International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 2 (2019) pp. 429-434

A Survey on Cloud Computing and Hybrid Cloud

M.P.Vaishnnave[1], K.Suganya Devi[*], P.Srinivasan[2]

[1]*Department of Computer Science and Engineering, University College of Engineering, Panruti, Tamilnadu, India.*

[*]*Assistant Professor, Grade-I, Dept. of Computer Science and Engg., National Institute of Technology,Cachar, Assam, India.*

[2] *Assistant Professor, Grade-I,Department of physics, National Institute of Technology,Cachar, Assam, India.*

Abstract

Cloud computing is the recently developing innovation. Every association needs to interface with the cloud computing condition.A survey on distinctive hybrid cloud organization models and cloud benefit models accessible in the field of cloud computing is discussed. An industry pattern has been noted where the utilization of hybrid cloud design can be utilized which supports, the upcoming industry challenges by giving the effective method for putting away their information in the cloud condition by utilizing the mix of both public and private cloud, so that it gives the office to store delicate information on private cloud and less basic information on to public cloud where large storing can be made. Hybrid cloud is particularly profitable for dynamic or extremely adjustable workloads. This paper portrays the overview, service model,traits,supplier storage and issues of cloud computing.

Keywords: Cloud Computing, Private Cloud, Public Cloud, Hybrid Cloud, SaaS, PaaS, IaaS, Cloud Security

1. INTRODUCTION

In Today's world, innovation is developing at a quick pace and offers the client with various services which are paperless and accessible online, for example, e-charging, email, e-message, e-transaction and so forth. All these accessible administrations require an online information exchange. Atta urRehman Khan et.al[1] has discussed on these information that might be any private or delicate data like business secret information, MasterCard detail, managing an account exchange and so on, which require more assurance as disclosure of these secret information of any unapproved client may be unsafe.The greatest advancement in the field of computing is capacity and access of information in the cloud, be that as it may, there are numerous things that need to take think about as well. Many creators disclose that cloud computing has a few advantages when contrasted with their drawbacks. Yet, this found that as association of information builds, security of information becomes into a huge issue in spite of the fact that we have to discover a way all you require with a specific administration.Cloud computing has been rising up out of the latest advances in innovation, for example, hardware Virtualization and distributed computing. The refinement with cloud computing is that the processing methodology may continue running on one or many related PCs meanwhile, utilizing the possibility of virtualization. The advantages and disadvantages of cloud computing are described in Fig.1.The cloud model is made out of six of cloud computing fundamental qualities, three service models and four deployment models. Cloud gives different service models as, IaaS, PaaS, and SaaS. It can be sent at various deployment models, i.e. at public, private, hybrid and community cloud.

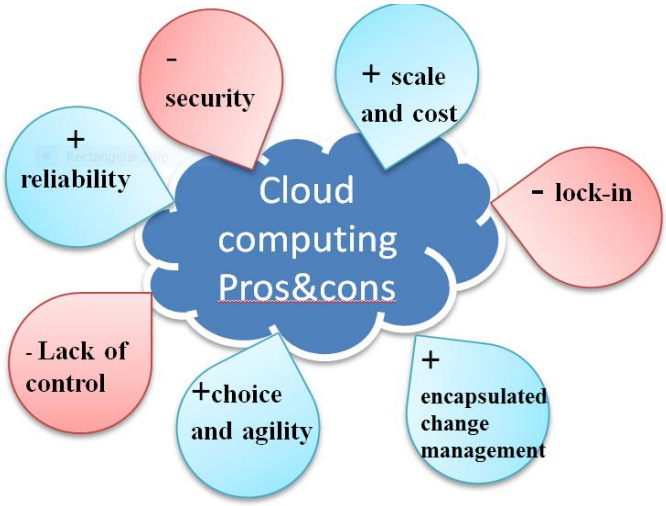

Fig.1. Cloud Computing pros&cons

2. SERVICE OF CLOUD

2.1 Software-as-a-Service (SaaS)

Software-as-a-Service (SaaS) displays permits for utilizing software applications as a support of end-clients. Priyadarshi S et. al[3] have discussed the SaaS as the most well known type of cloud computing, which is additionally the least demanding to comprehend and utilize. These cloud application services, fundamentally utilize the utilization of the Web to deliver applications. These services are given to the concerned customer by an outside vendor Haolong Fan et.al[2]. Since the greater part of these applications can be derived specifically from a Web program, customers'no need to install or download anything onto their very own PCs or servers.For this situation, the cloud provider manages everything viz.,applications, information, runtime, servers, storage, virtualization and systems administration. Utilizing

SaaS makes it simple for enterprise to keep up their frameworks, as a large portion of the information is overseen by the outside vendor.

2.2 Platform-as-a-Service (PaaS)

Patil BhagyashriD et.al [4]; S.Priyadarshi et.al[3] has stated that a Platform-as-a-Service (PaaS) gives the runtime condition to applications, development and arrangement tools, and so forth. This service model is the hardest to oversee from among the three. As the name proposes, the resource, here are offered through a platform. Developers then utilize this platform to make and customize applications based on the framework made accessible to them. Provided that the enterprise has an efficient development group, PaaS makes it simpler for development, testing and organization of applications on a basic server, storage, runtime, middleware and networking, however, it is up to the customer to manage applications and information .

2.3 Infrastructure-as–a-Service (IaaS)

The Infrastructure-as-a-Service (IaaS) is the most essential level of service.The most basic level of service.The fundamental distinction amongst SaaS and PaaS, subsequently, lies in the certainity that the responsibility of dealing with the framework is shared by the client or customer and the provider also S.Priyadarshi et.al[3]; Younis A Younis[6]. For this situation, providers still oversee IaaS as it gives access to key resource, for example, physical machines, virtual machines, virtual capacity, and so on. This service essentially provides computing infrastructure, for example, virtualization, storage and networking. Customers can buy completely outsourced service, which are then charged as per the resource they go through. The provider in this case charges a rent to install the clients' virtual server on their own IT infrastructure. While the merchant is in charge of overseeing virtualization, servers, storage and networking, the customer needs to deal with information, applications, runtime and middleware. Customers can introduce any platform as required, in light of the kind of framework they select. Likewise ,they will need to oversee updating of more up- to date forms as the necessity for accessibility arises.

3. DIFFERENT DEPLOYMENT MODELS

3.1 Public Cloud

It is the genuine portrayal of cloud hosting where the client and provider have a strong Service Level Agreement (SLA) to maintain the trust between them. Saurabh Singh et.al[5] has proposed a cloud framework, which provides open access to the public and the organization. Businesses, scholastics, or governmental associations possess a public cloud environment. A public cloud is run and managed by the Cloud Service Provider (CSP) and the physical foundation may introduced at off-site location of the client.Hence numerous elements may claim and work in a public cloud. This makes many issues, as it is unaware of where the resources are found or who claims them, expanding the trouble of protecting them from attack. Sahandi Reza et.al[11]has stated a public cloud computing as when a service provider makes a service or an application available to be used to people around the world over the world wide web and providing service to multiple organizations at a time by making use of the pay per usage system for payment of the service provided .

3.2 Private Cloud

Cloud computing works and manages inside the data center of an association are known as a private cloud. Numerous buyers of cloud infrastructure (e.g., business units) are including arrangement for elite use by a single association. Cearley W et.al[10]has stated that a Private cloud is like a general public cloud, however, they are scalable and self-servicing through an appropriate structure and it delivers the service of a single association. In a private cloud, it is significantly less demanding to recognize the client and provider relationship on the grounds that the foundation possessed and worked with a similar association. In this way, security dangers are less demanding to recognize.

3.3 Community Cloud

Chirag Modi et.al [9]has discussed about community cloud .A cloud that is deployed and shared among a group of people for sharing common interest, such as mission, security policy, application and services is known as community cloud.It is owned, and managed by community organizations, an outsider, or some mix of them driven by one or many, and that might be available on or off campus Saurabh Singh et.al[5]. In simple words, a community cloud is being shared and controlled by various organizations. It additionally reduces the security chance in the public cloud and reduces the cost of private clouds.

3.4 Virtual Private Cloud

Rahul Khurana1 et.al [7] has stated a virtual private cloud as a semi-private cloud, which uses fewer resources, and it consists of Virtual Private Network (VPN). It is a demand configurable pool of shared resources allocated within the cloud environment.

4. OVERVIEW OF HYBRID CLOUD

Shandi Reza et.al [11] has proposed a hybrid cloud as a blend of both public cloud and private cloud, as it can provide service to various organizations with a legitimate structure of the model, versatility and appropriate coordination between both platforms, for example, public cloud and private clouds.When people talk in terms of cloud computing, they are generally referring to public clouds, such as Rackspace, which is shared by several thousands of customers from all over the world. Rahul Khurana1 et.al [7] has discussed about

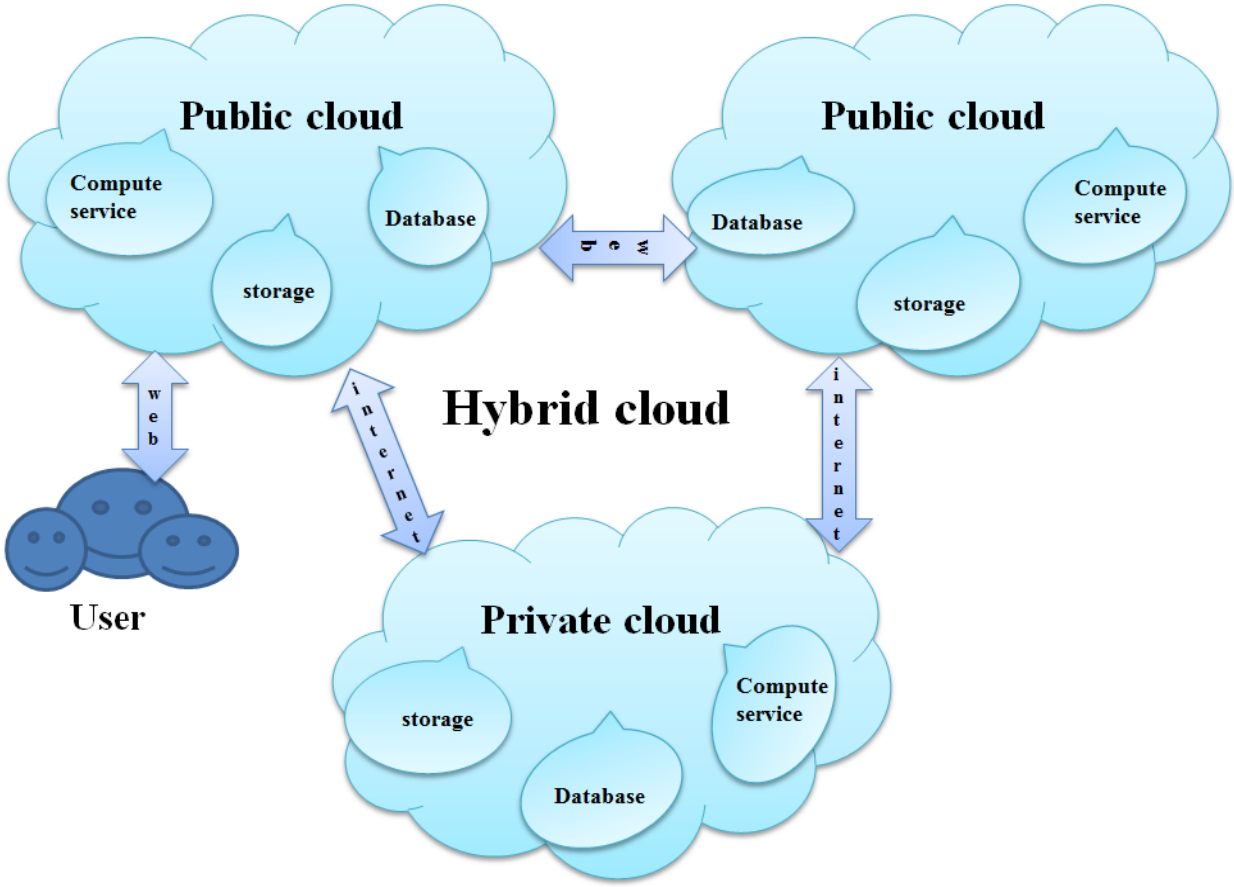

Fig.2. Hybrid cloud Services Model

a cloud provider that offers storage space, data transfer capacity and computing energy to organizations at substantially less expensive rates than those of actual, physical servers. While this saves the organization a tremendous chunk of investment, it could likewise bring about concerns over accessibility, availability and security. Most organizations would reconsider before porting delicate information onto a public cloud. Fig.2. shows the Hybrid cloud service model.

This kind of speculation got a few organizations working on setting up their own cloud-like computing procedures, which in turn, made what is known as the private cloud. While these mists work in an indistinguishable route from open mists, they are implied only for the organization and can be firewalled far from whatever is left of the Internet. This gives the private cloud greater security and better execution too.with the hybrid cloud demonstrate, IT leaders have an extra administration over each, the private and public components, than utilizing a pre-packed public cloud platform, especially for big business content administration Rahul Khurana1 et.al [7]. These pre-packed programming Software -as-a-service (SaaS) makes frequent redesigns and change without past notice or content and, if ineffectively composed, will break similarity with previous content. This hybrid approach will allow an organization to exploit the measurability and cost-effectiveness of cloud storage while not uncovering mission-basic data. The test is to incorporate and represent such a system, in a perfect world, without fixing the present on-premise infrastructure or the applications. Hybrid cloud provides regular data and software system management devices. Different providers attempt to solve this in a few routes, together with getting to everything through a web computing system Interface, coordination is essential for storage within the cloud or by means of a cloud gateway of some sort, for instance.

5. ADVANTAGE OF HYBRID CLOUD

(1) It is more versatile in wording that it contains both private and public cloud.

(2) Rahul Khurana1 et.al [7]; Saurabh Singh et.al[5] has outlined a hybrid cloud in a way as to rapidly scale the organization's needs. Since a few standardized procedures run together to accomplish synchronization between different type of cloud, it makes the perfect answer for load heavy projects, which can't be effectively handled by an organization's in-house server. Utilizing the hybrid cloud would likewise save the organization the additional cost of buying elite server hardware which would some way or another is vital.

(3) Hybrid cloud can be worked whenever and wherever from any part of the world. This gives them a worldwide reach for organizations that need to spread their range past geographic limits.It offers both secure resource and versatile public resource.

(4) It gives dependably a most level of security as it has assigned private cloud.It can diminish and deal with the cost based on the requirement.

(5) Hybrid cloud could turn out to be exceptionally costly for an organization to put resources into hosting suppliers or outsourcing the same. This innovation, then again, is accessible for exceptionally sensible rates and consequently, works out considerably less expensive for the foundation.

6. TRAITS OF HYBRID CLOUD

(1) Security: Security is regularly a common threat. Guaranteed safety efforts are set up when data is exchanged amongst storage and on-premises areas, furthermore as access- control measures once the data is stored Saurabh Singh et.al[5].Documents should be secure, whereas in storage as well.

(2) Reliability: Data integrity is also a touch of the hybrid cloud condition. The data received from person A to person B must keep up its integrity. Cloud provider would index the data. Its honesty also should stay in place once it's away. For example, if indexes are corrupted it prompts lose the data.

(3) Business coherence: Planned and even unplanned downtime will bring about issues for the business. The Capacity provider must embody snapshots, reflecting, and reinforcements, moreover as quick recuperation so if the supplier's framework goes down, it's secured.

(4) Reporting and charge-back: Rahul Khurana1 et.al [7]has stated that a cloud storage might be a compensation pay-you-pay model, bill are toward the end of the charge cycle. This can exemplify any value-based charges the provider would conceivably charge what's more as capacity costs.

(5) Management: In a hybrid cloud environment, if the client selects to store some of client's data on-premises and a few inside the cloud, they should be prepared to deal with the conditions together.

7. SUPPLIER STORAGE FOR HYBRID CLOUD

A few of the fundamental unusual providers and cloud providers have the particular item focused on building an agent cross hybrid cloud. Fig.3.shows some of hybrid cloud storage Vendors.

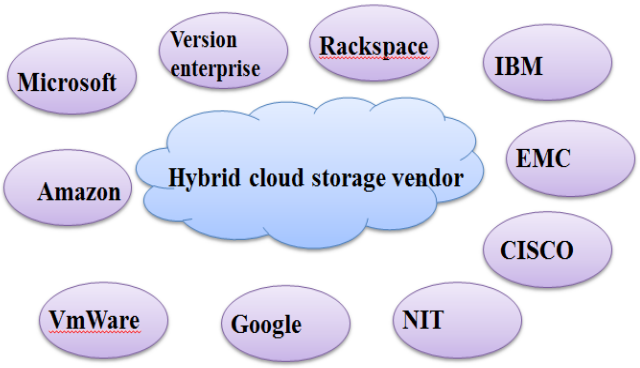

Fig. 3. Hybrid Cloud Storage Vendors

8. ISSUES IN CLOUD COMPUTING

There are different issues required in the field of Cloud Computing. These issues incorporate Cloud Compatibility, Compliance of the Cloud, Standardizing Cloud Technology, Monitoring while on the Cloud, and Cloud Security Rahul Khurana1 et.al [7]. These issues are depicted beneath quickly.

(1) R.Charanya et. Al[14] has discussed a Role based model where Data owner before storing the data in the cloud, they first encrypt the data in local system and then store the encrypted data in the cloud. Data users can't directly access the data from cloud. Each users are assigned with roles and responsibility. The roles are assigned based on the responsibilities and qualification. The authenticate users have privileges to access the data with specific roles. The users are assigned with different roles and each of them are having a set of permissions. A role manager responsibility is to assign a role to the user, and if the user is going out, then revoke a role from the user. Cloud Provider, users and others are not able to see the data if they are not assigned with proper roles. Data owner can revoke the role if they found as unauthorized user.

(2) Zheng Yan et.al[12] has stated the most difficult issue in the development of cloud computing, the trust management. Information privacy and security was a vital perspective. On account of the dynamic nature of cloud condition trust management was extremely testing.

(3) Chirag Modi et.al[9] has proposed the issues encompassing towards the difficulty of the web clients to trust the cloud service.This has been finished by doing customer criticism overview and after that proposal has been given to the cloud service provider.They proposed that if security is not taken care properly, the whole zone of cloud computing would come up short since cloud computing for the most part includes managing personal delicate data in a public network. Customer input study has been done on the basis of taking after targets, i.e. is there a purchaser with absence of trust or is there a route for cloud service providers to acquire consumer trust.

(4) There is a work process scheduling algorithm which concentrates on execution time and cost of cloud services. Be that as it may, it is not free from attacks and threats so a trust service oriented model is required.A trust service

oriented work process scheduling algorithm has been proposed in SanaeiZohreh et.al[17]. This algorithm works, to calculate trust metric and gives approaches to enable clients to choose from various services accessible as indicated by the requirement.

(5) Albert et.al[13] has proposed a trusted agent which will produce public key and master keys for the client.The role of the information proprietor is to encode the information with client public key and the client will decode the information with possessing private key.IT suggests two focal points in this plan 1) it reduces communication overhead in the web ,and 2) it provides fine grained access control.The issue behind in this method is the information owner needs to utilize the approved client public key for encryption .According to (ABE) Attribute Based Encryption, the access policy is grouped into two type: Key Policy Attributed Based Encryption(KP-ABE) and Ciphertext-Policy Attributed Based Encryption(CP-ABE).

(6) Kan Yang et.al[16]has proposed a Multi-authority Multi-specialist CP-ABE which is more reasonable for information access control.Various authorities issued the attributes to clients and utilizing access policy.The information owner shares the information characterized over attributes from various authorities. In this procedure, clients attribute can be changed dynamically. If a client has assigned with new attributes or denied some present attributes, then information access should be changed appropriately. Every information owner before encoding the information, they partition the information into various parts and each part is encrypted with contents keys by utilizing symmetric encryption system.

9.TECHNIQUES FOR CLOUD COMPUTING

Table 1. Techniques and its Advantage & Disadvantage

S.NO	Technique Name	Advantage	Disadvantage
1	Control Data Access(2015)	A structure was made for securing cloud computing by applying a different algorithm. The cloud administrations can be secured default as the cryptographic keys were produced based on trust models.	Cryptographically stored information sometimes creates a problem as some other common application access it.
2	Security and Trust(2015)	Trust management was presented.	It considers only client input. Different parameters were not considered.
3	Trust based Reputation model(2015)	A few methods have been shown detecting attacks	Very little accurate outcomes were obtained
4	Multi Authority(2014)	The specialists are working independent of each other. Therefore, the failure or working of one authority won't affect the working of different authorities.	Overhead occurs in managing with the distributed authorities.
5	A trust service scheduling (2014)	The outcomes demonstrated by the approach were effective and feasible and clients can choose workflow services from different cloud services	It was hard to manage dynamic changes in cloud computing condition
6	Attribute based encryption(2013)	Decrease the communication overhead. Provide a fine-grained access control. Collusion-resistance is a significant security highlight of Attribute-Based Encryption(ABE)	The information owner needs to utilize each approved client's public key to encrypt information
7	Hierarchical Attribute-set based encryption(2013)	Lower maintenance cost and operational costs. Easier disaster recovery	Data owners are controlled by domain authority
8	CP-ABE(2012)	The detriment of key policy-Attributed Base Encryption (KP-ABE) is overcome in CP-ABE and it support the access control in the real condition.	The client consolidates all attributes in a single set issued in their keys to fulfill approaches.

10. CONCLUSION

Protection and security of information is a prime concern in cloud computing information storage. Despite the fact that cloud gives flexibility and ease public information storage and management, yet there are chances for any intruder interaction and malicious activity. Information stored at cloud server might be secret along with greater security. In this paper, we have discussed about the fundamental components of the cloud computing and the security issues that begin due to the fertilized, shared, public, private and hybrid nature of the cloud. Therefore, the paper proposed various counter measures to address the security issues and various method in the cloud computing.

REFERENCES

[1] Atta urRehman Khan, Mazliza Othman, Sajjad Ahmad Madani, A Survey of Mobile Cloud Computing Application Models, IEEE Communications Surveys & Tutorials , Volume.16, pp: 393-413, 2014.

[2] Haolong Fan, Farookh Khadeer Hussain, Muhammad Younas, and Omar Khadeer Hussain,An integrated personalization framework for SaaS-based cloud services, Future Generation Computer Systems,Volume. 53, pp:157-173, 2015.

[3] S.Priyadarshi, N.Deepa, Himamshu Kumar, Implementation Software as a Service in Cloud Android Applications,International Journal of Advanced Research in Computer Engineering & Technology Volume.1, pp:383-386, 2012.

[4] PatilBhagyashri D,P L Ramteke, Development of android Based Cloud Server for Efficient Implementation of Platform as a Service, International Journal of Advanced Research in Computer Science and Software Engineering Volume .4, pp:309-312, 2014.

[5] Saurabh Singh, Young-Sik Jeong, Jong Hyuk park, A Survey on Cloud Computing Security: Issues, Threats, and Solutions ,Journal of Network and Computer Applications, SI1084-8045, ,2016.

[6] Younis A Younis, Madjid Merabti, Kashif Kifaya, A Survey on cloud Computing Security,Journal of Network and Computer Application, Volume.75,pp:200-22, ,2013.

[7] Rahul Khurana1, Himanshu Gupta, A Hybrid Model on Cloud Security 5th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) ,Volume.16,pp:347-352, ,2016.

[8] Mazhar Ali, Samee U Khan, Athanasios V Vasilakos, Security in cloud computing: Opportunities and challenges, Information Sciences ,Volume. 305,pp:357-383, , 2015.

[9] Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, Muttukrishnan Rajarajan, A survey on security issues and solutions at different layers of Cloud computing,Journal of Supercomputing, Volume. 63, pp:561-592, 2013.

[10] W Cearley, Kyle Hilgendorf, Cloud Computing Innovation Key Initiative Overview, Gartner Research Database, Volume.15 pp:45-52, 2014.

[11] Sahandi Reza, Alkhalil Adel, Martins Opara, cloud computing from SMES Perspective: A Survey Based Investigation,Journal of Information Technology Management, Volume-24,pp:1-12, 2013.

[12] Zheng Yan, Xueyun Li, Mingjun Wang and Athanasios V Vasilakos, Flexible Data Access Control based on Trust and Reputation in Cloud Computing, IEEE Transactions on Cloud Computing,Volume.99,pp:1-4, 2015.

[13] Albert S Horvath and Rajeev Agrawal, 2015,Trust in Cloud Computing Proceedings of the IEEE Southeast Con - Fort Lauderdale, Florida, Volume.25, pp: 1-8.

[14] R Charanya and M Aramudhan, Survey on Access Control Issues in Cloud Computing, IEEE,Volume.26,pp:4673-6725, 2016.

[15] Junbeom Hur,Improving Security and Efficiency in Attribute-Based Data Sharing,IEEE Transactions on Knowledge And Data Engineering,Volume. 25,pp: 2271 – 2282, 2013.

[16] Kan Yang, Xiaohua Jia, Expressive, Efficient, and Revocable Data Access Control for Multi-Authority cloud Storage, IEEE Transactions on Parallel and Distributed Systems,Volume.25,No 7,pp: 1735 – 1744, 2014.

[17] SaeidAbolfazliBuyyaolfazli, ZohrehSanaei, Ejaz Ahmed, Abdullah Gani and RajkumarBuyya,Cloud-Based Augmentation for Mobile Devices: Motivation, Taxonomies and Open Challenges , ,IEEE Communications Surveys & Tutorials ,Volume.16,pp: 337-368, 2014.

[18] SanaeiZohreh, AbolfazliSacid, Abdullah Gani, Heterogeneity in Mobile Cloud Computing: Taxonomy and Open Challenges, IEEE Communication Survey & Tutorials ,Volume. 16, pp:-369-392, 2014.

[19] InukolluVenkataNarasimha, SailajaArsi and Srinivasa RaoRavuri, Security Issues Associated with Big Data in Cloud Computing,International Journal of Network Security & Its Applications, Volume.6, pp:45-56, 2014.

[20] KhannaLeena and AnantJaiswal, Cloud computing: Security Issues and Description of Encryption Based Algorithm to Overcome Them, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) , Volume 3, pp:279-283, 2013.

[21] Xiaofeng Chen, Jin Li, Xinyi Huang, Jingwei Li, Yang Xiang and Duncan S Wong, Secure Outsourced Attribute-Based Signature, EEE ,,Volume.25,pp: 3285-3, 2014.