ANALYSIS OF DESIGN & ARCHITECTURE OF CLOUD COMPUTING

Submitted By:

Afra Sadat – 002

Tooba Khalique - 031

Submitted To:

Sir Ahsan Ilyas

Abstract:

Cloud computing is turning out to be exceptionally famous and promising innovation. This paper examines the design and architecture of various sorts of deployment models that are: public, private, hybrid and community and how these models help to work on various kinds of bushiness. Each model has its own advantages and downsides. In spite of the fact that there are many benefits of cloud computing yet there are a few disadvantages as well. Security is as yet one in the event that the main issues of cloud computing.

1. INTRODUCTION

In past few years numerous technologies have evolved and many new services have emerged. But still to this development there are some restrictions and limitations of computer devices that needed to be overcome. Storage and maintenance of data has always been a costly task even for established companies. Storing the data physically requires more space and maintenance. Cloud Computing was invented to overcome certain limitations and provide new services to users virtually.

The term cloud is used to denote Network or Internet. In simple terms cloud can be defined as something which is at a distant or remote location. A cloud provides services to users through public or private networks such as WAN, LAN or VPN.

The name cloud computing emerged from the symbolic representation of Internet i.e.; cloud used in many flowcharts and diagrams. It refers to deploying, organizing and accessing both physical i.e.; hardware and software resources remotely. It provides unlimited online services and resources like data storage, backup and maintenance, infrastructure and applications.

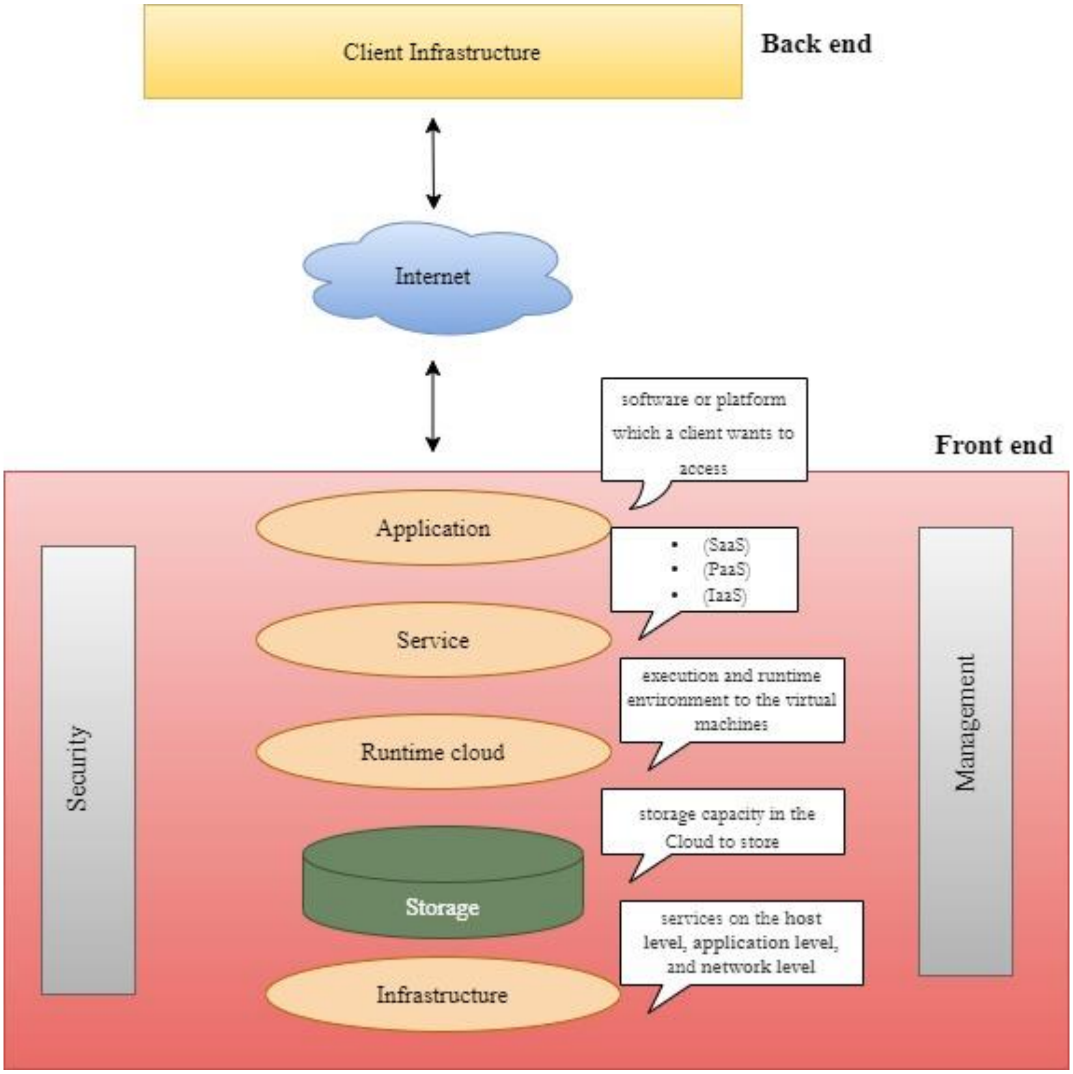
Cloud computing doesn’t require the local software installation on PC, hence providing its users platform independency and making business applications and services mobile compatible and collaborative. It is less costly, easy to use and user friendly. There are multiple advantages of cloud computing including self-service provisioning, flexibility, resistance, broad network access and resource pooling.

1.1. Architecture of Cloud Computing

Cloud computing is done by using remote physical servers, databases and computer devices to provide users access to data and applications over internet.

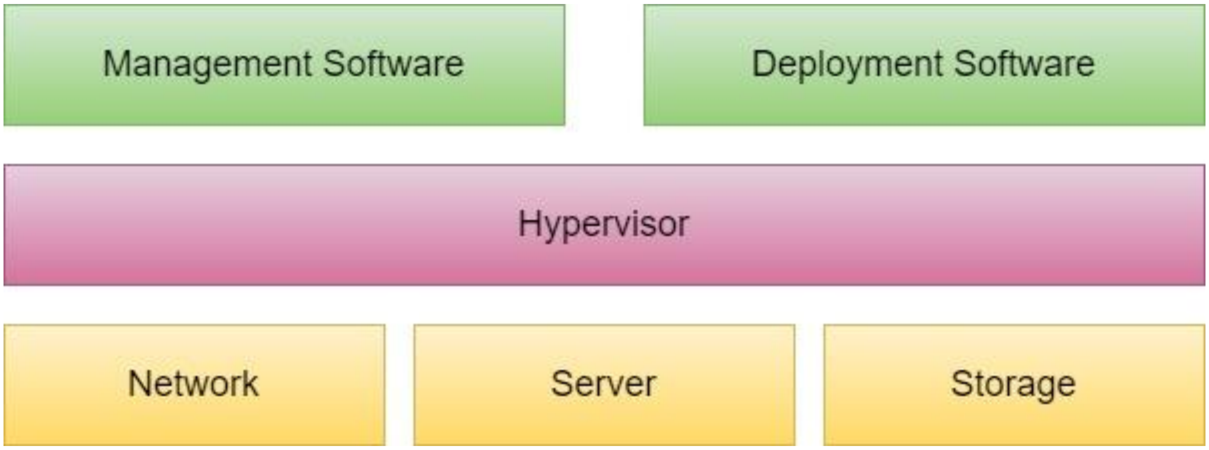
The front end contains access to client device, browser, software applications and network which is connected to back end through internet network. The back end contains remote servers, computer devices and databases, and it acts as a repository that stores data accessed by the front end.

A central server manages all the communications between both front and back ends. It manages the connectivity of multiple client devices and cloud servers by the use of both softwares and middleware. This central server uses certain protocols to manage the transfer of data. Generally, each different application or workload has its own dedicated server.


Client Infrastructure
Back end
Internet
software or platform which a client wants to access
Front end
Application
(SaaS)
(PaaS)
(IaaS)
Service
execution and runtime environment to the virtual machines
Runtime cloud
storage capacity in the Cloud to store
Storage
services on the host level, application level, and network level
Infrastructure
Security
Management

1.2. Infrastructure of Cloud Computing

Elements included in cloud computing infrastructure are servers, storage devices, cloud management applications, network, deployment models and platform virtualization. Transparency, Scalability, security and Intelligent monitoring are basic constraints in Infrastructure.



Hypervisor acts as a Virtual Machine Manager allowing sharing of single physical instance of cloud services between several tenants. It is generally a firmware or a low-level-program.

Management Software is used for maintenance and configuration of infrastructure.

Deployment Software helps in deployment and integration of applications on cloud.

Network is the vital element of cloud infrastructure. It allows availability of cloud services over Internet. Network can be used as a service which means user can customize network route and protocol.

Server helps in computing resource sharing and provides service like resource allocation, de-allocation, monitoring the resources and providing security etc.

Storage stores user data. There are multiple replicas of storage in cloud. In case of one resource failure, data can be extracted from another making cloud computing reliable.

1.3. Models in Cloud Computing Architecture

There are two types of models used in cloud computing.

1.3.1. Deployment Models

Following is a brief description of all deployment models:

- **Public cloud:**

Public cloud deployment model allows the access of systems and its services to anybody which makes it less secure. The services of infrastructure cloud in plain cloud deployment model are available to general public over internet. Its infrastructure is not owned by consumer. It is best for the companies that have low security concerns as anyone can easily access systems and services.

Example: Google, Amazon, Microsoft etc.

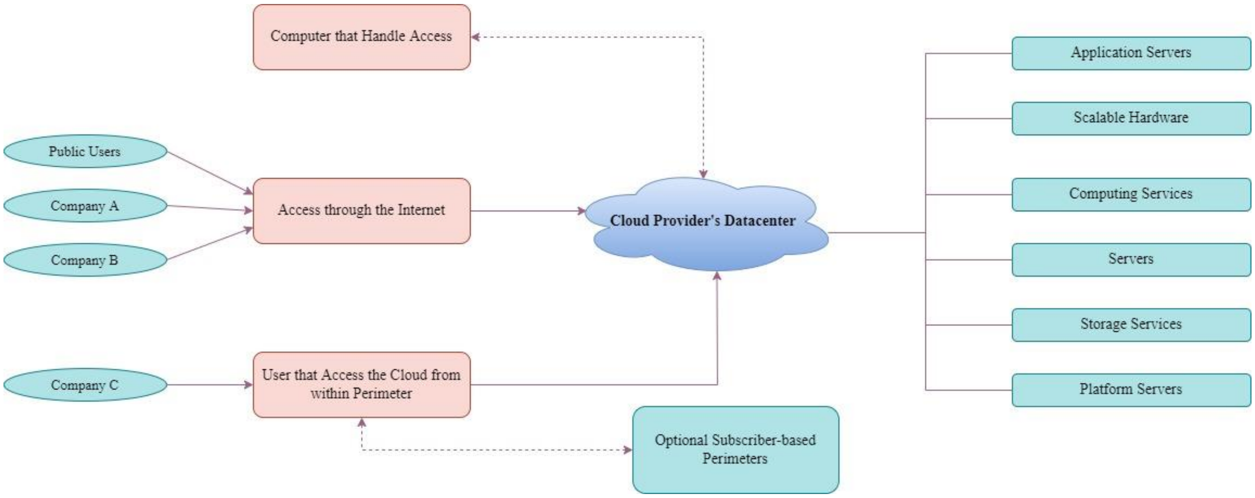

Computer that Handle Access
Public Users
Company A
Company B
Access through the Internet
Cloud Provider's Datacenter
Company C
User that Access the Cloud from within Perimeter
Optional Subscriber-based Perimeters
Application Servers
Scalable Hardware
Computing Services
Servers
Storage Services
Platform Servers

Figure 1.3.1: Public cloud

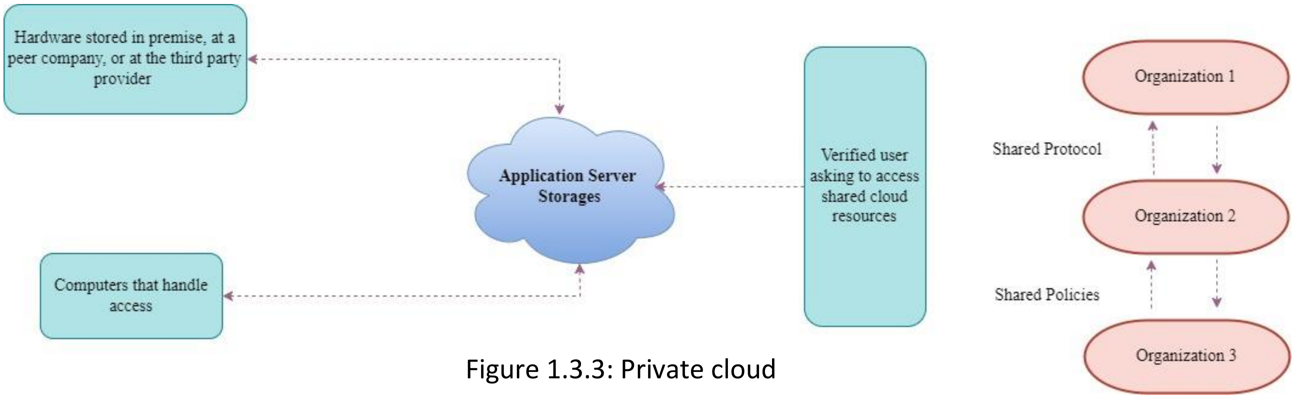

Hardware stored in premise, at a peer company, or at the third party provider
Application Server Storages
Computers that handle access
Verified user asking to access shared cloud resources
Organization 1
Shared Protocol
Organization 2
Shared Policies
Organization 3

Figure 1.3.3: Private cloud

- **Private Cloud:**

The opposite of public cloud deployment model is private cloud deployment model. Organizations with high security concerns use private cloud. When there is no need of sharing hardware with everyone. It provides high level of security, having under the protection of firewall and IT departments. The systems and services can only be access within a border or organization. Private cloud also notes as "corporate cloud" or " internal cloud".

Examples: HP data centers, Ubuntu etc.

- **Community cloud:**

Community cloud deployment model is not as secure as private cloud deployment model but better than public cloud deployment model. Groups and community can access systems and its services and can share information which makes it cost effective. It is in the supervision of third party or one or more organizations.

- **Hybrid Cloud:**

Hybrid cloud is the combination of both private cloud and public cloud. It means that it is partially secured, data in the private cloud and the data in public can be access by anyone. Data can be moved by an organization according to their need. The confidential information can be stored in private cloud while the less critical data can be stored in public cloud.

Example: Google Application Suit, Office 365

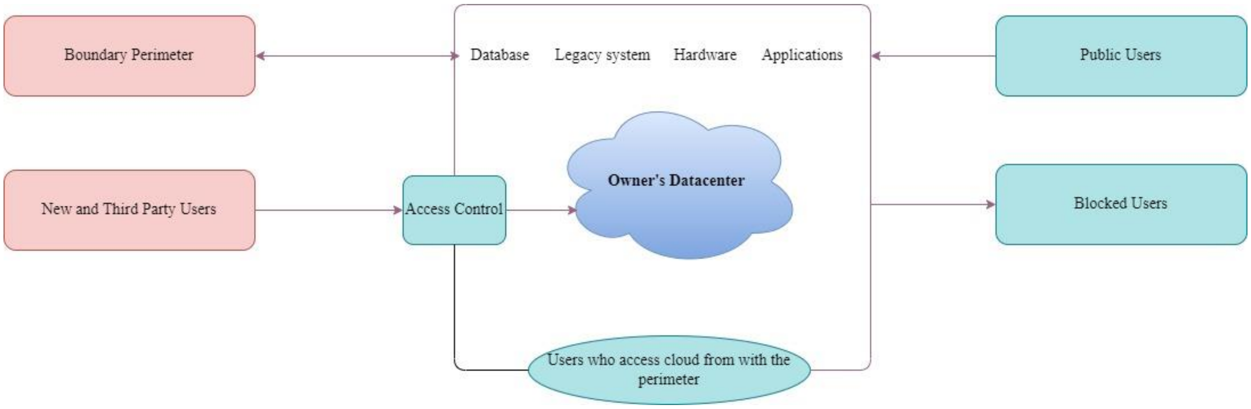


Figure 1.3.3: Community cloud

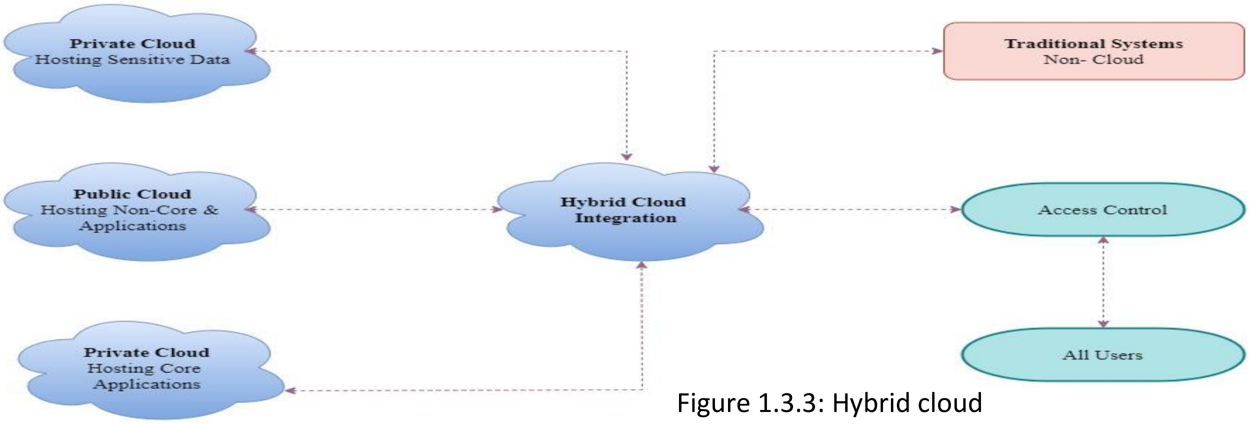


Figure 1.3.3: Hybrid cloud

1.3.2. Service Models

Following is a brief description of all service models:

- **Infrastructure-as-a-Service (Iaas):**

The basic functionality of Iaas is to provide its clients essential resources including hardware machines, virtual machines and virtual storage. Apart from these resources, the IaaS also offers:

- Virtual local area network (VLANs)
- Software packages
- Load balancers
- Virtual disk storage
- IP addresses

These resources are accessed by users using virtualization.

- **Platform-as-a-Service (Paas):**

Users can develop and deploy applications using tools provided by Paas along with a runtime environment for applications. It enables non-developers to create web applications using the point and click tools. Main examples of Paas are App Engine of Google and Force that allows users to use built-in API's by logging in and creating applications. But the drawback is that the client gets committed to a single vendor. •

- **Software-as–a-Service (SaaS):**

It enables the client to access software applications as a service by deploying it on a host system and making it accessible through internet. Given below is the list of some SAAS applications.

- Billing and invoicing system
- Customer Relationship Management (CRM) applications
- Help desk applications
- Human Resource (HR) solution

1.3. Security in Cloud Computing

One of the main concerns in cloud is security. Data in cloud is stored in encrypted form and to restrict access to data directly, proxy and brokerage services are employed. Before deploying a resource to cloud many aspects should be observed such as cloud service model, deployment model, analyzing the resource sensitivity to risk in cloud and understand the service provider's system about storage and transfer of data on and off cloud. Mainly the risk in deployment models depend on service and cloud types.

Service models define the boundary that elaborates services of service provider and clients. Cloud Security Alliance stack model defines boundaries between different service models and shows connectivity of different functional units.

The lowest layer in model is Iaas and upper two are Paas and Saas and each upper mode inherits capabilities of lower models. Iaas provides Infrastructure, Paas provides platform development and Saas provides operating environment. Saas has the most integrated functionalities. The following model shows security boundaries at which provider's responsibilities end and clients begin. Any security constraint below the security boundary must be maintained and built in to system by client.

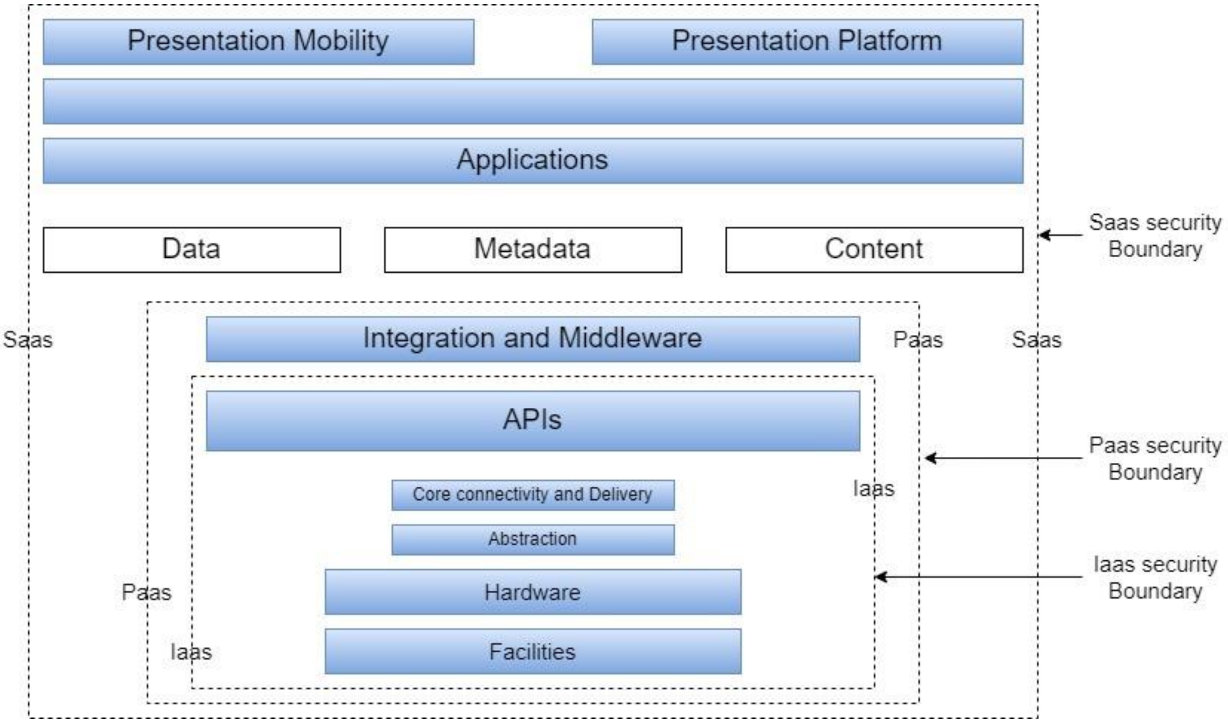
2. LITERATURE REVIEW

The idea of network-based computing dates to the 1960's but the first practical use of cloud computing occurred in 2006 when this term was introduced to an industry conference by former google CEO Eric Schmidt.

The first ever model designed for cloud computing was Public Cloud Model which allows resources and services to be easily accessed by general public. The services offered by Google, Amazon and Microsoft are the best examples of Public Clouds.

The three service models are deployed in every deployment model with two additional present sometimes. The security and resource management are associated with the deployment models.

There are multiple advantages of deploying a cloud computing environment as a public cloud Model. Public clouds are most cost-



effective due to their shared resource architecture which enables large number of clients to share same resources. Resources in a public cloud are employed from different locations which increases its reliability in case of resource failure. These types of clouds are based on pay-per-use model which means resources become available on customer demand. These resources are provided from a pool of resources which allows the scaling of resources according to requirement. Location Independency is one of the many features of cloud computing and the biggest advantage of cloud model. Moreover, public clouds can easily integrate with private clouds providing customers a flexible and smooth approach.

Like every technology apart from advantages there are also some limitations of public cloud models. Due to the shared resource architecture and presence of data off-site, public clouds do not ensure high level of security. As, this model uses multi-tenant approach it offers limited or no customization to its clients which is unfavorable for companies with complex network architecture.

These issues of less customization and security were overcome by Private Cloud Model. Although development on private clouds were initiated in **2008**, they were still not fully functional and not popular. But the issue of security in public clouds were a strong factor for promoting private models. Finally, in 2010, companies like AWS, Microsoft, and OpenStack successfully developed private clouds that provided full functionality. A private cloud model operates only within a single organization and offers services only to that organization. It is accessible from only within the organization network but can be managed either internally from within the organization or by some other third-party.

Unlike Public cloud private cloud doesn’t general public to access its resources and these resources shared from discrete pool of resources ensuring high security and privacy crucial for an organization. As, the private cloud is accessible only within an organization it has more control over its resources and hardware and allows customization. In terms of cost private clouds are mostly costly than public clouds comparing to resources but their efficiency is higher than public clouds. The more costly factor rises due to the deployment of more hardware resources for transactions.

Private cloud is better than public clouds in many ways but it has its own limitations. Unlike public cloud a private cloud is accessible only within an organization or locally which makes it difficult to deploy globally. Public cloud offers high scalability since its resources are more general but private clouds offer limited scalability due to their specific resources. They can only be scaled within internal resources. Another disadvantage of private networks includes demand of expertise to manage, deploy and organize private clouds.

Next evolution of model introduced a new kind of model which is a combination of both private and public models. The hybrid cloud was invented in 2011. It divided the activities into two types i.e.; critical which operated using private cloud and non-critical which operated in public cloud.

Hybrid cloud combines the best features of both private and public clouds. It provides both kinds of scalability i.e.; public and private. It ensures high level of security and are cost-effective. Hybrid clouds are flexible and provide secure resources.

Due to the involvement of both public and private clouds network architecture of hybrid cloud is complex and problematic. It is important to make sure that cloud services are compatible with organization's security policies. The hybrid cloud model depends on the internal IT infrastructure; therefore, data redundancy is to be ensured across data centers.

To overcome the issues of security in public model and specific area of operation in private model was resolved by Community model which is a mixture of both public and private models. It was introduced in 2013 and its key feature was allowing a number or group of organizations to access shared resources making it partially public and partially private. It shares the cloud to specific organizations of a giver community. The cloud can be managed by both internal bodies or a third-party. It was mainly developed for business use.

Community model provides less security than private clouds but more security than public clouds at less cost than private clouds. It provides all advantages of private cloud adding on the service to share data and resources between multiple organization in same community infrastructure. The main issue in community clouds is of privacy and maintenance. As, all the data in one cloud is accessible to all members of the organizations within cloud, any data stored on cloud can be accessed by other clients which can violate the privacy of a user. Moreover, this type of cloud requires to assign roles and responsibilities of governance, security and cost among different organizations which is a problematic task.

3. LIMITATIONS

Although cloud computing has evolved and overcame its limitations through multiple models but there are still some limitations that still need attention. Every cloud model has its own drawbacks and specialties but still there is no such cloud that meets all the qualities of functionality, flexibility, security and ease of use and deployment. Public cloud has security and customization issue but vast resources, private cloud overcame these issues but became limited in resources. Community Cloud provided both customization and secure environment. And hybrid cloud provides customization, vast resources and security but has deployment issues. It requires skilled operators and has complex deployment and management. Every model is designed for specific environments but for general public there is no secure model till now that provides vast resources, customization along with security without increasing the complexity. So, there is need for a model that will be secure, usable, customizable, less costly with more resources and less complexity.

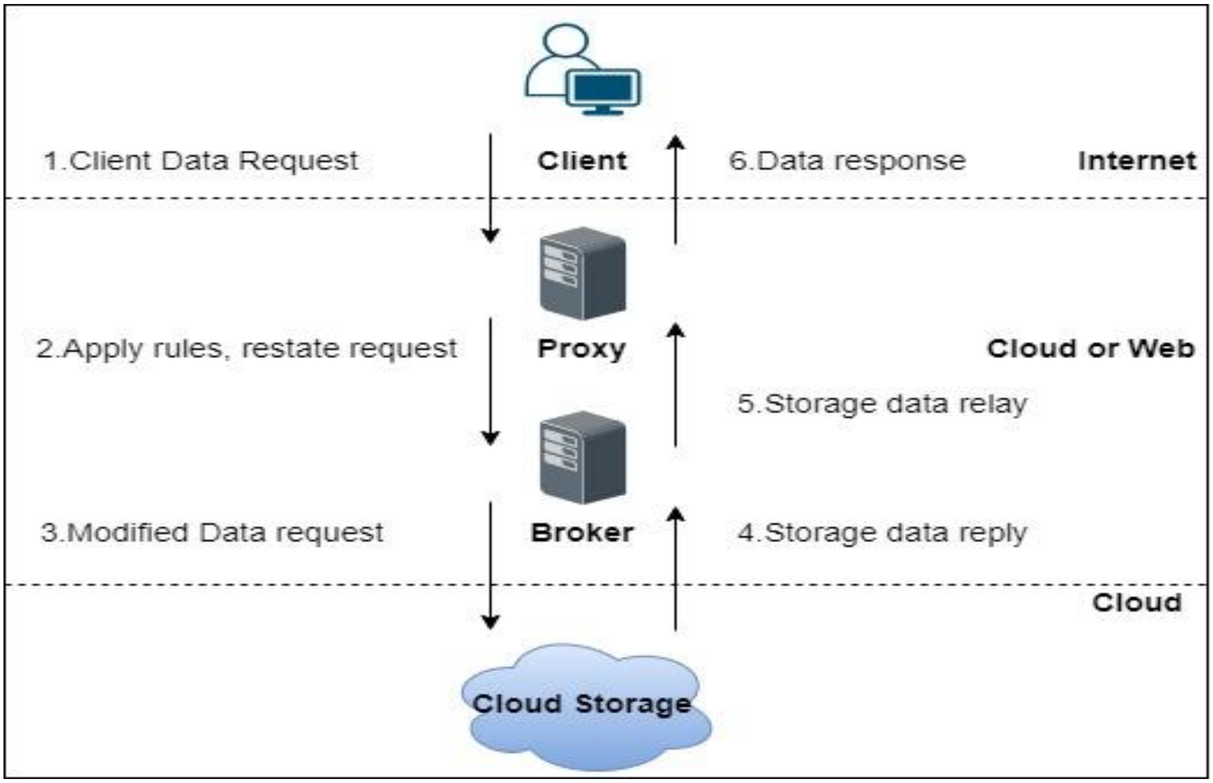
4. DISCUSSION

The security of a model is concerned with its deployment model along with its service models. Till now the issue of security along with cost effectiveness, customization and less complexity is not resolved. This demand for the need of another hybrid model for general use that is less complicated and easy to deploy. Security and Privacy are the major challenges in cloud computing and this issue can be over come by applying encryption, security hardware and security applications. A **Brokered Cloud Storage Access** is an efficient approach for isolating storage in the cloud. It is deployed by creating two services, one broker that has full access to storage but none to client and a proxy with no access to storage but access to both client and broker.

The following diagram shows the working of Brokered Cloud Storage.

Another main concern is portability that a cloud application should be easily migrated from one provider to another. It is a challenge as there should be no vendor lock-in. This feature is not yet possible because each provider has its own standard platform language which will not be compatible with all other.

Interoperability is still offered via web services but its development is complex. It allows an application to use services from other platforms. Data intensive application need high network bandwidth which is costly. Low bandwidth cannot be used as it doesn't meet desired computing performance of cloud application. A cloud system should be reliable and robust due to the massive use of clouds in business.



5. CONCLUSION

Cloud computing assumes a focal part in information handling and data storage, the eventual fate of cloud and data storage is evolving quickly. The cloud has advanced decisively over the long time. This paper gives the information on the prologue to cloud computing, its ideas, models and services. Cloud deployment models have a special contribution and can gigantically enhance business. For independent venture public cloud is ideal model and as your necessity transforms you can change to various sending models. A compelling deployment strategy can be created depending on your necessities utilizing cloud deployment models. Information security is one of the central issues in cloud storage, and in the future however new systems are making to conquer its downsides.

6. REFRENCES

[1] Abd Elminaam , D. S. (2018). Improving the security of cloud computing by building new hybrid cryptography algorithms.International Journal of Electronics and Information Engineering, 8(1), 40–48.

[2] Ahuja R. Mohanty S. K. Sakurai K. (2017). A scalable attribute-set-based access control with both sharing and full-fledged delegation of access privileges in cloud computing. Journal of Computers and Electrical Engineering, 57, 241–256. 10.1016/j.compeleceng.2016.11.028

[3] Ali A. Ahmed M. Khan A. Ilyas M. Razzaq M. S. (2017, May). A trust management system model for cloud. In Proceedings of the2017 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1-6). IEEE.10.1109/ISNCC.2017.8072029

[4] Antonolpoulos F. Petrakis E. G. M. Sotiriadis S. Bessis N. (2018). A physical access control system on the cloud. Computer Networks, 134, 46–54. 10.1016/j.comnet.2018.01.037

[5] Assante, D., Castro, M., Hamburg, I. & Martin, S., 2016. The Use of Cloud Computing in SMEs. Procedia Computer Science, 83(1), pp. 1207-1212.

[6] Bhattasali T. Chaki R. Chaki N. Saeed K. (2018). An adaptation of context and trust aware workflow oriented access control for remote healthcare.International Journal of Software Engineering and Knowledge Engineering, 28(06), 781–810. 10.1142/S0218194018500225

[7] Buzzanca M. Carchiolo V. Longheu A. Malgeri M. Mangioni G. (2017). Direct trust assignment using social reputation and aging.Journal of Ambient Intelligence and Humanized Computing, 8(2), 167–175. 10.1007/s12652-016-0413-0

[8] Chen J. Tian Z. Cui X. Yin L. Wang X. (2018). Trust architecture and reputation evaluation for internet of things.Journal of Ambient Intelligence and Humanized Computing, 1–9.

[9] Ching Yuen Luk (2019). Security Frameworks in Contemporary Electronic Government (pp. 96-128).

[10] Choudhary & Singh. (2019). Safety Measures and Auto Detection against SQL Injection Attacks. International Journal of Engineering

and Advanced Technology, 9(2), 2827 – 2833.

[11] Coppolino L. D'Antonio S. Mazzeo G. Romano L. (2016). Cloud security: Emerging threats and current solutions. Computers & Electrical Engineering.

[12] Gartner. (2019, Apr. 2). Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019.

[13] Harrath Y. Bahlool R. (2019, July-September). Multi-Objective Genetic Algorithm for Tasks Allocation in Cloud Computing. International Journal of Cloud Applications and Computing, 9(3), 37–57. 10.4018/IJCAC.2019070103

[14] Kaur N. Sood S. K. (2018). A trustworthy system for secure access to patient centric sensitive information.Telematics and Informatics, 35(4), 790–800. 10.1016/j.tele.2017.09.008

[15] Kaushik S. Gandhi C. (2020, January-March). Capability Based Outsourced Data Access Control with Assured File Deletion and Efficient Revocation with Trust Factor in Cloud Computing. International Journal of Cloud Applications and Computing, 10(1), 64–84. 10.4018/IJCAC.2020010105

[16] Lopez J. Rubio J. E. (2018). Access control for cyber-physical systems interconnected to the cloud. Journal of Computer Networks, 134, 46–54. 10.1016/j.comnet.2018.01.037

[17] Mojtaba Alizadeh, Saeid Abolfazli, Mazdak Zamani, Sabariah Baharun and Kouichi Sakurai, "Authentication in mobile cloud computing", Journal of Network and Computer Applications, vol. 61, no. C, pp. 59-80, 2016.

[18] Sambrekar K. Rajpurohit V. S. (2019, January-March). Fast and Efficient Multiview Access Control Mechanism for Cloud Based Agriculture Storage Management System. International Journal of Cloud Applications and Computing, 9(1), 33–49. 10.4018/IJCAC.2019010103

[19] Sinha K. Choudhary S. Paul S. Paul P. (2018). Security of Multimedia in Cloud using Secret Shared Key. International Conference on Computing, Power and Communication Technologies, 908-912.10.1109/GUCON.2018.8675031

[20] Vasco Ribeiro Santos, Tiago Ferreira Vitorino, Alvaro Dias and Bruno Barbosa Sousa (2022). International Journal of Service Science, Management, Engineering, and Technology

[21] Wu X. (2018). Study on Trust Model for Multi-users in Cloud Computing.International Journal of Network Security, 20(4), 674–682.