# Research in Cloud Computing–An Overview

**Article** *in* International Journal of Distributed and Cloud Computing · January 2015

DOI: 10.21863/ijdcc/2015.3.1.002



**2 authors:**

Vijayarani Mohan
Bharathiar University
**95** PUBLICATIONS **1,419** CITATIONS

SEE PROFILE

s. Sharmila Sathyanathan
Bharathiar University
**2** PUBLICATIONS **2** CITATIONS

SEE PROFILE

Article can be accessed online at http://www.publishingindia.com

# Research in Cloud Computing-An Overview

**S. Vijayarani Mohan*, S. Sharmila Sathyanathan****

**Abstract**

Cloud computing is an Internet based resource sharing which trigger broad network access. This cloud computing technology is a new technology which delivers a new model for information and services by means of an existing grid computing technology. Further, this new technology uses Internet infrastructure to communicate between the client and the server side service applications. Apart from this, cloud computing has cloud service provider they offers cloud platform for their customers to create and use web oriented services. The hardware and software resource sharing is possible in cloud with the help of internet and it can be managed and maintained by the third party cloud service provider. The cloud service provider facilitates cloud computing to increase the capacity or add capability, for example without investing in a new infrastructure, training new people or licensing new software. It is packed with a new infrastructure to improve the services like scalability, elasticity, business agility, faster start up time, reduced management cost and availability of resources. This special Internet based shared resource has its own conceptual, technical, economical and user experience characteristics. Nowadays, cloud computing has become one of the most important and popular research areas in the field of computer science. Many open research problems are available in cloud computing and good solutions also been proposed by the researchers by developing new techniques and efficient algorithms. In this paper, a detailed study about cloud computing, its basic concepts, history, virtualisa tiontechnique, and cloud services are discussed. In addition to this, research issues in cloud computing also discussed.

**Keywords:** Cloud Computing, virtualization, Brokering Services, Research Issues, Security Issues

## Introduction

Cloud computing is a technology it delivers a new model form existing grid technology and based on internet resources sharing and broad network access Cloud computing model is composed of five essential cloud characteristics, namely on demand self-services, Broad network access, Independent resources pooling, Rapid elasticity, and Measured service, which include four deployment models such as private, public, hybrid, and community. Cloud computing has three service models namely PAAS, IAAS, SAAS. Cloud computing has rapid deployment which is used to speed up the time which fastens the workload. It also facilitates low start-up cost which includes the capital investment; costs based on usage or subscription, multi-tenant sharing services and resources, and accelerated deployment. This modern technology has massive scalability which has theability to scale the bandwidth and storage space of tens and thousands of systems and the elasticity users can increases a multi-tenancy.

Cloud computing is based on a business model in which resources are shared at the network, host, and application

* Assistant Professor, Department of Computer Science, Bharathiar University, Coimbatore, Tamil Nadu, India.
E-mail: vijimohan_2000@yahoo.com

** Ph.D Research Scholar, Department of Computer Science, Bharathiar University, Coimbatore, Tamil Nadu, India.
E-mail: sharmilasathyanathan@gmail.com

level. They decrease their computing resources as they needed. When the resources are not required for a longer time, they can release resources for other uses, such as self-provisioning where users can self-provision resources like additional systems and network resources. The significant advantages of cloud are cost reduction, storage space, highly automated flexibility, and more mobility. Apart from the advantages this technique have some disadvantages such as vital data storage, external server by external provider, lack of data security, lack of physical or local back up, Internet connection is needed to access anything even our own documents and the complete performance is based on the speed of the internet (Bhadauria & Sanyal, 2012).

The cloud computing payment is made as 'pay as you use', where the users can pay only for the resources they utilise and the time they require. Moreover, as the software is maintained by a third party the users are freed from installing the software and to run the application on their local compute (Gong, Liu, Zhang, Chen & Gong, 2010).

The remaining portion of the paper is organised as follows. The second section gives the history of cloud computing. Cloud computing models are discussed in third section. Fourth section describes the essential characteristics of cloud computing. Fifth section discusses virtualization concept in cloud computing. Sixth section gives the detailed description about brokering services in cloud computing, broker and coordinator secure cloud communication paradigms, and service level agreement. Seventh section presents few research issues and security issues of cloud computing. Eighth section analyses few controls and challenges of cloud computing. The last section concludes and discusses about future trends.

## History of Cloud Computing

In 1950s, cloud computing was introduced through the concept of mainframe computers. Large scale mainframes were used in institutions and organisations and enormous hardware infrastructure was installed. In cloud computing this infrastructure is known as server roomwhich contains a single mainframe and multiple users can access the mainframe through dumb terminal. In 1969, computer network was introduced; they enabled the development of ARPANET. In 1970s IBM released an operating system called virtual machine that allows admin on their system to have a multiple virtual system. In 1990s Telecommunication Company launched virtualised private network connection with the same quality of service at a reduced cost. During 1999, cloud computing was introduced with the new concept of delivering enterprise application through a simple website. In 2006, Amazon introduced EC2 a commercial website which promoted the rent of computers to individuals and small companies to run their own application.

There are many types of computer architecture among them the first one is centralised computing similar to the client server model (Neto, 2014). Computing is done at a central location using terminals that are connected to a central computer which controls all the peripherals directly. It runs on a single system and do not interact with other computers. Master card has been installed to perform all the functions of the system but, if the master card fails the system do not work, to overcome this problem parallel computing was introduced which consists of multiple disk and processor connected by a fast interconnection network. This parallel machine consists of few powerful processors measuring two performances like through put and response time. The main disadvantage of parallel computing is the need of high processor to speed up the processing. Considering this problem distributive computing was introduced to rectify the problems. Data is spread over the multiple machines and the interconnections are done on the machine by networking and shared by the user on multiple machines.

Distributed computing (Azcuy, 2009) is divided into four categories of system model-cluster, grid, peer to peer, and cloud computing. Cluster computing is a technique of linking two or more computers by LAN, consisting of tightly or loosely coupled computer that work together, but they can be viewed as a single system. They support high performance distributed computing, and provides faster processing speed, large storage capacity, and better data integrity. Developing software for distributing computing, loss of transmission is difficult task and is not secured. Hence, it moves on to grid computing and uses distributive computing which speed up the connection. This system is connected through WAN. Grid computing has two types data grid and compute grid. At this juncture comes the cloud computing to overcome all the problems but still cloud computing is facing security problem. Many researches are on process to solve this security issue (Neto, 2014). Table 1 gives the comparison chart which compares the cloud computing and grid computing concepts based on their characteristics.

**Table 1: Comparative Chart - Cloud Computing Vs Grid Computing**

| Characteristics | Grid computing | Cloud computing |
|---|---|---|
| **Aim** | Resources are shared in collaboration manner | Resources are shared upon use of service |
| **Level of abstraction** | Abstraction level is low | Abstraction level is high |
| **Scalability** | Degree of scalability is low | Degree of scalability is high |
| **Dependency** | Grid computing depends on grid certificate service so the security in grid computing is low | Cloud computing depends on virtualization so the security in cloud computing is high |
| **Flexibility** | Grid computing supports any standard operating system | Multiple operating system can run on cloud computing |
| **Load balancing** | Few number of user can use at a time Example GIMPS , SEIT | Many number of user can use at a time Example Google , face book |

## Cloud Computing Model

The cloud computing model consists of three service models, four deployments and two management models. Figure 1 shows the cloud computing model.

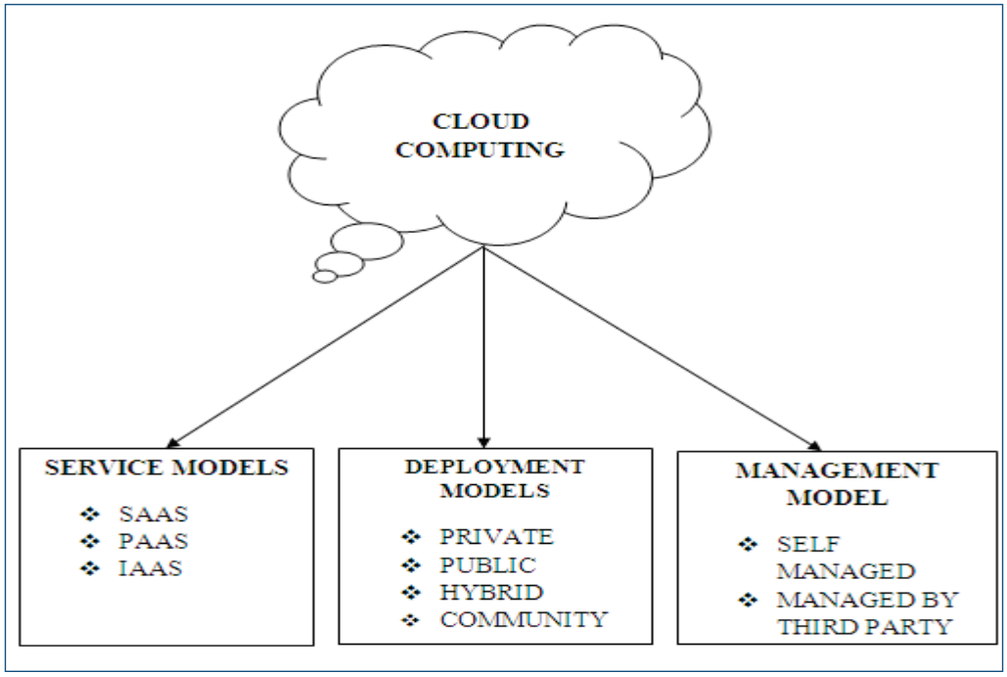
## Service Models

### SAAS – Software as a Service

SAAS is a software delivery model, which delivers application over the Internet. It allows the user to utilise various application software like MS-Word, mobile applications, image processing, paint, game application, and web browsers which are hosted on Internet, which is specially designed for end users. The access is based on network and the activities are managed from one location, which allows its users to access the applications remotely. These services are provided in SAAS for many online applications. The process of acquiring licence for the application software is expelled for the end users. The advantages of SAAS are highly secured, flexible, less installation cost, software is maintained by the cloud providers, reduced hardware, and operating system costs. For example, online shopping sites and mobile applications software run on one environment and are controlled by a provider.

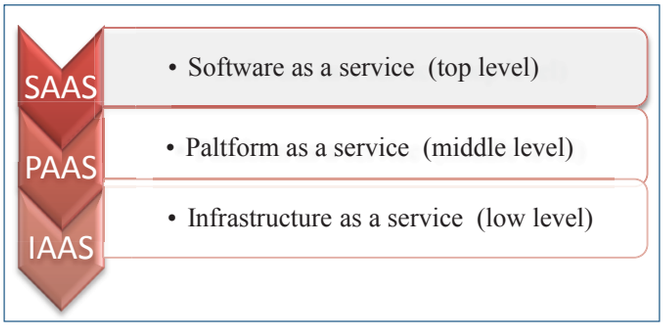
Few characteristics of SAAS are commercial software has internet access, software is managed from one location, it deals with one - many model, collaboration of a software which is used for specific projects (Neto, 2014). There are two mechanism used in SAAS; Divided Cloud and

**Figure 1: Cloud Computing Model**




Convergence Coherence. These two mechanisms provide the services for many online applications and which are used to reduce the traffic in network. It supports UNIX semantic when data is accessed in cloud computing. Every datum has read lock (Bhadauria & Sanyal, 2012) and write lock and when the read lock is obtained, user can store the data in local buffer and they can perform write operation without communicating with server when write lock is obtained (Mishra & Sudevalayam, n. d. ). There are two types of server in SAAS: "main consistence server" and "domain consistence server. "SAAS is used to reduce the cost of maintenance, storage, operating software, and hardware (Neto, 2014). Figure 2 shows the cloud computing service model.

**Figure 2: Cloud Computing Service Model**

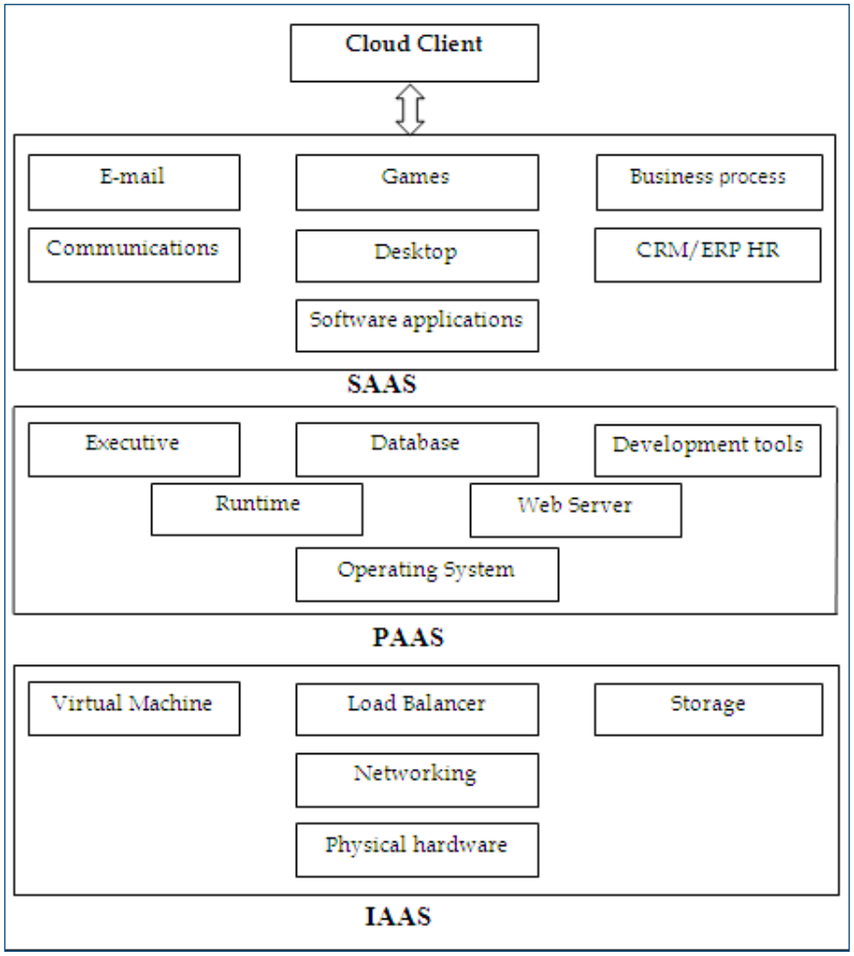



## PAAS-Platform as a Service

PAAS is responsible for managing the storage space, bandwidth allocation, and computing resources for the application. It is a group of tools and services designed together to write coding and implementing the application. Cloud service provider will take care of the disk space and the storage of data. The main role of PAAS is to protect data, without purchasing the actual software the users can access the software. Every time the operating system is upgraded and in addition they rent the operating system, storage space and resources via internet (Neto, 2014). New applications are developed from the existing one by renting server and services. Characteristics of PAAS are mainly used to test, implement, develop, and maintain applications. There are various types of PAAS-private PAAS and public PAAS.

Public PAAS is used to build the application delivered by the service provider, for example, Microsoft Azure delivered by the organisation is used to build Red Hat open shift, add-on development facilities, standalone development model, application delivery model, open PAAS, and mobile PAAS. In private PAAS, developers can run their application in minutes instead of weeks. Private PAAS is generally used in organisation because data are kept inside their own firewall on their own private

**Figure 3: Detailed View of Cloud Computing Service Models**




cloud. Few benefits of PAAS are flexibility, security, no physical structure investment, portability, scalability and availability (Pai & Jayalakshmi, 2013), and reduction of cost and complexity. The cloud user has control over the application and the security providers are split between the cloud provider and the user (Mishra & Sudevalayam, n. d. ). Figure 3 gives the detailed view of cloud computing service models.

## IAAS-Infrastructure as a Service

IAAS shares all the hardware resources for executing services. They dynamically scale bandwidth allocation and server resources for the cloud. They provide physical and virtual machine, and guest operating System. Users are charged for how much bandwidth or server they used on a pay-per-use basis; example, Amazon web services (Neto, 2014). The hypervisor supports the large number of virtual machines which scales up the services and the load balancer splits the work to the set of the virtual machine and it scales up the work and balances the load (Mishra & Sudevalayam, n. d. ). Important characteristics of IAAS are, they distribute resources as service and allow many users to access a single piece of hardware. IAAS can be divided into public and private cloud. It reduces the cost of maintenance.

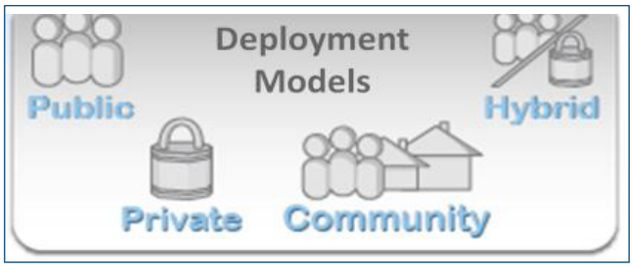
The cloud user has the freedom to choose the operating system and to develop the settings to be clouded. The provider manages the networking, virtualization storage and hard drives. Many providers deal with databases and messaging queues. Few models are used in IAAS name lyvirtual private IAAS, dedicated IAAS, private community IAAS and hybrid IAAS (Pai & Jayalakshmi, 2013).

## Deployment Models

### Private Cloud

Infrastructure of a cloud is available to a specific customer, operated and managed either by the organisation or a third party service provider; example, eucalyptus. Services are accessed within the specified area via intranet. The few advantages of the private cloud are information stored behind firewall; internet is not needed to isolate the infrastructure. User knows the exact location of the data. In case if cloud provider fails, private cloud will provide the service. The main disadvantages in private cloud is physical access is visible to all. Comparing to other deployment model private cloud is secured but more expensive (Neto, 2014). Figure 4 represents the cloud computing deployment model.

**Figure 4: Cloud Computing Deployment Model**




### Public Cloud

A cloud infrastructure is provided to many customers and managed by a third party. Many enterprises can work on the infrastructure at the same time. Resource wastage is checked as the user pay for whatever they use, for example Google. Few advantages of public cloud are, it protects from hardware failure, trouble- free and inexpensive frame work because everything is controlled by the cloud provider, no proper utilisation of resources (Mishra & Sudevalayam, n. d. ).

### Community Cloud

The infrastructure is shared by several organisations, when the requirements are same. It is managed by organisation or third party service provider, for example sales force. It may be managed and operated by two or more organisation in the community (Neto, 2014).

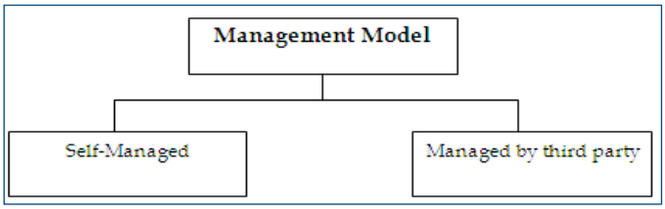
### Hybrid Cloud

Combination of two or more deployment model is known as hybrid cloud. The data should be transferred without affecting each other. Linking should be carefully done, for example Microsoft. Other model cloud computing provides distributed cloud, in which different machines are running at different location but are connected to the single machine or single hub. Multi-cloud or inter-cloud is an interconnection of cloud of cloud which is like networks of networks in the Internet (Mishra & Sudevalayam, n. d. ).

## Management Models

In cloud computing, resources are managed by two parties ethier self managed nor managed by third party. Figure 5 shows the cloud computing management model.

**Figure 5: Cloud Computing Management Model**




## Essential Characteristics of Cloud Computing

### On-demand Self Services

Computing capabilities are automated. Users can access their own resources as they needed without human involvement. Users are allowed to configure and manage the services.

### Broad Network Access

Services are available on internet which can be accessed from multiple devices like desktop, PDAs, mobile phones, tablets and laptops (Neto, 2014). Figure 6 tells about cloud computing characteristics.

### Independent Resources Pooling

They provide pooled resources to multiple clients. The physical and virtual resources are allocated and reallocated according to the user demand.

### Rapid Elasticity

Speed up the process and balances the load. Scaling is automated it scales up the work (Pai & Jayalakshmi, 2013).

### Measured Service

Pay per use model is used. It costs only for how much it's used. The usage is measured and crystal clear reports are maintained (Mishra & Sudevalayam, n. d. ). Cloud computing characteristics are depicted in Figure 6.

**Figure 6: Cloud Computing Characteristics**


## Virtualizations

Virtualizations is the back bone of cloud computing. The basic idea of cloud computing is to separate the application and operating system from hardware server. There are two types of virtualizations namely full virtualizations and para virtualizations. In full virtualizations , anentire installation is done on one machine, if the machine is failed, it can run on another machine. Paravirtualizations allows many operating systems to run on a single hardware device simultaneously (Anthony *et al*, 2009). Software can be installed in virtual server that allows multiple instances and guest Operating system and it can run on physical server. When power supply failure occurs, the access will be denied and virtualizations is used to rectify the problem.

When operating system or application fails it will migrate to another operating system and application stored in another hardware server and balances the load.

Virtualizations brings security concerns for customers or tenants of a public cloud. It can alter the relationship between operating system and underlying hardware. Virtualizations must be properly configured managed and secured (Jansen & Grance, 2011). It provides an environment which is able to render all the services being supported by a hardware that can be observed on a personal computer to the end users. Virtualizations in process can be applied in different places such as server virtualizations, storage virtualizations, application virtualizations and network virtualizations (Mishra & Sudevalayam, n. d. ).

**Figure 7: Virtualization Architecture**

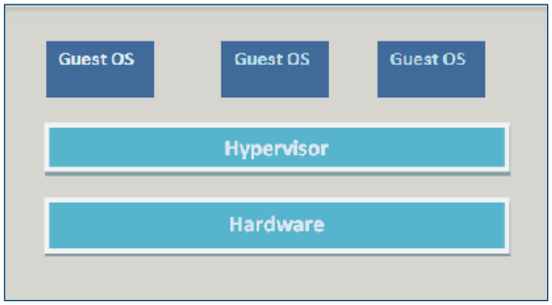



Figure 7 represents the virtualizations architecture with client installed virtualizations software and hypervisor. Hypervisor is very powerful comparing to client installed virtualizations software. It is linked with management software through networks. Hypervisors are categorised into two types. Type 1 Bare-metal hypervisoris directly installed on the x86-based hardware. A bare-metal hypervisor has direct access to the hardware resources. Secondly (Wayne *et al*, 2011) Type 2 Hosted hypervisor is installed and runs as an application on top of an OS.

Since it is running on an operating system, it supports the broadest range of hardware configurations. There are two types of virtual machines, 1. process view of machine and 2. system view of machine. Few benefits are virtual machine migration, scalability, load balancing, and security. There are three virtual machine techniques name lybinary translation, para-virtualizations, and hardware supported virtualizations (Gampala, Inuganti & Muppidi, 2012).

## Brokering Services in Cloud Computing

Cloud computing architecture brokering services plays an important role. The brokers provide services to the end user. Many researches are done on cost effective management

system. Secured cloud communication paradigm is usedto find the minimum cost of communication link. Broker cloud communication paradigm is used to find the cloud providers. The two algorithms are used to rectify some security issues namely secured optimised route cost finder and secured optimised route management. Secured optimised route cost finder which finds the optimum solution between broker and cloud and other one secured optimised route management which maintains the optimum route. In broker cloud communication link route discovery protocol is used and they follow the defined steps. In first step it sets the path between source node and the destination node and finds the route for request packet. Secondly, each intermediate node updates the information and sends it to the next node. Thirdly, the route request packet reaches to the destination node it sends back the route response packet in the reverse route as defined in the route request packet. In fourth step, secured dynamic source protocol will authenticate and verify the information and establish the route.

Broker cloud communication paradigm (BCCP) is helpful to understand the backend communication which the client cloud exchanges and broker (Raj & Kaur, 2012). Client should identify the task specification, usage and budget; they should be capable of taking decisions. Broker should manage the secured work between client and the broker and other cloud. Cloud exchange should update all information clearly and they can update service level agreement, conditions, cost parameter and usage costs etc. in free data centre. In data centre system efficiency can be improved using performance overhead techniques like power aware scheduling techniques. Cloud coordinator should be defined with the works and responsibility; they should handle security issues, work flow management, load balancing, variable resource management, live migration, and minimal virtual machine design. Communication links are used to communicate between client and broker. Communication links are classified into four types, i. e. service developer and service provider, service client and service provider, service provider and cloud, and cloud and resource provider (Kaur & Raj, 2013).

## Broker and Coordinator Secure Cloud Communication Paradigms

There are three secure cloud communication paradigms; they are, secure developer broker communication, secure user broker communication, and secure broker cloud communication paradigms. In secure developer broker communication, the developer has to find the availability resource from the cloud. They have to deal with the resources and SLA terms and conditions and request for suitable resources to develop services. When the developers signs in the SLA, broker searches for suitable resources. Developers request for the communication link. The broker accepts the request and provides the secured communication link, broker will manage the resources and allocation. The developer has to register with broker for profit making benefits. In secure user broker communication paradigm, registered user has to give specified requirements to search for the specific resources for specific task. Broker searches for the resources deliver to the user. They suggest special services like financial and time analysis. The user will select the service signs in the SLA and requests for the secure communication link (Raj & Kaur, 2012).

Secure broker cloud communication is broadly divided into three communication link scenarios namely broker–cloud exchange communication, cloud exchange–cloud coordinator communication, and broker–cloud coordinator communication. In the first scenario broker-cloud exchange communication, broker searches for the free data centre with the specific requirements. Cloud exchange will deliver the information and the broker request for secured communication link (Singh & Raj, 2012). The cloud exchange will provide the secured link and closes the link. In the second scenario cloud exchange-cloud communication, the cloud exchange will request cloud coordinator to update the information, they update the information and services. The third scenario broker-cloud coordinator communication, tells about the communication between the coordinator and the broker, broker requests for the services and cloud coordinator asks for the authentication. When the authentication procedure is completed they provide the service (Kaur & Raj, 2013).

## Service Level Agreement

SLA is an agreement between the client and the provider. SLA includes address, defined services, measured performance, problem management, assurance, customer duties, disaster recovery, and termination of SLA. SLAs are defined at different levels. Customer-based SLA is an agreement between the single customer group. Service-based SLA is an agreement between customer and the

services provided by the service provider. Mult-ileve lSLA split into different levels but different set of customer has same SLAs and same services. Corporate-level SLA includes all common service level management.

Customer-level SLA includes service level management issues related to the particular customer group and the services. Service-level SLA includes service level management issues related to the particular services and the particular customer group. Service level agreement is one of the major issues in cloud computing. SLA manager is responsible to manage the SLA templates. Loss of governance SLA may not offer commitments to provide such services on the part of the cloud provider they leave the gap in security defences (Singh & Raj, 2012).

## Research Issues in Cloud Computing

1. Infrastructure security
   - Network level
   - Host level
   - Application level
2. Data security and storage
3. Identity and access management
4. Privacy
5. Security issues
   - Physical security
   - Operational security
   - Programmatic security
6. Data issues
   - Data backup
   - Data usage
   - Data loss
   - Data integrity
   - Data theft
7. Performance issues
8. Energy related issues
9. Bandwidth related issues
10. Design issues
    - Energy management
    - Novel cloud architectures
    - Software licensing
11. Reliability
12. Legal issues
    - The physical location of your data
    - Responsibility of your data
    - Intellectual property rights

## Security Issues in Cloud Computing

Security issues are either faced by the cloud providers or their customers. The provider must ensure the protected data and application; provider should take proper security measures to protect their information. There are several security issues in cloud computing, some of the important security issues are data security, storage security, network security, security in virtualizations (Bhadauria & Sanyal, 2010). These issues are rectified using few technologies like virtualizations, operating system, database, networking, resource scheduling, load balancing transaction management, memory management, and concurrency control. Data mining techniques may be used to detect the malwares.

Most of the security problem occurs because of loss of control, lack of trust and multi-tenancy. These types are issues occurred mostly in management model which is managed by third party. Conflicts occur when service providers fail to give proper services to perform the task and achieve the goals. Physical structure is shared by multi users so attacker can easily track the information.

Cloud computing and web servers (Mishra & Sudevalayam, n. d. ) run on a network structure so they are open to network type attack that may denial the service. Few types of attacks are user hijacking a server; the hacker could stop the web services from functioning. Secured socket layer (SSL) isincorrectly configured then the client/server authentication will not behave as expected (Gampala *et al*., 2012). Network sniffing is done with a packet sniffer, which records all network packets; an attacker can capture sensitive data easily. If unencrypted data such as password and other web services related to security configuration such as UDDI – Universal description discovery and integrity WSDL – Web service description language and SOAP – Simple object access protocol (Bhadauria & Sanyal, 2012).

Port scanning is another threat in security issues (Jamil & Zaki, 2014). Port 80 is always open web server works on

it. This can be easily encrypted and as long as the server software is configured correctly then it' sprotected from intrusion. SQL Injection uses special characters as term to return unexpected data, they attack DOS for buffering flow. Lock-in tools, procedures and services could not assure data application and service portability. It is very difficult for users to migrate from one provider to another provider. In data protection, data must be protected with certification summaries. Next issue is insecure or incomplete data detection (Mangala K *et al*, 2013) in whichthey request to delete a cloud resource made with many operating systems. Erase data, and timely data deletion may beimpossible. Extra copies of information are stored but not available. To provide security measures incomplete data detection forms a private cloud in which three tier web, applications and database are used. Only authorised third party can access the database.

In order to maintain various security and privacy issues like confidentiality, operational, integrity, and disaster recovery and identity management (Subashini & Kavitha, 2010) and to secure the data, following schemes should be followed. An encryption (Bhadauria & Sanyal, 2010) scheme assures data security in a highly interfering environment that maintains security standards over suitable threats and data storage security. The service provider should be given defined access to the data. Stringent access control is to prevent unauthorised and illegal access to the server. Data backup and redundant strategy store the data to make data retrieval accessible due to any type of loss.

Distributed identity management: They maintain security by using either lightweight directory accessprotocol (LDAP) or published API to associate with identity system (Angadi & Gull, 2013).

## Cloud Security Controls

- Deterrent Control: These controls are set in a place to prevent the attack on a cloud system and the attack gives warning sign on a fence. They do not reduce vulnerability of a system.
- Preventative Control: It is used to upgrade the strength of the system by managing the vulnerability. It will safeguard the weakness of the system when attack is occurred. It finds the attack to reduce the damage and violation to the system.
- Corrective Control: They are used to reduce the effect of an attack. When attack occurs the action is taken by the corrective control.
- Detective Control: It is used to detect any kind of attack when it occurs. They give intimation to preventative and corrective control to address the issue.

## Cloud Computing Challenges

- Regulatory compliance: The providers refuse to external audits and security certifications.
- Privileged user access: Sensitive data are processed outside the organisation this leads to a major risk.
- Data location: Exact location of the data is not known by the users.
- Data segregation: It is a shared environment.
- Recovery: When the data is lost from the own system cloud providers are responsible to recover the data.
- Investigative support: Illegal activities might be impossible in cloud computing.
- Long term Viability: Data will remain available even after the task is over (Mishra & Sudevalayam, n. d. )

## Conclusion and Future Trends

The main objective of this paper is to envision the cloud computing basics, cloud computing models, technology, services, research and security issues related with cloud computing. This paper gives a complete study about different brokering services, secure cloud communication paradigms, and service level agreement. Cloud computing is compared with other computing technologies based on their characteristics and applications. Many software organisations and institutions used cloud computing.

Akamai and Amazon are the top most companies to deliver cloud servers. They use three-tier security architecture for data security. Most of the risk has occurred due to the nature of service delivery model of a cloud computing system. More attention is given on data privacy and data protection. Few technologies are used for security purposes like username, password authentication, image processing, digital signature, and cryptography. Most of the researches can be done on cloud computing security,

trusted third party, key infrastructure and information security.

Data mining techniques like rule based techniques are used for detecting malware in cloud. It mines the data and gives meaningful information. Security issues may occur on database, operating systems, virtualizations, resource sharing, transaction management, concurrency control, and memory management. Third party providers own and manage all the computing resources like services, software, storage and network. Internet connection and electricity are needed for services. Users need to plug into the cloud servers. Nowadays, mobile cloud computing is also implemented. Speed up connectivity is recommended for betterment of connection. Connections can be done through direct cable connection. Multi clouds and cloud within clouds is used to improve the technologies which reduce the security issues.

## References


Angadi, A. B., Angadi, A. B., & Gull, K. C. (2013). Security issues with possible solutions in cloud computing- A survey. *International Journal of Advanced Research in Computer Engineering and Technology*, February, 2(2), 652-661.

Azcuy, J. (2009). Centralized vs distributed Computing: Director of Service Delivery: Posted & Filed under Technical Education.

Bhadauria, R., & Sanyal, S. (2012). Survey on security issues in cloud computing and associated mitigation techniques.

Cuomo, A. & Di Mobica, G. (2012). An SLA based broker for cloud infrastructure. *Journal of Grid Computing*. DOI 10723-012-9241-4.

Gampala, V., Inuganti, S., & Muppidi, S. (2012). Data security in cloud computing with elliptic curve cryptography. *International Journal of Soft Computing and Engineering*, July, 2(3), 138-141.

Gong, C., Liu, J., Zhang, Q., Chen, H., & Gong, Z. (2010). *The characteristics of cloud computing*. Paper Presented at the 2010 International Conference on Parallel Processing Workshops in China.

Jamil, D., & Zaki, H. (2011). Cloud computing security. *International Journal of Engineering Science and Technology*, 3(4), 3478-3483.

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public and private cloud computing. National Institute of Standards and Technology.

Kaur, A., & Raj, G. (2013). Secure broker cloud computing paradigm using AES and selective AES algorithm. *International Journal of Advanced Research in Computer Science and Software Engineering*, March, 3(3), 79-83.

Mishra, M. & Sudevalayam, S. (n. d. ) Introduction to cloud computing and virtualization. CSE, IIT Bombay.

Neto, M. D. (2014). A Brief History of Cloud Computing.

Pai, M. K., & Jayalakshmi, D. S. (2013). Survey on privacy and data security issues in cloud computing: A survey. *International Journal of Engineering and Advanced Technology*, 2(5), 129-134.

Raj, G., & Kaur, K. (2012). Secure cloud communication for effective cost management system through MSBE. *International Journal on Cloud Computing: Services and Architecture*, June, 2(3), 19-30.

Rani, A. M. G., & Marimuthu, A. (2013). An Investigation on the Issues in Cloud Data Security. *International Journal of Computer Applications*, November, 82(1), 39-43.

Singh, N., & Raj, R. (2012). Security on BCCP through AES encryption techniques. *International Journal on Engineering Science and Advanced Technology*, 2(4), 813-819.

Subashini, S., & Kavitha, V. (2010). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, July, 34(1), 1-11.

Velte, A. T., Velte, T. J., & Elsenpeter, R. (2009). *Cloud Computing: A Practical Approach*.

Younge, A. J., Laszewski, G. V., Wang, L. (2010). *Efficient resource management for cloud computing environments*. Proceedings of the International Conference on Green Computing.