A Survey & Analysis of Various Trust Model for Security in Cloud Computing: Issues & Challenges

Mr.Ashish Sharma
ashish55359@yahoo.co.in

Dr.SanjayKumar
sanjaysatyam786@gmail.com

Abstract—Cloud computing enables sharing of data over internet, hence the chances of security attacks also increases. So for the security of Data Sharing or Resources Allocation various Trust Models are implemented which provides security from various attacks. One of the efficient and improved Trust Model is implemented which increases the strength of Security in Cloud Computing [1]. Here in this paper various Trust Models their advantages and limitations are analyzed and com pare on the basis of various parameters. This paper deals with the analysis and survey of all the techniques implemented for Cloud Security so that on the basis of various issues a new and efficient Trust Model is implemented in Future.

Keywords—Cloud Computing, Cloud Service Provider, Trust Model, Load Balancing, Scheduling.

I. INTRODUCTION

Cloud computing (CC) is a promising and emerging technology for the next generation of IT applications. The difficulty and problems in the direction of the quick development of cloud computing are data security and privacy issues. Cloud computing is a capable tool that cost-effectively allows data outsourcing as an examination using Internet tools with elastic provisioning and usage-based pricing [2]. Cloud computing provides a low-cost, scalable, location independent infrastructure for data management and storage that is available anyplace and anytime over the Internet application on cloud storage services such as Drop-Box, Mozy and Memopal are increasing recognition.

Cloud computing has raised the delivery of IT services to a novel stage that carries the console of conventional utilities such as water and electricity to its users. The advantages of Cloud computing, such as cost effectiveness, scalability, and ease of management, encourage more and more friendship and service providers to become accustomed it and present their explanations passing through Cloud computing models. According to a modern review of IT decision makers of huge companies, 68% of the respondents expect that by 2014, more than 50% of their company's IT services will be migrated to Cloud platforms [3]. Cloud computing has become a scalable service consumption and delivery platform. Figure 1 shows the system architecture in cloud computing. In a cloud environment, the cloud provider grips a huge number of distributed examines (e.g. databases, servers, Web services, etc.), which can be offered to expensive for increasing a range of cloud applications. Expensive of cloud applications can prefer from an extensive collection of distributed services when creating cloud applications. These examinations are frequently bring into play distantly through communication links and are enthusiastically put together into the applications. The cloud application designers are located in different geographic and network environments. Since the users invoke services via different communication links, the quality of services they observed are diverse.

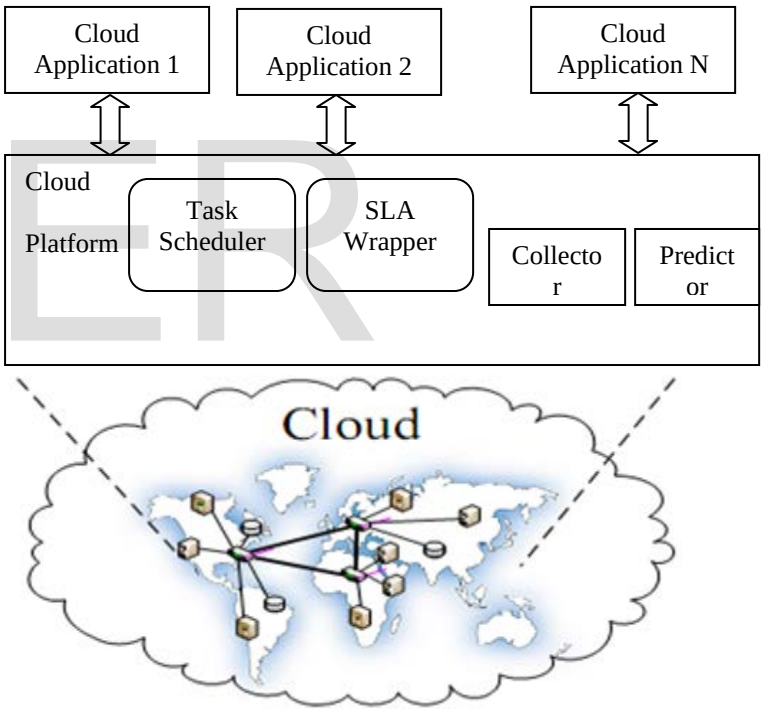

Figure 1: System Architecture of cloud computing.

In Fig. 2, the lower layer represents the different deployment models of the cloud namely private, community, public and hybrid cloud deployment models. The layer just above the deployment layer represents the different delivery models that are utilized within a particular deployment model. These delivery models are the SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) delivery models. These delivery models form the core of the cloud and they exhibit certain characteristics like on-demand

self-service, multi-tenancy, ubiquitous network, measured service and rapid elasticity which are shown in the top layer. These fundamental elements of the cloud require security which depends and varies with respect to the deployment model that is used, the way by which it is delivered and the character it exhibits. Some of the fundamental security challenges are data storage security, data transmission security, application security and security related to third-party resources. This paper is concentrated towards the issues related to the service delivery models. SaaS is a model of software deployment whereby a provider licenses an application to customers for use as a service on demand. One example of SaaS is the Salesforce.com CRM application. IaaS is the delivery of computer infrastructure (typically a platform virtualization environment) as a service. Rather than purchasing servers, software, data center space or network equipment, clients instead buy those resources as a fully outsourced service. One such example of this is the Amazon web services. PaaS is the delivery of a computing platform and solution stack as a service. It facilitates the deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers. PaaS provides the facilities required to support the complete lifecycle of building and delivering web applications and services. An example of this would be GoogleApps.

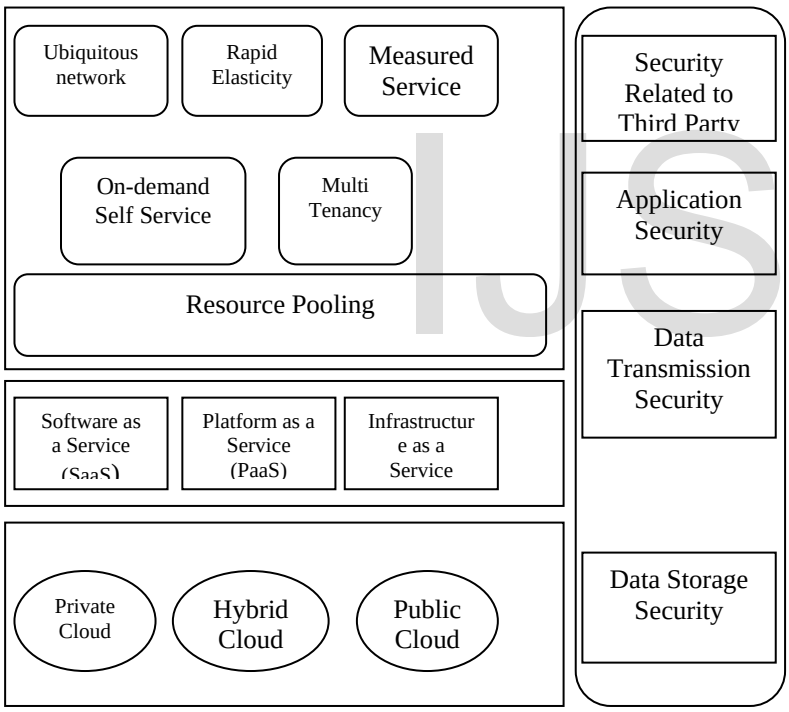

Figure 2: Cloud Computing Security Complexity Model [3]

II. Cloud Security Issues

The Cloud security is besides the focus of this effort. Unlike earlier investigations of cloud security concerns, our vital objective is to make available a much more absolute and methodical reporting of the research literature shared to this topic. We give a wide general idea of publications in the areas of cloud computing security and security of remote storage and computation [4]. In particular, the topics covered in this work include:

- **Client authentication and authorization:** We cover the existing unit of work on techniques for troublesome and developing the border between a cloud provider and its customers more often than not carried out by means of a web browser.
- **Security limitations of hardware virtualization:** We explain the difficulties that have faced along with the enormous exploit of hardware virtualization by cloud providers. We point out how virtualization can be used to acquire illegal information from susceptible clients and also point out improvement methods that can be utilized. As well, we also concentrate on vulnerabilities associated to the procedure and sharing of virtual machine (VM) images.
- **Flooding attacks and denial of service (DoS):** Because cloud computing schemes are planned to level according to the demand for stores, an attacker may utilize that feature to maliciously concentrate huge segments of the cloud's computing power, infuriating the superiority of service that the cloud provides to other simultaneous customers. We talk about dissimilar types of attacks on cloud ease of use and their possible results.
- **Cloud dependability, or its capability to confine and representation illegal action:** We discuss competence that a detained liable scheme should have and explanations for accomplishing this competence most cloud providers incriminate their customers according to the authentic procedure of their infrastructure during a pre-established time slice. In the case of a service that is being flooded this procedure will be understandable high which in its twist will most probable interpret to bills that are much advanced than anticipated.
- **Tests and results for remote storage security:** We describe numerous methods that can be utilized by cloud clients to authenticate reliability of their outsourced data.
- **Security of outsourced calculation:** As a final point, we offer a general idea of existing techniques for promising confidentiality and reliability of outsourced calculations.

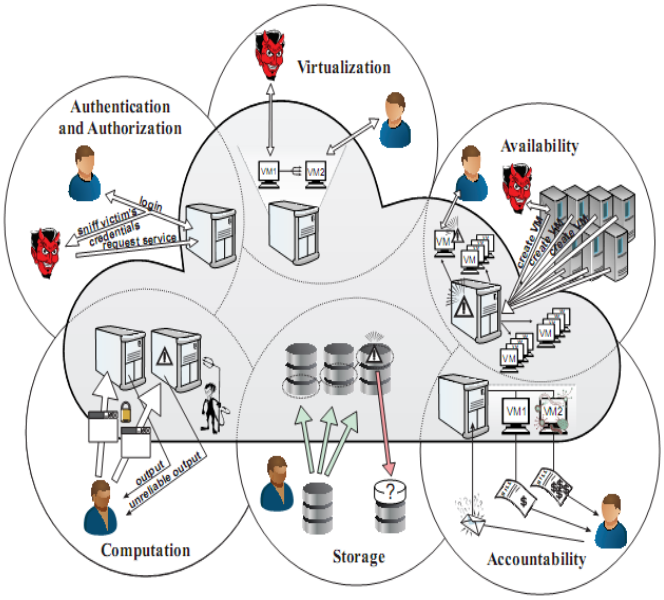

Figure 3: Overview [12] of cloud security issues.

III. LITERATURE SURVEY

Rizwan Shaikh et. al's proposed a new and efficient methodology for the security of clouds by providing trust model [1]. Here in this paper an effective trust model is implanted which computes trust value and hence on the basis Security Strength of the Cloud Computing increases. Trust model can be integrated with the cloud services and their descriptions as a cloud service manager.Cloud service manager stores trust value repository of registered cloud providers and their services. The trust valuemeasures can be used to select a service globally by the users.

Hyukho Kim et. al's implemented a new trust model for the evaluation of Quality of Service of Cloud Computing [5]. Here a new and efficient trust model is implemented for the effective reconfiguration of Cloud Computing resources as well as allocation of resources. The Model collects and analyzes reliability based on historicalinformation of servers in a Cloud data center. Then it prepares the best available resourcesfor each service request in advance, providing the best resources to users.

S. Subashiniet. al's analyses various service delivery models in cloud computing and a survey is done with various advantages and issues over these service delivery models [6]. The paper discusses and analyze the various problem in security model of cloud computing and how to overcome these issues.

	Infrastructure Management	**Infrastructure Ownership**	**Infrastructure Location**	**Access & Consumption**
Public Cloud	Third Party Provider	Third Party Provider	Off-premise	Untrusted
Private/ Community Cloud	Organization or Third Party Provider	Organization or Third Party Provider	On-premise or Off-premise	Trusted
Hybrid Cloud	Both Organization and Third Party Provider	Both Organization and Third Party Provider	Both on-premise and off-premise	Trusted and untrusted

Table : Cloud Service Deployment Model

Manash Sarkar et. al's implemented Fuzzy Reasoning based Trust Model for Cloud Computing [7]. In this paper, a secured andtrusted cloud system is proposed. Security could beembedded in middleware architecture of the cloud system.Threats related to the cloud security are dynamic in natureand recurrently changing the types of attacks encounteredover time. Therefore, a computationally intelligent andadaptive decision mechanism based on fuzzy rules isintroduced to take a proper decision according to thecontextual variables. Fuzzy decision maker identify theanomalies and sustain the trust of the cloud computing.

In this paper [8], author has to solving efficiently the problem of deduplication with differential privileges in cloud computing, here they think about a hybrid cloud architecture consisting of a public cloud and a private cloud. As using existing approach for data deduplication the private cloud is involved as a proxy to permit data owner/users to strongly achieve duplicate check with differential benefits. Such architecture is convenient and has concerned much awareness from make inquiries from data owners only outsource their data storage by utilizing public cloud while the data process is deal with in private cloud. A new method sustaining differential duplicate ensure is proposed under this hybrid cloud architecture where the S-CSP resides in the public cloud. The user is only permitted to execute the duplicate check for files marked with the parallel privileges.

The main goal of this paper is to provide stronger security by encrypting the file with differential privilege keys. In this approach, the users without corresponding privileges cannot achieve the duplicate check. In addition, such unauthorized users cannot decrypt the ciphertext even join together with the S-CSP.

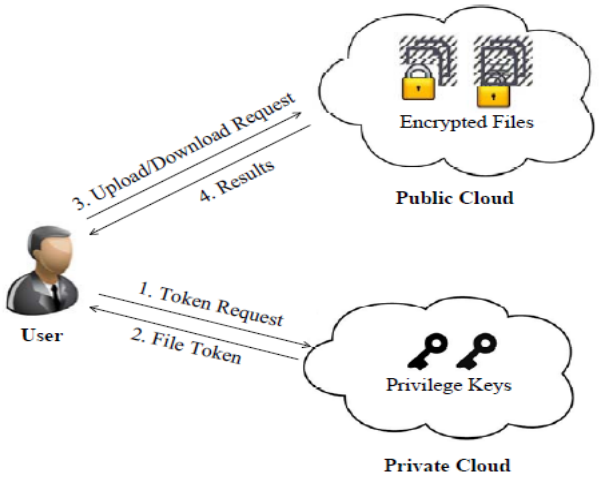

Figure. 4. Architecture for authorized deduplication[8].

As their proposed method has to authorize duplicate check and conduct test-bed experiments to calculate the overhead of the prototype. Security analysis shows that their system is secure in terms of the definitions particular in the proposed security model. Here they show that the overhead is minimal compared to the normal convergent encryption and file upload operations.

To protect the confidentiality author has been proposed [9] to encrypt the data before outsourcing. To enhanced protect data security this paper makes the initial attempt to officially concentrate on the difficulty of authorized data deduplication. Unusual from conventional deduplication systems the degree of difference privileges of users are additional considered in duplicate check as well the data itself. Here they also present common new deduplication constructions sustaining authorized duplicate check in hybrid cloud architecture. Security analysis shows that their method is secure in expressions of the descriptions particular in the anticipated security representation. As a proof of idea, they put into practice a prototype of our proposed approved duplicate check method and behavior testbed experiments using our prototype. We demonstrate that our suggested authorized replica check method bring upon yourself negligible transparency evaluated to normal operations.It keeps the memory by deduplicating the data and thus makes available us with enough memory. It provides authorization to the private firms and protects the confidentiality of the significant data.

To achieve a secure and dependable cloud storage service, a secure multi-owner data sharing method is proposed [10] according to any user in the group so that they can steadily share data with others users by the un-trusted cloud. The Group manager is used for decrease of the execution time of the key generation at the user end or data owner side. Public-key cryptosystem construct constant-size ciphertext as efficient delegation of decryption rights for any set of ciphertexts are achievable. Anyone can comprehensive any set of secret keys and make them as compressed as a single key. The private key proprietor can generate a constant-size aggregate key of ciphertext set in cloud, but another encrypted files outside stay behind secret. The aggregate key strongly sent to users or keep in a smart card with limited storage. We characterize recognized investigation of security in the average model.

In particular, their approach [10] is more flexible than hierarchical key assignment which can only save spaces if all key-holders share a similar set of privileges methods give the first public-key patient-controlled encryption for flexible hierarchy, which was until now to be known. The difficult trouble is how to efficiently share encrypted data. Obviously users can download the encrypted data from the storage, decrypt them then send them to others for sharing, but it loses the value of cloud storage. Users should be able to delegate the access rights of the sharing data to others so that they can access these data from the server directly. However, finding an efficient and make safe way to share unfinished data in cloud storage is not insignificant. An inadequacy of their work is the predefined bounce of the number of maximum ciphertext classes. In cloud storage, the number of ciphertexts more often than not produces quickly. So we have to hold back an adequate amount of ciphertext classes for the upcoming expansion.

In this paper, author [11] presents a new privacy-preserving security solution for cloud services. Here in this method deal with user unspecified access to cloud services and shared storage servers using non-bilinear group signatures to ensure anonymous authentication of cloud service client's user. Users use tamper resistant devices during the generation and storing of user keys to protect against collusion attacks. Here the solution provides registered users with anonymous access to cloud services and also offers anonymous authentication. This signifies that user's personal attributes (age, valid registration, successful payment) can be proven without make knowing user's identity. Consequently, users can use services without any threat of profiling their performance. On the other hand, if users break provider's rules, their access rights are withdrawn. Here we analyze modern privacy preserving solutions for cloud services and summarize our explanation based on advanced cryptographic components it also offers anonymous access, unlink ability and the confidentiality of transmitted data. Due to this fact, cloud service providers using our solution can authenticate more clients in the same time. Additionally, there method gives output the experimental results and measure up to the performance with related solutions.

In this paper author [12] has try to assess how can cloud providers earn their customer's trust and provide the security, privacy and reliability, when a third party is meting out sensitive data in a remote machine established in various countries. A thought of utility cloud has been characterized to provide a variety of services to the users. Various technologies can help to concentrate on the challenges of security, privacy and trust in cloud computing. Unfortunately, the implementation of cloud computing came before the suitable technologies become visible to deal with the supplementary confronts of trust. This opening between implementation and improvement is so extensive that cloud computing consumers don't fully expectation this innovative way of computing. To

close this opening, we require identifying with the trust issues join together with cloud computing from both a technology and business perception. Then we'll be able to establish which up-and-coming technologies could best address these problems. Here the author [12] has analyzed the trusted computing in the cloud computing environment and the function of trusted computing platform in cloud computing. The advantages of this move toward are to make bigger the trusted computing technology into the cloud computing environment to accomplish the trusted computing prerequisites for the cloud computing and then accomplish the trusted cloud computing. The significance of trust varies from organization to organization, depending on the data's value. Additionally, the less expectation an endeavor has in the cloud provider, the more it wants to be in charge of its data smooth the technology. On the other hand, it's fundamental that consumers and providers change their way of thinking's. Trusting cloud computing might differ from trusting other systems, but the objective stay behinds the same to improve business and continue aggressive by take advantage of the advantages of a new technology. Any new technology must progressively build its standing for good presentation and security, earning user's trust over time. We will make more protocol to make available high security for security management, Business continuity management, Identity & access management, Privacy & data protection and application Integrity in the future.

S. No.	Paper	Author/Year of Publication	Technique Used
1.	Trust Model for Measuring Security Strength of Cloud Computing Service [1].	Rizwana Shaikh, Dr. M. Sasikumar, International Conference on Advanced Computing Technologies and Applications, Elsevier,2015	Here in this paper an effective trust model is implanted which computes trust value and hence on the basis Security Strength of the Cloud Computing increases. Trust model can be integrated with the cloud services and their descriptions as a cloud service manager.Cloud service manager stores trust value repository of registered cloud providers and their services. The trust valuemeasures can be used to select a service globally by the users.
2.	Achieving Secure, Scalable and Fine-grained Data Access Control in Cloud Computing [13].	Shuchengyu, Cong Wang, Kui Ren and Wenjing Lou, IEEE Communication Society, 2010.	This paper addresses Security challenging openissue by, on one hand, defining and enforcing access policies basedon data attributes, and, on the other hand, allowing the dataowner to delegate most of the computation tasks involved in finegraineddata access control to untrusted cloud servers withoutdisclosing the underlying data contents.
3.	User Friendly and Secure Architecture (UFSA) for Authentication of Cloud Services [14].	Reza Fathi, Mohsen Amini, Ernst L. Leiss, 8th International Conference on Cloud Computing, 2015.	Here a multi-factor authentication architecture that aims at minimizing the perceived authentication hardship for cloud users while improving the securityof the authentication. To achieve the goal, our authentication architecture suggests a progressive manner to leverage access to different levels of cloud services. At each level, the architectureasks for authentication factors by considering the perceivedhardship for users. To increase

			the security and user convenience,the architecture also considers implicit authentication factors inaddition to the explicit factors.
4.	TTS: A Study of Trusted Tenant System in Cloud Computing Environment [15].	Mr. KundanKunal, Dr. L.G. Malik, IEEE Sponsored 2nd International Conference Innovations in Information Embedded and Communication Systems, 2015.	Here a new architecture is proposed which isTrusted Tenant System (TTS). This TTS introduced in cloudcomputing to provide the trust to data security. 1) TTS meets thesecurity to uploaded data using the AES encryption algorithm.2)TTS share the cloud data by Tunneledtransport layer security(TTLS).In this paper combined technique for data security incloud which explore probably a higher level of security in cloudcomputing to outsourced data .
5.	Privacy-Preserving Public Auditing forSecure CloudStorage [16]	Cong Wang, Qian Wang, Kui Ren	A secure cloud storage systemsupporting privacy-preserving public auditing.
6.	Secure Ranked Keyword Search over Encrypted Cloud Data [17].	Cong Wang, Ning Cao, Jin Li, Kui Ren, and Wenjing Lou	Here define and solve the problem of effective yet secure ranked keyword search over encryptedcloud data.
7.	Towards Secure Multikeyword top-k retrieval over encrypted cloud data [18].	Jiadi Yu, Peng Lu, YanminZhu .	A two-round searchable encryption (TRSE) scheme that supportstop-k multikeyword retrieval.
8.	Dynamic Multi-keyword Top-k Ranked Search over Encrypted Cloud Data [19].	Xingming Sun, Xinhui Wang, Zhihua Xia, Zhangjie Fu and Tao Li .	A secure and efficient multi-keyword ranked search scheme over encrypted data, which additionally supports dynamic update operations like deletion and insertion of documents.
9.	An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds [20].	Seung Hyun Seo, Xiaoyu Ding, IEEE Transanction 2014.	Here propose a mCL-PKE scheme without using pairing operations. Here apply mCL-PKE scheme to construct a practical solution to the problem of sharing sensitive information in public clouds. The cloud is employed as a secure storage as well as a key generation center.
10.	Improving Security and Efficiency in Attribute-Based Data Sharing [21].	Hur, Junbeom, IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 10, pp. 2271 – 2282, October 2013.	Here novel CP-ABE attribute based data sharing technique is used which solves key escrow problem and user revocation problem.

References

[1] Rizwan Shaikh, Dr. M. Sasikumar," Trust Model for Measuring Security Strength of Cloud Computing Service", *Elsevier*, 2015.

[2] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, et al., "Above the clouds: A berkeley view of cloud computing," Technical Report UCB/EECS-2009-28, Dept. EECS, UC Berkerely, 2009.

[3] B. Narasimhan and R. Nichols, "State of cloud applications and platforms: The cloud adopters' view," Computer, vol. 44, no. 3, pp. 24–28, 2011.

[4] Everaldo Aguiar, Yihua Zhang, and Marina Blanton, "An Overview of Issues and Recent Developments in Cloud Computing and Storage Security" 2012.

[5] Hyukho Kim, Hana Lee, Woongsup Kim, Yangwoo Kim," A Trust Evaluation Model for QoS Guarantee in Cloud Systems", *International Journal of Grid and Distributed Computing*, Vol. 3, No.1, March, 2010.

[6] S. Subashini, V. Kavitha," A Survey on Security issues in Service models of Cloud Computing ", *Journal of Network and Computer Applications. Elsevier*, 2011.

[7] Manash Sarkar, Soumya Banerjee, Valentina E. Balas," Configuring Trust Model for Cloud Computing: Decision Exploration using Fuzzy Reasoning", *IEEE 19th International Conference on Intelligent Engineering Systems*, 2015.

[8] Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P. C. Lee, Wenjing Lou, "A Hybrid Cloud Approach for Secure Authorized Deduplication", IEEE Transactions on Parallel and Distributed Systems, 2014.

[9] N.B. Kadu, Mr. Amit Tickoo, Mr.Saurabh I. Patil, Mr. Nilesh B. Bhagat , Mr. Ganesh B. Divte, "A Hybrid Cloud Approach for Secure Authorized Deduplication" International Journal of Scientific and Research Publications, Volume 5, Issue 4, April 2015.

[10] Gade Swati,Prof.Prashant Kumbharkar, "Cryptosystem For Secure Data Sharing In Cloud Storage" IJIRT Volume 1 Issue 6 2014.

[11] Lukas Malina and Jan Hajny, "Efficient Security Solution for Privacy-Preserving Cloud Services" 6th International Conference On Telecommunications Signal Processing Year 2013.

[12] Pardeep Kumar, Vivek Kumar Sehgal, Durg Singh Chauhan, P. K. Gupta and Manoj Diwakar, "Effective Ways of Secure, Private and Trusted Cloud Computing "JCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011.

[13] Shuchengyu, Cong Wang, Kui Ren and Wenjing Lou," Achieving Secure, Scalable and Fine-grained Data Access Control in Cloud Computing", IEEE Communication Society, 2010.

[14] Reza Fathi, Mohsen Amini, Ernst L. Leiss," User Friendly and Secure Architecture (UFSA) for Authentication of Cloud Services", 8th International Conference on Cloud Computing, 2015.

[15] Mr. KundanKunal, Dr. L.G. Malik," TTS: A Study of Trusted Tenant System in Cloud Computing Environment", IEEE Sponsored 2nd International Conference Innovations in Information Embedded and Communication Systems, 2015.

IV. [16] C. WANG ; S. S. M. CHOW ; Q. WANG ; K. REN ," PRIVACY-PRESERVING PUBLIC AUDITING FOR SECURE CLOUD STORAGE ", IEEE TRANSACTIONS ON COMPUTERS, 2011.

[17] Cong Wang, Ning Cao, Jin Li, Kui Ren, and Wenjing Lou," Secure Ranked Keyword Search over Encrypted Cloud Data", Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference, 2010.

[18] Jiadi Yu, Peng Lu, Yanmin Zhu," Towards Secure Multi keyword top-k retrieval over encrypted cloud data", IEEE Transactions on Dependable and Secure Computing, 2013.

[19] Xingming Sun, Xinhui Wang, Zhihua Xia, Zhangjie Fu and Tao Li," Dynamic Multi-keyword Top-k Ranked Search over Encrypted Cloud Data", International Journal of Security and its applications, 2014.

[20] Seung Hyun Seo, Xiaoyu Ding," An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds", IEEE Transanction 2014.

[21] Hur, Junbeom. "Improving security and efficiency in attribute-based data sharing", IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 10, pp. 2271 – 2282, October 2013.