ISSN No. 0976-5697

Volume 8, No. 3, March – April 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Survey on Data Security Issues in Cloud Computing

Sanjay Kumar
M.TECH CSE
Department of Computer Science
BBAU Lucknow, U.P., India

Ram Singar Verma
(Assitant Professor)
Department of Computer Science
BBAU Lucknow, U.P., India

Kuber Mohan
M.TECH CSE
Department of Computer Science
BBAU Lucknow, U.P., India

Abstract: Cloud Computing is a way to deal with fabricate the breaking point or incorporate capacities effectively without placing assets into new system, planning new staff, or approving new programming. They have various potential purposes of intrigue and various attempt applications and data are moving to open or half and half cloud. However, regarding some business-fundamental applications, the affiliations, especially considerable attempts, still wouldn't move them to cloud. The market gauge the Cloud Computing shared is as yet far behind the one expected. From the clients' perspective, Cloud Computing security concerns, especially data security and security confirmation issues, remain the basic inhibitor for gathering of Cloud Computing organizations. In this paper, we present a diagram on data security and security protection issues related with Cloud Computing over all periods of data life cycle.

Firstly,, we moreover focus a related works and after that we show unpretentious components of Cloud Computing security issues, and a short time later data security and insurance affirmation issues, and a while later we display some present courses of action in cloud. Finally, we look at future work about data security and security affirmation issues in cloud.

Keywords: cloud computing; security deployment; privacy protection infrastructure.

I. Introduction

Cloud computing is the idea that data and programs can be stored centrally, in the cloud, and accessed anytime from anywhere through thin clients and lightweight mobile devices. This brings many advantages, including data ubiquity, flexibility of access, and resilience. In many ways, it also enhances security: the cloud provider may be able to afford to invest in better and more up to-date security technologies and practices than the data owner can. However, since cloud computing necessarily puts data outside of the control of the data owner, it inevitably introduces security issues too. Throughout computer science history, numerous attempts have been made to disengage users from computer hardware needs, from time-sharing utilities envisioned in the 1960s, network computers of the 1990s, to the commercial grid systems of more recent years. This abstraction is steadily becoming a reality as a number of academic and business leaders in this field of science are increase towards cloud computing. Cloud computing is an innovative Information System architecture, a driving force demanding from its audience to reorganize their understanding of operating systems, client–server architectures, and browsers. Cloud computing has leveraged users from hardware requirements, while reducing overall client side requirements and complexity. From initial concept building to current actual deployment, cloud computing is growing more and more grown-up. Nowadays, many organizations, especially Small and Medium Business enterprises, are increasingly realizing the benefits by putting their applications and data into the cloud. The adoption of cloud computing may lead to gains in efficiency and effectiveness in developing and deployment and save the cost in purchasing and maintaining the infrastructure. The cloud computing model, the most widely used one is made by NIST as “Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models”. I) The cloud computing model NIST defined has three service models and four deployment models. The three service models, also called SPI model, are: Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS) and Cloud Infrastructure as a Service (IaaS). The four deployment models are: Private cloud, Community cloud, Public cloud and Hybrid cloud. Compared with the traditional IT model, the cloud computing has many potential advantages. But from the consumer’s is the possibility that information and projects can be put away midway, in the cloud, and got to at whatever time from anyplace through thin customers and lightweight cell phones. This brings many points of interest, including information pervasiveness, adaptability of get to, and strength. From multiple points of view, it likewise upgrades security: the cloud supplier might have the capacity to stand to put resources into better and more breakthrough security advancements and practices than the information proprietor can. Notwithstanding, since Cloud Computing essentially puts information outside of the control of the information proprietor, it unavoidably presents security issues as well. All through software engineering history, various endeavors have been made to separate clients from PC equipment needs, from time-sharing utilities imagined in the 1960s, arrange PCs of the 1990s, to the business network frameworks of later years. This deliberation is consistently turning into a reality as various scholarly and business pioneers in this field of science are increment towards Cloud Computing. Cloud Computing is an inventive Information System engineering, a main thrust requesting from its crowd to rearrange their comprehension of working frameworks, client–server models, and programs. Cloud Computing has utilized clients from equipment necessities, while decreasing general customer side prerequisites and many-sided quality. From introductory idea working to current real sending, Cloud Computing is developing increasingly grown-up. These days, numerous associations, particularly Small and Medium Business endeavors, are progressively understanding the advantages by putting their applications and information into the cloud. The reception of Cloud Computing may prompt picks up in proficiency and adequacy in creating and arrangement and spare the cost in acquiring and keeping up the foundation. The Cloud Computing model, the most broadly utilized one is made by NIST as "Cloud Computing is a model for empowering advantageous, on-request arrange access to a common pool of configurable registering assets, for example, systems, servers, stockpiling, applications, and administrations that can be quickly provisioned and discharged with negligible administration exertion or specialist organization collaboration. This cloud display advances accessibility and is made out of five fundamental attributes, three administration models, and four arrangement models". I) The Cloud Computing model NIST characterized has three administration models and four organization models. The three administration models, likewise called SPI model, are: Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS) and Cloud Infrastructure as a Service (IaaS). The four sending models are: Private cloud, Community cloud, Public cloud and Hybrid cloud. Contrasted and the customary IT show, the Cloud Computing has numerous potential focal points. Be that as it may, from the shopper's point of view, Cloud Computing security concerns remain a noteworthy hindrance for the selection of Cloud Computing. II) The essential reason not to utilize Cloud Computing administrations is that there are information security and protection concerns. Despite the fact that Cloud Computing specialist co-ops touted the security and dependability of their administrations, real sending of Cloud Computing administrations is not as protected and solid as they claim. In 2009, the real Cloud Computing merchants progressively seemed a few mischances. Amazon's Simple Storage Service was interfered with twice in February and July 2009. This mischance brought about some system locales depending on a solitary sort of capacity administration were compelled to a stop. In March 2009, security vulnerabilities in Google Docs even prompted genuine spillage of client private data. Google mail additionally showed up a worldwide disappointment up to 4 hours. It was uncovered that there was not kidding security defenselessness in VMware virtualization programming for Mac form in May 2009. Individuals with shrouded intentions can exploit the defenselessness in the Windows virtual machine on the host Mac to execute malignant code. Microsoft's Azure Cloud Computing stage likewise occurred a genuine blackout mishap for around 22 hours. Genuine security occurrences even prompt crumple of Cloud Computing sellers. As directors' abuse prompting loss of 45% client information, cloud storage seller Link-Up had been compelled to close. Security control measures in cloud are like ones in customary IT condition. Conventional security issues are as yet present in Cloud Computing situations. However, as big business limits have been reached out to the cloud, customary security systems are no longer appropriate for applications and information in cloud. Because of the openness and multi-occupant normal for the cloud, Cloud Computing is bringing enormous effect on data security field:

- Due to element versatility, benefit deliberation, and area straightforwardness components of Cloud Computing models, a wide range of utilizations and information on the cloud stage have no settled foundation and security limits. In case of security break, it's hard to disengage a specific physical asset that has a danger or has been traded off
- According to the administration conveyance models of cloud computing, assets cloud administrations in view of might be possessed by various suppliers. As there is an irreconcilable circumstance, it is hard to send a bound together safety efforts..
- As the openness of cloud and sharing virtualized assets by multi-inhabitant, client information might be gotten to by other unapproved clients.
- As the cloud stage needs to manage huge data stockpiling and to convey a quick get to, cloud safety efforts need to address the issue of gigantic data handling.

This paper depicts information security and protection assurance issues in cloud. This paper is composed as takes after: In segment II, we introduce a related works. In area III, points of interest of Cloud Computing security issues. In area IV, we talk about information security and protection insurance issues related with Cloud Computing over all phases of data life cycle. In area V, indicates current answers for information security and security insurance issues in cloud. In segment VI, at long last we finish up and future work.

II. RELATED WORKS

Ryan M. D has talked about quickly review issues in Cloud Computing security. The way that information are imparted to the cloud specialist co-op is distinguished as the center logical issue that isolates Cloud Computing security from different points in processing security. They study three flow explore bearings, and assess them as far as a running programming as-an administration case [1]. Han S. also, J. Xing have talked about the issue of information stockpiling security in Cloud Computing. A novel outsider reviewer plan is proposed. The undeniable preferred standpoint of our plan is the cloud specialist organization can offer the capacities which were given by the customary outsider examiner and make it trustful. So it in fact decreases the constitution's multifaceted nature in Cloud Computing [2]. S Sakthivel, B Dhiyanesh have propose a protection safeguarding open inspecting framework for information stockpiling security in Cloud Computing, where TPA can play out the capacity examining without requesting the nearby duplicate of information. We use the homomorphism authenticator and irregular cover method to ensure that TPA would not take in any information about the information content put away on the cloud server amid the productive reviewing process, which not just dispenses with the weight of cloud client from the dull and potentially costly evaluating assignment, additionally reduces the clients' dread of their outsourced information spillage. Considering TPA may simultaneously deal with numerous review sessions from various clients for their outsourced information records, we additionally develop our security protecting open examining convention into a multi-client setting, where TPA can play out the different evaluating assignments in a cluster way, i.e., all the while. Broad security and execution examination demonstrates that the proposed plans are provably secure and very productive. We trust every one of these favorable circumstances of the proposed plans will reveal insight into economies of scale for Cloud Computing [3].

Wang Q., Wang C et al., they have accomplished in this paper takes a shot at guaranteeing remote information uprightness frequently does not have the support of either open review capacity or element information operations. They first distinguish the challenges and potential security issues of direct expansions with completely dynamic information refreshes from earlier works and after that demonstrate to develop a rich confirmation conspire for the consistent coordination of these two remarkable components in our convention outline. Specifically, to accomplish proficient information progression, they enhance the current evidence of capacity models by controlling the great Merle Hash Tree development for square label verification. To bolster productive treatment of different evaluating assignments, they additionally investigate the strategy of bilinear total mark to augment our fundamental outcome into a multi-client setting, where TPA can play out numerous reviewing errands all the while. Broad security and execution investigation demonstrate that the proposed plans are exceedingly productive and provably secure [4]. Ren K., Cao N. et al., they have propose in this paper an adaptable conveyed stockpiling honesty reviewing component, using the homomorphism token and dispersed deletion . coded information. They proposed configuration permits clients to review the distributed storage with extremely lightweight correspondence and calculation cost. The examining result guarantees solid distributed storage accuracy ensure, as well as all the while accomplishes quick information blunder confinement, i.e., the recognizable proof of getting into mischief server. Considering the cloud information are rapid in nature, the proposed configuration additionally bolsters secure and proficient element operations on outsourced information, including square adjustment, erasure, and annex. Investigation demonstrates the proposed plan is profoundly effective and versatile against Byzantine disappointment, noxious information change assault, and much server conspiring assaults [5].

III. CLOUD COMPUTING SECURITY ISSUSES

A. *Cloud Computing Security*

Cloud Computing security concerns every one of the parts of making Cloud Computing secure. A large number of these viewpoints are not one of a kind to the cloud setting: information is defenseless against assault regardless of where it is put away. In this manner, Cloud Computing security incorporates every one of the points of figuring security, including the plan of security designs, minimization of assault surfaces, insurance from malware, and requirement of get to control. In any case, there are a few parts of Cloud Computing security that seem, by all accounts, to be particular to that domain.

1 The cloud is typically a shared resource, and different sharers (called inhabitants) might be assailants.

2 Cloud-based information is typically purposefully generally available by conceivably unreliable conventions and APIs crosswise over open systems.

3 Data in the cloud is helpless against being lost (e.g., inadvertently erased) or inaccurately altered by the cloud supplier.

4 Data in the cloud can be gotten to by the cloud supplier, its subcontractors and workers

As cloud computing is accomplishing expanded fame, concerns are being voiced about the security issues presented through the reception of this new model. The adequacy and proficiency of customary security components are being reevaluated, as the attributes of this inventive sending model, contrast broadly from them of conventional designs. In this paper we endeavor to demystify the one of a kind security challenges presented in a cloud situation and elucidate issues from a security point of view. The idea of trust and security is researched and particular security prerequisites are recorded. This paper proposes a security arrangement, which use customers from the security trouble, by confiding in a Third Party. The Third Party is entrusted with guaranteeing particular security attributes inside an appropriated data framework, while understanding a trust work between included elements, shaping leagues of mists. The examination philosophy embraced towards accomplishing this objective, depends on programming engineering and data frameworks configuration approaches. The fundamental strides for planning the framework design incorporate the gathering of necessities and the investigation of theoretical utilitarian determinations. Cloud computing security, for example, once in a while alluded to just as cloud security, is a developing sub-area of PC security, organize security, and, all the more comprehensively and data security. It alludes to an expansive arrangement of approaches, advancements, and controls sent to secure information, applications, and the related foundation of cloud computing.

B. *Security Issues Associated with the Cloud*

There are numerous security issues related with cloud computing and they can be assembled into any number of measurements.

As per Gartner [6], before settling on a decision of cloud merchants, clients ought to approach the sellers for seven particular wellbeing issues: Privileged client get to, administrative consistence, information area, information isolation, recuperation, investigative support and long haul practicality. In 2009, Forrester Research Inc. [7] assessed security and protection practices of a portion of the main cloud suppliers, (for example, Salesforce.com, Amazon, Google, and Microsoft) in three noteworthy angles: Security and protection, consistence, and legitimate and legally binding issues. Cloud Security Alliance (CSA) is social affair arrangement suppliers, non-benefits and people to go into exchange about the present and future prescribed procedures for data affirmation in the cloud [8]. S. Subashini and V. Kavitha made an examination of cloud computing security issues from the cloud computing administration conveyance models (SPI model) and give a point by point investigation and appraisal strategy portrayal for every security issue [9]. Mohamed Al Morsy et al, have investigated the cloud computing security issues from alternate points of view, incorporating security issues related with cloud computing engineering, benefit conveyance models, cloud qualities and cloud partners [10]. The engineering of Cloud registering security is given beneath, and benefit conveyance models, there are some security issues in all parts of the framework including system level, have level and application level

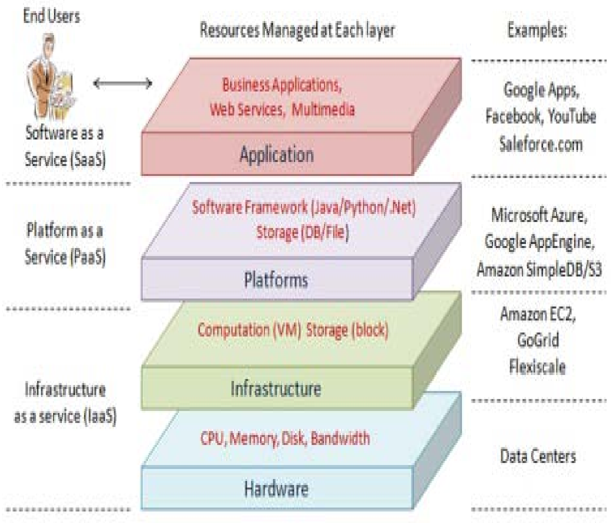
End Users
Resources Managed at Each layer
Examples:
Business Applications, Web Services, Multimedia
Application
Google Apps, Facebook, YouTube Saleforce.com
Software as a Service (SaaS)
Software Framework (Java/Python/.Net) Storage (DB/File)
Platforms
Platform as a Service (PaaS)
Microsoft Azure, Google AppEngine, Amazon SimpleDB/S3
Computation (VM) Storage (block)
Infrastructure
Amazon EC2, GoGrid Flexiscale
Infrastructure as a service (IaaS)
CPU, Memory, Disk, Bandwidth
Hardware
Data Centers

Figure 1. Cloud computing security architecture

IV. DATA SECURITY AND PRIVACY PROTECTION ISSUES

The substance of data security and security assurance in cloud is like that of customary information security and security insurance. It is likewise required in each phase of the information life cycle. But since of openness and multi-occupant normal for the cloud, the substance of data security and security insurance in cloud has its particularities.

The idea of security is altogether different in various nations, societies or locales. The definition embraced by Organization for Economic Cooperation and Development is "any data identifying with a recognized or identifiable individual (information subject) [11]." Another well known definition gave by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) in the Generally Accepted Privacy Principles (GAPP) standard are "The rights and commitments of people and associations regarding the accumulation, utilize, maintenance, and exposure of individual data." Generally, protection is related with the gathering, utilize, divulgence, stockpiling, and annihilation of individual information. ID of private data relies on upon the particular application situation and the law, and is the essential assignment of protection assurance The following a few segments examine data security and security insurance issues in cloud around the information life cycle.

A. Data Life Cycle

Data life cycle refers to the whole procedure from era to decimation of the data. The data life cycle is partitioned into seven phases, appeared in figure below:

Phase1: Data Generation

Data generation is included in the data proprietorship. In the conventional IT condition, typically clients or associations possess and deal with the information. In any case, if information is to be relocated into cloud, it ought to be viewed as that how to keep up the information possession. For individual private data, information proprietors are qualified for comprehend what individual data being gathered, and sometimes, to stop the accumulation and utilization of individual data.

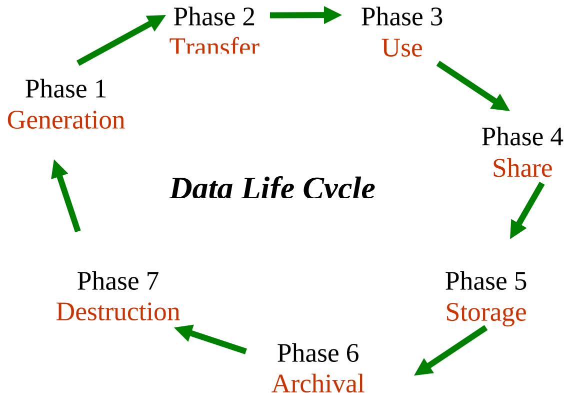

Figure 2: Data life cycle

Phase2: Transfer

Inside the venture limits, data transmission as a rule does not require encryption, or simply have a straightforward data encryption measure. For data transmission crosswise over big business limits, both data classification and uprightness ought to be guaranteed so as to keep information from being tapped and altered by unapproved clients. At the end of the day, just the information encryption is insufficient. Information uprightness is likewise should have been guaranteed. Along these lines it ought to guarantee that vehicle conventions give both privacy and respectability. Privacy and honesty of information transmission need to guarantee between big business stockpiling and cloud storage as well as between various cloud storage administrations. At the end of the day, classification and honesty of the whole exchange procedure of data ought to be guaranteed.

Phase3: Use

For the static data utilizing a simple storage service,, for example, Amazon S3, data encryption is practical. In any case, for the static data utilized by cloud-based applications in PaaS or SaaS demonstrate, data encryption much of the time is not possible. Since data encryption will prompt issues of ordering and inquiry, the static data utilized by Cloud-based applications is for the most part not encoded. In cloud, as well as in customary IT condition, the data being dealt with is practically not encoded for any program to manage. Due to the multi-inhabitant highlight of cloud computing models, the data being set up by cloud based applications is put away together with the data of different clients. Decoded data in the process is a genuine danger to information security. With respect to utilization of private data, circumstances are more confounded. The proprietors of private data need to concentrate on and guarantee whether the utilization of individual data is steady with the reasons for data accumulation and whether individual data is being imparted to outsiders, for instance, cloud specialist organizations.

Phase4: Share

Data sharing is growing the utilization scope of the data and renders data authorizations more mind boggling. The data proprietors can approve the data access to one gathering, and thusly the gathering can additionally share the data to another gathering without the assent of the information proprietors. Thusly, amid data sharing, particularly when imparted to an outsider, the data proprietors need to consider whether the outsider keeps on keeping up the first security measures and utilization limitations. With respect to of private information, notwithstanding approval of data, sharing granularity and data change are likewise should be worried about. The sharing granularity relies on upon the sharing arrangement and the division granularity of substance. The data change refers to separating delicate data from the first data. This operation makes the data is not pertinent with the data proprietors.

Phase5: Storage

The data in the cloud might be isolated into: (i) The data in IaaS condition, for example, Amazon's Straightforward Stockpiling Administration; (ii) The data in PaaS or SaaS condition identified with cloud based applications. The data put away in the cloud stockpiles is comparative with the ones put away in different places and needs to consider three parts of data security: secrecy, honesty and accessibility. The basic answer for data privacy is data encryption. To guarantee the viable of encryption, there necessities to consider the utilization of both encryption algorithm and key quality. As the cloud computing condition including a lot of data transmission, stockpiling and dealing with, there likewise needs to consider handling speed and computational productivity of encoding a lot of data. For this situation, for instance, symmetric encryption calculation is more appropriate than uneven encryption calculation. Another key issue about data encryption is key administration. Is who in charge of key administration? In a perfect world, it's the data proprietors. Be that as it may, at present, on the grounds that the clients have insufficient mastery to deal with the keys, they more often than not depend the key administration to the cloud suppliers. As the cloud suppliers need to keep up keys for countless, key administration will turn out to be more unpredictable and troublesome.

Phase6: Archival

Archiving for data concentrates on the capacity media, regardless of whether to give off-site stockpiling and capacity length. On the off chance that the data is put away on compact media and afterward the media is crazy, the data are probably going to go out on a limb of spillage. In the event that the cloud specialist co-ops don't give off-site documenting, the accessibility of the data will be debilitated. Once more, regardless of whether capacity term is reliable with archival prerequisites? Something else, this may bring about the accessibility or protection dangers.

Phase7: Destruction

At the point when the data is did not require anymore, regardless of whether it has been totally wrecked? Because of the physical qualities of capacity medium, the data erased may at present exist and can be reestablished. This may bring about unintentionally reveal of touchy data.

V. CURRENT SECURITY SOLUTIONS FOR DATA SECURITY AND PRIVACY PROTECTION

IBM built up a completely homomorphism encryption conspire in June 2009. This plan permits data to be handled without being decrypted[12]. This framework can avoid security spillage without approval in Map-Reduce computing process. A key issue for data encryption arrangements is key administration. From one viewpoint, the clients have insufficient ability to deal with their keys. Then again, the cloud specialist co-ops need to keep up an expansive number of client keys. The Association for the Headway of Organized Data Benchmarks (Desert garden) Key Management Interoperability Protocol (KMIP) is attempting to understand such issues [13].

About data honesty check, in light of data correspondence, exchange charges and time cost, the clients can not first download data to confirm its accuracy and after that transfer the data. What's more, as the data is powerful in cloud storage, traditional uprightness arrangements are no longer appropriate. NEC Labs provable information uprightness (PDI) arrangement can bolster open data trustworthiness check [14]. Cong Wang proposed a numerical approach to confirm the trustworthiness of the data powerfully put away in the cloud [15].

In the data storage and utilize stages, Mow-bray proposed a client based security management tool. It gives a client driven trust model to help clients to control the capacity and utilization of their delicate data in the cloud. Munts-Mulero talked about the issues that current security assurance advancements, (for example, K unknown, Diagram Anonymization, and data pre-preparing techniques) confronted when connected to huge data and examined current arrangements [16]. The test of information security is sharing information while ensuring individual protection data. Randike Gajanayake proposed a security insurance system in view of data responsibility (IA) segments [17]. The IA operator can recognize the clients who are getting to data and the sorts of data they utilize. At the point when unseemly abuse is recognized, the specialist characterizes an arrangement of techniques to consider the clients responsible for abuse. About information demolition, U.S. Division of Protection (DoD) 5220.22-M (the National Mechanical Security Program Working Manual) indicates two endorsed techniques for information (pulverization) security, however it doesn't give a particular prerequisites to how these two strategies are to be accomplished [18].

VI. CONCLUSION

The cloud computing has many points of interest and there are as yet numerous real issues that should be tackled. As per administration conveyance models, arrangement models and fundamental elements of the cloud computing, data security and protection assurance issues are the essential issues that should be unraveled as quickly as time permits. Data security and protection issues exist in all levels in SPI benefit conveyance models and in all phases of data life cycle. The difficulties in security insurance are sharing data while ensuring individual data. The run of the mill frameworks that require security insurance are online business frameworks that store Visas and medicinal services frameworks with wellbeing data. The capacity to control what data to uncover and who can get to that data over the Web has turned into a developing concern. These worries incorporate whether individual data can be put away or read by outsiders without assent, or whether outsiders can track the sites somebody has gone by. Another worry is whether sites which are gone by gather, store, and potentially share individual data about clients. The way to security assurance in the cloud condition is the strict partition of touchy data from non-delicate data took after by the encryption of delicate components. About the security assurance, protection data distinguishing proof and separation are the essential assignments. We ought to be considered amid the outline of cloud-based applications and usage in future works.

VII. References

[1] Ryan, M. D., ., "Cloud computing security: The scientific challenge, and a survey of solutions. Journal of Systems and Software", 2013.

[2] Han S. & Xing J., "Ensuring data storage security through a novel third party auditor scheme in cloud computing", International Conference on Cloud Computing and Intelligence Systems, IEEE, September 2011.

[3] Sakthivel, S., & Dhiyanesh, B., A privacy-preserving storage security for spatial data in dynamics cloud environment. In Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on, IEEE, July 2013.

[4] Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J., "Enabling public auditability and data dynamics for storage security in cloud computing". IEEE transactions on parallel and distributed systems 2011.

[5] Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W., "Toward secure and dependable storage services in cloud computing". IEEE transactions on Services Computing, 2012.

[6] Brodkin, J., Gartner: Seven cloud-computing security risks. InfoWorld, 2008.

[7] Cloud Security Front and Center. Forrester Research, 2009.

[8] Cloud Security Alliance. http://www.cloudsecurityalliance.org.

[9] S. Subashini, V.Kavitha, "A survey on security issues in service delivery models of cloud computing". Journal of Network and Computer Applications, 2011.

[10] Mohamed Al Morsy, John Grundy, Ingo Müller, "An Analysis of The Cloud Computing Security Problem," in Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.

[11] OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

[12] IBM Discovers Encryption Scheme That Could Improve Cloud Security, Spam Filtering.

[13] OASIS Key Management Interoperability Protocol, TC.

[14] Zeng K, "Publicly verifiable remote data integrity,". Birmingham: Springer, 2008.

[15] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing," in Proceedings of the 17th International Workshop on Quality of Service.2009.

[16] Muntes M., V., and J. Nin. "Privacy and Anonymization for very large datasets." Proceedings of the 18th ACM conference on Information and knowledge management. ACM, 2009.

[17] Randike Gajanayake, Renato Iannella, and Tony Sahama, "Sharing with Care An Information Accountability Perspective," Internet Computing, IEEE, July-Aug. 2011.

[18] DoD, "National Industrial Security Program Operating Manual", 5220.22-M, February 28, 2006.