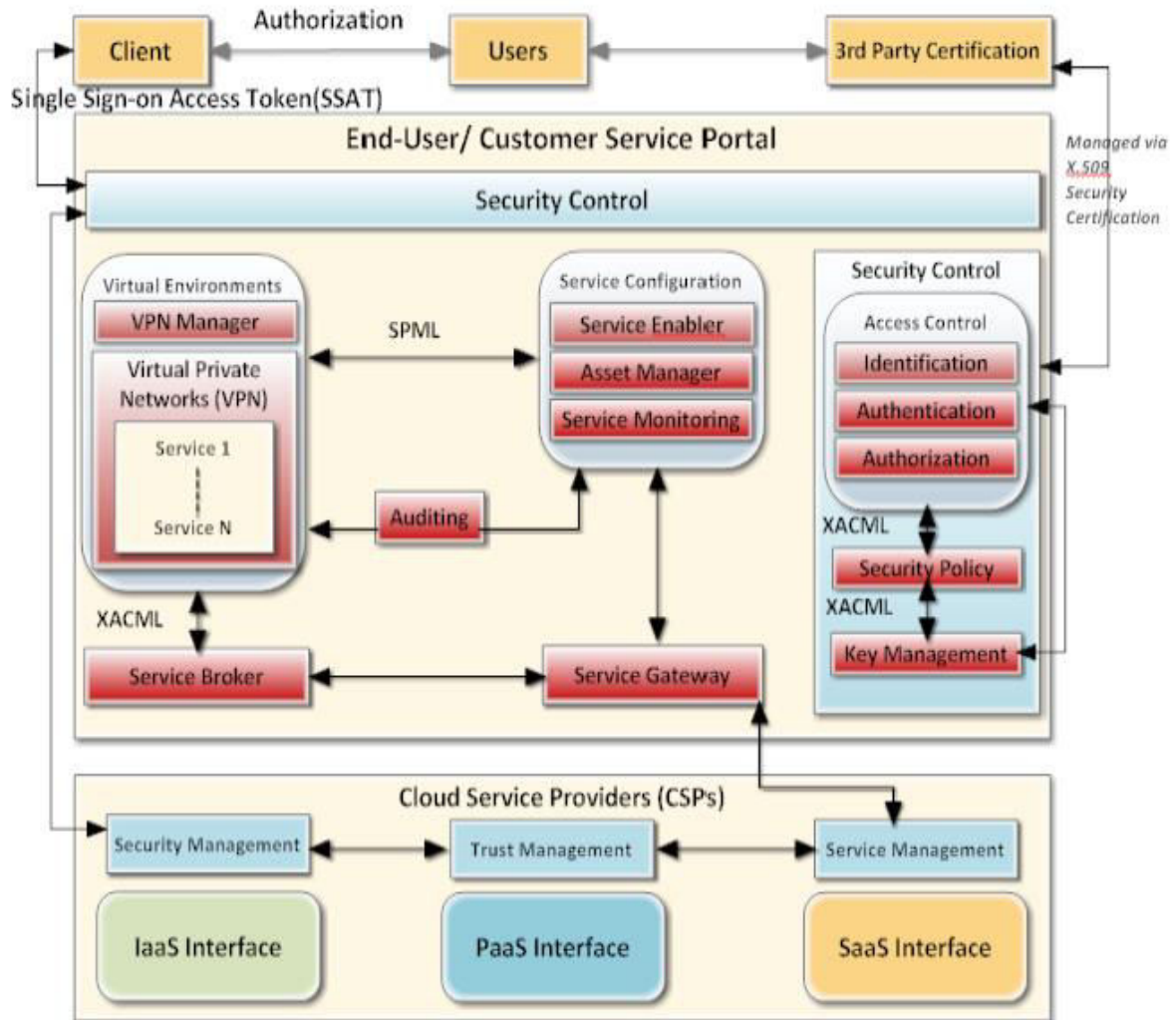
- **Single Sign-on:** Users may have multiple accounts on different cloud services with same user name and password which poses inherent security risks. To overcome this problem, it is suggested that, to streamline security management and implement strong authentication with in the cloud.

- **Service Configuration:** The service enabler makes provision for personalized cloud service using user's profile for the integration and interoperation. The SPML can be used to share user's profile. The asset manager requests user's personalized resources with SPML to cloud service provider and configuration service via VPN connection.

- **Service Gateway, Service Broker:** Service gateway manages network resources and VPN on the information life cycle of service broker.

- **Service Control:** The security control component provides significant protection against

security threats. Based on the providers access control needs various access control models can be used. Role Based Access Control (RBAC) has been widely accepted as the most promising access control model.

- **Security Management:** Provides the security and privacy specification and enforcement functionality. The authentication and identity management module is responsible for authenticating users and services based on credentials and characteristics.

- **Trust Management:** Due to the cloud's nature i.e service oriented, the trust level should also be integrated with the service. One possible approach is integrated with service, and bidirectional.

- **Service Monitoring:** An automated service monitoring systems to guarantee a high level of service performance and availability.

3.Applications of Cloud Computing for Rural development: The concept of cloud computing with internet must be infused into the rural areas through PCs, laptops, notebooks, tablets or mobile phones etc. connected to cloud so that the information is available to the poorest of the poor giving them a better life.

1. Education: Rural education in CG is facing problems like lack of qualified teachers, lack of IT institutes with proper infrastructure and teaching facilities, lack of involvement in and control of educational matters and difficulties of stu-dents in higher education [4]. Lack of IT study institutes in

rural areas because of the huge amount of money spent on buying software licenses, setting up proper infrastructure is required for computation, storage etc.
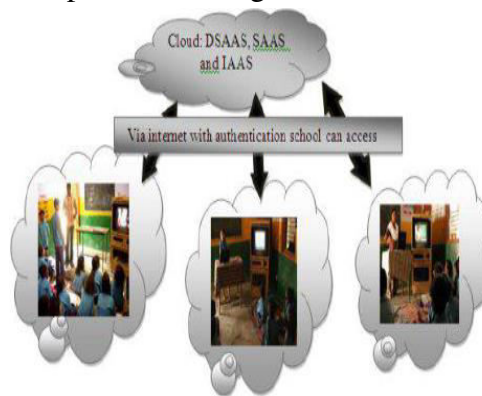

Fig.4 Cloud computing model for e learning

The three fundamental services offered by cloud computing i.e. IaaS, PaaS and SaaS will reduce the total expenses on setting up an IT institute by huge amount because:

☐ There is no need to buy expensive software licenses when they can pay for it on a pay-per cycle basis whether it is software.

☐ There is no need to setup huge and expensive infra-structure (such as high speed processing computers or huge data storage devices) when they can use these re-sources from the cloud providers.

☐ There is no cost involved in procuring and maintenance of infrastructure- mainly software and hardware.

CONCLUSION

Cloud computing, is a new style of computing technology depend on PAY AS YOU GO principle , users can use cloud resources and entering to system with less disk device and deal with cloud resources to using system benefits , provides users multiple benefits and characteristics , cloud computing has many disadvantages and

challenges become future researches and studies , In this paper we discussed the cloud computing models , benefits , obstacles, and focused on challenges and characteristics of cloud computing .

REFERENCES

1. Peter Mell and Tim Grance, ― The NIST Definition of Cloud Computing, NIST Report, July 2009 Recommen-dations of National Institute of Standards and Technol-ogy.http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

2. Shaily Malik *et al.,* "Cloud Computing - A Hope For The Rural India", International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 20,2010

3. Micheal Miller, Cloud Computing, 2008, Edition

4. Cloud Analyst http://www.cloudbus.org/cloudsim

5. Piracy rates in India http://www.bsa.org/country.aspx

6. Gmail,http://www.technopulse.com/2011/06/cloud-service-models-saas-paas-iaas.html

7. G. Gruman, "What cloud computing really means", In-foWorld, Jan. 2009

8. www.joyant.com, Performance and scale in cloud com-puting, A Joyant white paper, 2010

9. http://en.wikipedia.org/cloud_computing