Volume 7, Issue 1, January 2017 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Data Storage Security in Cloud Computing: A Survey

Dr. S Durga Bhavani
MTech, Ph D, Director & Professor
School of Info. Technology(JNTUH)
Telangana, India

Gudlanarva Sudhakar
Mtech(SE), (Ph D), Lecturer
School of Info Technology(JNTUH)
Telangana, India

Ujjwal Karna
Student, M.Tech(CNIS)
School of Info Technology(JNTUH)
Telangana, India

DOI: 10.23956/ijarcsse/V7I1/0148

Abstract— Cloud processing is the figuring innovation which gives assets like programming, equipment, administrations over the web. Cloud computing gives calculation, programming, information get to and capacity benefits that don't require end-client learning of the physical area and setup of the framework that conveys the administration. Since the information transmission on the web or over any systems are defenceless against the programmer assault. Cloud based information capacity frameworks have numerous complexities with respect to basic, private, delicate information of customer. The trust required on distributed storage is so far had been restricted by clients. The information stockpiling in the cloud has been a promising issue in these days. This is because of the way that the clients are putting away their significant information and data in the cloud. The clients ought to believe the cloud specialist organizations to give security to their information. The cloud specialist organizations likewise giving the security however not up to a total level. The assault of noxious insiders into the cloud and to take the information has been expanded. Information store is fundamental future that cloud benefit gives to the organizations to store gigantic measure of capacity limit. Yet at the same time many organizations are not prepared to actualize distributed computing innovation because of absence of legitimate security control approach and shortcoming in insurance which prompt to many test in distributed computing. This paper deals about the study on various issues identified with information stockpiling security on single cloud and also multi cloud what's more, adaptation to internal failure.

Keywords— Cloud; cloud computing; multiple cloud; service provider; data storage; data security; audit policy; data correctness; data availability; data integrity

I. INTRODUCTION

Cloud computing is the cutting edge in the Internet's innovation which gives the client everything regarding administrations like figuring energy to registering framework, applications, business forms according to the need of client over the web. The "cloud" in distributed computing can be characterized as the arrangement of equipment, systems, stockpiling, administrations, and interfaces that join to convey parts of processing as an administration [1]. Distributed computing has four primary elements: versatility, self-administration of provisioning and need base utilization instalment.

A. Organization Models

There are Four diverse sending models [2] of distributed computing.

1. Open Cloud:

Open or outer cloud is one of sort of cloud in which client can utilize the recourses according to the need and pay for utilization. This kind of cloud likewise has different specialist co-ops who give conventional distributed computing administrations to clients and charged for it.

2. Private Cloud:

Private cloud is the sort of cloud in which the cloud is worked in just a single association or created for one association and oversaw by them or outsider administration gives. Essentially this sort of cloud is for the inner motivation behind association which is worked in topographically circulated.

3. Crossover Cloud:

Crossover Cloud can be made up with the mix of two sort of cloud like private and open cloud or the mix of cloud virtualization server with physical equipment. This sort of cloud is much cost costly contrast with open cloud.

4. Group Cloud:

In the event that few associations have comparative sort of prerequisite, they can share the cloud then this kind of cloud foundation is made conceivable in market. This cloud is additionally exorbitant in contrast with open cloud however gives high level security.

B. Cloud computing:

Distributed computing is offered in various structures: open mists, private mists, and half and half mists, which join both open and private [3].

1. Cloud Software as a Service (SaaS) :

Programming as a Service gives programming or application which can be utilized over the web and client does not have not mindful of any data with respect to working framework, physical equipment. This kind of use can be get to by means of web and through program at client side. Client can have just some of control setting for application.

2. Cloud Platform as a Service (PaaS) :

Stage as a Service give the setup of customer's product bundles and different devices which set up on specialist co-ops' physical equipment over the web. So entire foundation is occur on specialist co-ops' surroundings and client can get to that product after validation prepare passes effectively. This client can free from the equipment disappointment issue by receiving this administration.

3. Cloud Infrastructure as a Service (IaaS) :

In this sort of cloud, client can have entire virtual server and client can get to it as he can get to it neighborhood like begin, stop, and get to and arrange the server. In this kind of administration, client pays just for the limit and model he needs them.

C. Advantages of Cloud Computing

1. Lessening in capital use on equipment and programming organization.
2. Area freedom, the length of there is access to the Internet.
3. Expanded adaptability and market readiness as the brisk organization model of distributed computing builds the capacity to re-arrangement quickly as required.
4. Permits the undertaking to concentrate on its center business.
5. Expanded upper hand.
6. Expanded security at a much lesser cost when contrasted with customary independent applications because of centralization of information and expanded security-centered assets.
7. Simple to keep up as they don't need to be introduced on every client's PC.

The cloud benefits that are executed or those that will be actualized will dependably be joined by a few dangers. Learning about these dangers might turn out to be the initial step to avoid them. Consequently security is the central concern of a few customers who craving to influence cloud administrations. In a wide range of cloud, security issues touch base from numerous points of view in distinctive stages, for example, client's confirmation, open source arrangement, virtual foundation, SLA, information stockpiling and asset request [5]. Out of these, Cloud based information stockpiling frameworks have numerous complexities with respect to basic/classified/delicate information of customer. The trust required on Cloud stockpiling is so far had been constrained by clients [6].

The overview of related research work done on the cloud information stockpiling security is talked about in the paper. The examination traverses the security challenges as for the kind of sending, administration and normal system issues.

II. LITERATURE SURVEY

A. Cloud computing: Storage as a service

Among different advances, distributed computing has brought focal points as online stockpiling. In this segment, Storage-as a-Service is alluded. The scope of administration offerings in this space is astounding, and they are keeping on developing. Information security for such a cloud benefit includes a few viewpoints counting secure channels, get to controls, and encryption. What's more, when we consider the security of information in a cloud, we must consider the security set of three: classification, honesty, and accessibility. In the distributed storage show, information is put away on various virtualized servers. Physically the assets will traverse various servers and can even traverse stockpiling destinations. Among the extra advantages of such for the most part ease administrations are the capacity upkeep errands, (for example, reinforcement, replication, and calamity recuperation), which the CSP performs.

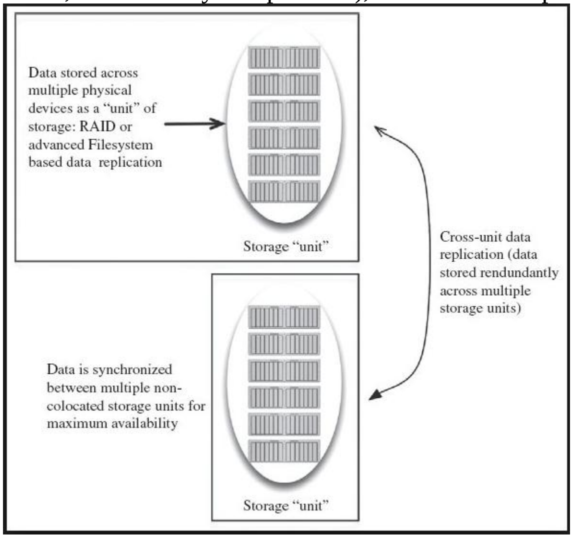
Data stored across multiple physical devices as a "unit" of storage: RAID or advanced Filesystem based data replication
Storage "unit"
Cross-unit data replication (data stored rendundantly across multiple storage units)
Data is synchronized between multiple non-colocated storage units for maximum availability
Storage "unit"

Figure 1: Cloud storage-replication and availability

The most outstanding supplier in this space is Amazon with its S3 (Simple Storage Benefit). Amazon propelled S3 in March of 2006. A typical part of many cloud-based capacity offerings is the unwavering quality furthermore, accessibility of the administration Figure 1 portrays a disconnected perspective of what number of individual plates in many collected stockpiling gadgets are formed into a virtualized unit of capacity. [6]

Replication of information is performed at a low level by such systems as RAID or by a record framework. One such record framework is ZFS, which was composed by Sun Microsystems as both a record framework and a volume director. ZFS underpins high stockpiling limits and plays out various security applicable capacities counting duplicate on-compose cloning and consistent trustworthiness checking alongside programmed repair. One of the later slants in online cloud-based capacity is the distributed storage portal. A few sellers offer such arrangements that are for the most part actualized as a machine that dwells nearby at the client premises. These machines can give numerous elements, counting: Interpretation of customer utilized APIs and conventions, (for example, REST or Cleanser) to those that are utilized by cloud-based capacity administrations (for example, NFS, iSCSI, or Fiber Channel). The objective is to empower coordination with existing applications over standard system conventions.

Reinforcement and recuperation capacities that work with in-distributed storage.On location encryption of information that keeps keys neighborhood to the on location apparatus.

The merchants and items in this space incorporate Gladnet, Nasuni Distributed storage Gateway, StorSimple, and Emulex. The item and arrangements that are accessible are seeing fast changes and new usefulness. Figure 2 portrays a run of the mill distributed storage passage application as it is utilized to enlarge nearby capacity by going about as an on location optional duplicate and as an go-between to the CSP stockpiling administration.

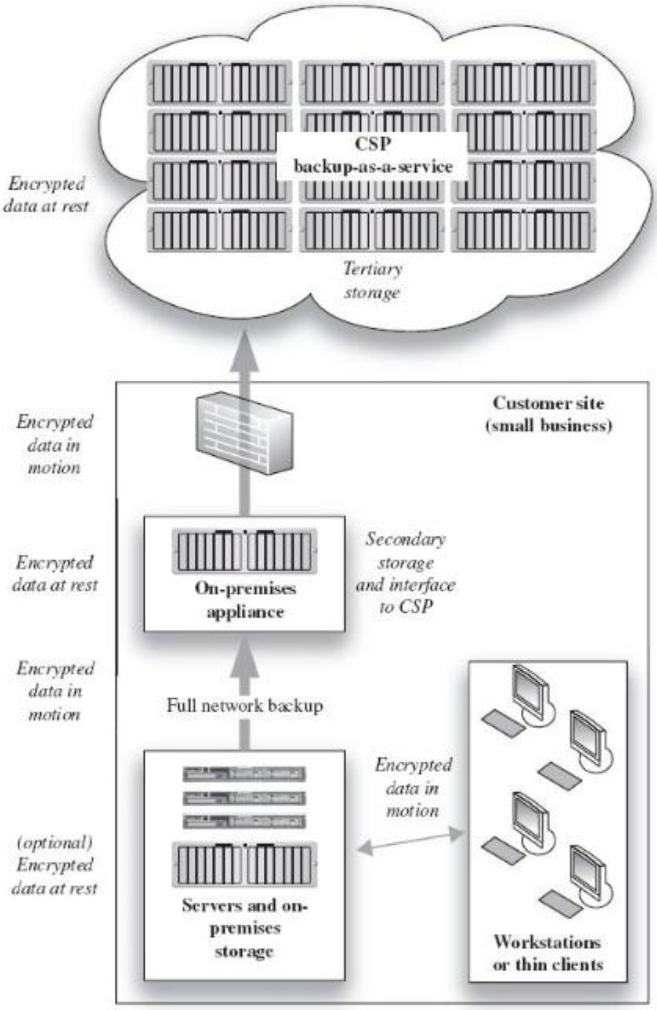

Figure 2: Cloud storage gateway appliance

B. Need for Security Techniques

Customary cryptographic primitives with the end goal of information security assurance cannot be specifically embraced because of the clients' misfortune control of information under Cloud Computing. Along these lines, check of right information stockpiling in the cloud must be led without express learning of the entire information. Distributed computing is not only an outsider information warehouse. The information put away in the cloud might be every now and again upgraded by the clients, including addition, erasure, adjustment, affixing, reordering, and so on. To guarantee stockpiling accuracy under element information overhaul is vital. The sending of Cloud Computing is controlled by server farms running in a concurrent, coordinated and circulated way. Individual client's information is needlessly put away in various physical areas which increment the information honesty dangers.

C. Enabling Public Auditability And Data Dynamics For Storage Security In Cloud Computing

The outsider examiner (TPA), who has aptitude and abilities that cloud clients don't have and is trusted to survey the distributed storage benefit security in the interest of the client upon demand. Clients depend on the CS for cloud information stockpiling and upkeep .They may likewise powerfully connect with the CS to get to and redesign their put away information for different application purposes. The clients may depend on TPA for guaranteeing the capacity security of their outsourced information, while wanting to keep their information private from TPA. The Author considers the presence of a semi-put stock in CS as does. To be specific, in the greater part of time it acts appropriately and does not veer off from the recommended convention execution. In any case, amid giving the cloud information capacity based administrations, for their own particular advantages the CS may disregard to keep or intentionally erase infrequently got to information records which have a place with common cloud clients. In addition, the CS may choose to conceal the information debasements created by server hacks or Byzantine disappointments to look after notoriety. It is accepted that the TPA, who is in the matter of, examining, is solid and free, and in this manner has no motivating force to plot with either the CS or the clients amid the examining procedure. TPA ought to have the capacity to productively review the cloud information stockpiling without neighbourhood duplicate of information and without getting extra on-line load to cloud clients. The Cloud Computing model of figuring is a disseminated application structure that parcels errands then again workloads between the suppliers of an asset or administration, called Cloud servers, and administration requesters, called customers [3].

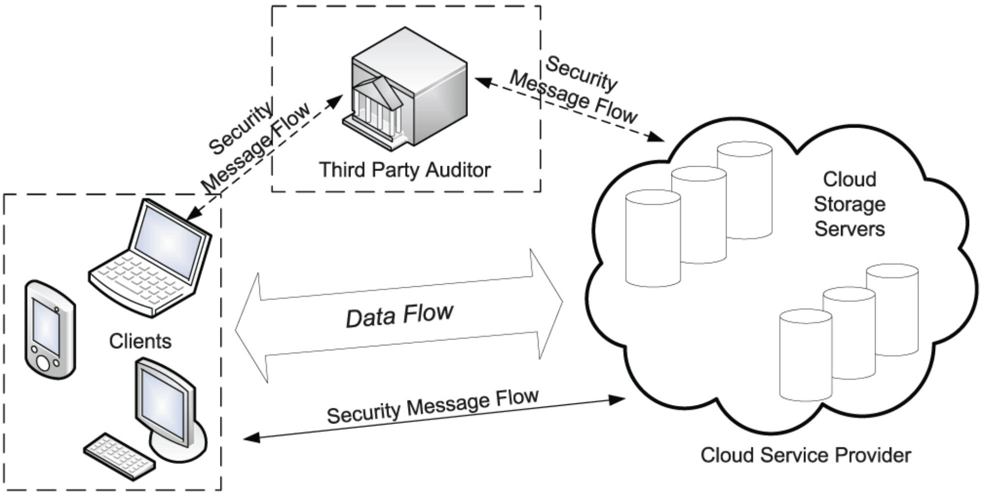

Figure 3: System Model

D. Achieving Secure, Scalable, And Fine-Grained Data Access Control In Cloud Computing

The proposed conspire empowers the information proprietor to delegate errands of information document re-encryption and client mystery key redesign to cloud servers without uncovering information substance or client get to benefit data .Author accomplishes this objective by misusing and interestingly consolidating systems of characteristic based encryption (ABE), intermediary re-encryption, and sluggish re-encryption. The proposed plot additionally has striking properties of client get to benefit privacy and client mystery key responsibility and accomplishes fine graininess, versatility and information privacy for information get to control in distributed computing. Broad investigation demonstrates this proposed plan is exceptionally proficient and provably secures under existing security models [9].

Advantages

Low introductory capital speculation
Shorter start-up time for new administrations
Bring down upkeep and operation costs
Higher use through virtualization
Simpler debacle recuperation

So as to accomplish secure, versatile and fine-grained get to control on outsourced information in the cloud, the creator use and interestingly join the accompanying three progressed cryptographic systems:
Key Policy Attribute-Based Encryption (KP-ABE).
Proxy Re-Encryption (PRE)
Lazy re-encryption
Module Description

Key Policy Attribute-Based Encryption (KP-ABE): KP-ABE is an open key cryptography primitive for one-to many correspondences. In KP-ABE, information are connected with traits for each of which an open key segment is characterized. Client mystery key is characterized to mirror the get to structure so that the client can unscramble a figure content if and just if the information traits fulfill his get to structure. A KP-ABE plan is made out of four calculations which can are recorded as takes after:

Setup Attributes
Encryption
Mystery key era
Decoding

Proxy Re-Encryption (PRE): Intermediary Re-Encryption (PRE) is a cryptographic primitive in which a semi-trusted intermediary can change over a figure content encoded under Alice's open key into another figure message that can be opened by Bob's private key without seeing the basic plaintext.

Lazy re-encryption: The lazy re-encryption strategy permits Cloud Servers to total calculation errands of numerous operations. The operations for example,

Overhaul mystery keys
Overhaul client traits.

E. Toward Publicly Auditable Secure Cloud Data Storage Services

The author's suggest that openly auditable cloud information stockpiling can help this early cloud economy turn out to be completely set up. With open auditability, a put stock in substance with mastery what's more, capacities information proprietors don't have can be assigned as an outer review gathering to evaluate the danger of outsourced information when required. Such an examining administration not just spares information proprietors' calculation assets additionally gives a straightforward yet financially savvy technique for information proprietors to pick up trust in the cloud. The creator portray approaches and framework necessities that ought to be brought into thought, what's more, diagram difficulties that should be settled for such a freely auditable secure distributed storage administration to end up distinctly a reality [10].

F. Online Data Storage Using Implicit Security

The authors portray the utilization of an information dividing plan for actualizing such security including the underlying foundations of a polynomial in limited field. The allotments are put away on haphazardly picked servers on the system and they should be recovered to reproduce the first information. Information recreation requires get to every server, login watchword and the learning of the servers on which the parcels are put away. This plan may likewise be utilized for information security in sensor systems and web voting conventions. The creators have depicted a certain security engineering suited for the utilization of online stockpiling. In this conspire information is parceled in a manner that every segment is verifiably secure and does not should be scrambled. These parcels are put away on various servers on the system which are known just to the client. Remaking of the information requires access to every server and the information as to which servers the information parcels are put away. A few varieties of this plan are depicted, which incorporate the certain capacity of encryption keys as opposed to the information, and where a subset of the segments might be united to reproduce the information [11].

G. Identity-Based Authentication for Cloud Computing

The authors propose a character based encryption (IBE) and decoding and personality based mark (IBS) plans for IBHMCC. In light of the previous IBE and IBS plans, a personality based validation for distributed computing (IBACC) is proposed. The creator displayed a character based validation for distributed computing, in view of the character based progressive display for distributed computing (IBHMCC) and relating encryption and mark plans. They have proposed Identity-based Verification Protocol. Personality based Authentication Convention contains grouping of steps.

In step (1), the customer C sends the server S a ClientHello message. The message contains a new irregular number C n, session identifier ID and C detail.

In step (2), the server S reacts with a ServerHello message which contains another crisp arbitrary number S n, the session identifier ID and the figure detail S determination The ciphertext is transmitted to C as ServerKeyExchange message. At that point S creates a mark Sig S [M] as the IdentityVerify message to forward to C. At last, The ServerHelloDone message implies the progression (2) is over.

In step (3), C firstly checks the mark S Sig S with the assistance of S ID Being endorsement free, the validation convention adjusted well with requests of distributed computing. Execution investigation demonstrated that the validation convention is more proficient and lightweight than SAP, particularly the more lightweight client side [12].

H. Security Framework Of Cloud Data Storage Based On Multi Agent System Architecture

The creators proposes Multi-Agent System (MAS) strategies that can be gainful in distributed computing stage to encourage security of cloud information stockpiling (CDS) among it.MAS design offered eleven security traits created from four principle security approaches of accuracy, respectability, privately what's more, accessibility of clients' information in the cloud.

I. Privacy-Preserving Public Auditing For Secure Cloud Storage

A Public Auditing Scheme Consists of four calculations (KeyGen, SigGen, GenProof, VerifyProof):

KeyGen: key era calculation that is controlled by the client to setup the plan

SigGen: utilized by the client to create check metadata, which may comprise of MAC, marks or other data utilized for evaluating.

GenProof: keep running by the cloud server to create a proof of information capacity rightness

VerifyProof: keep running by the TPA to review the evidence from the cloud server. The creator utilizes homomorphic authenticator method for total the information. Additionally utilizes an arbitrary veil method accomplished by a Pseudo Random Function (PRF)

III. CONCLUSIONS

Despite the fact that the utilization of cloud computing has expanded in market, however it has different security issues like information accuracy, respectability, accessibility and so forth. Proprietor of the information would prefer not to be stolen his information or information misfortune in cloud. In this manner, high security and information accessibility must be kept up with in cloud. The fundamental motivation behind this work is to review the later research done on single cloud and additionally on multi cloud to explain the security issues confronted by the information proprietors. By this study I reason that much research has been done to address the security issue in information stockpiling in cloud yet for multi cloud that a lot of research is not done and still it has some security issues like information honesty and accuracy at the time of information recovery in cloud. Thus, multi cloud information stockpiling security needs more consideration in zone of information stockpiling security in distributed computing.

REFERENCES

[1] Judith Hurwitz, Robin Bloor, Marcia Kaufman, and Fern Halper,”what is Cloud Computing For Dummies”, ”http://www.dummies.com/how-to/content/what-is-cloud-computing.html”, last modified 2013.

[2] Jason, “Defining Cloud Deployment Models”:” http://bizcloudnetwork.com/defining-cloud-deployment-models”, Last modified on AUGUST 4, 2010.

[3] Margaret Rouse, “CLOUD APPLICATION PERFORMANCE MANAGEMENT: DOING THE JOB RIGHT“, last modified December 2010.

[4] Anju Bala, Inderveer Chana, “Fault Tolerance- Challenges, Techniques and Implementation in Cloud Computing”, in the year of January 2012.

[5] R. Yogamangalam and V.S. Shankar Sriram, “A Review on Security Issues in Cloud Computing”, in the year of 2013.

[6] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, Sugata Sanyal, ―A Survey on Security Issues in Cloud Computing‖.

[7] S.Sajithabanu, Dr.E.George Prakash Raj, ―Data Storage Security in Cloud‖, 2011.

[8] Zoran Pantic and Muhammad Ali Babar, ―Guidelines for Building a Private Cloud Infrastructure,‖ in IT University of Copenhagen, Denmark, 2012.

[9] Shucheng Yu., Cong Wan, Kui Ren, Wenjing Lou.,"Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing‖, IEEE Communications Society for publication,2010.

[10] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li,"Toward Pu blicly Auditable Secure Cloud Data Storage Services‖, IEEE Network, 2010.

[11] Abhishek Parakh, Subhash Kak, "Online data storage using implicit security‖, 2009.

[12] Hongwei Li, Yuanshun Dai, Ling Tian, Haomiao Yang,"Identity - Based Authentication for Cloud Computing‖, CloudCom 2009, 2009.

[13] Sushil Bhardwaj, Leena Jain and Sandeep Jain,‖ cloud comp uting: a study of infrastructure as a service (IAAS),‖ M.M.University, Mullana (Ambala, India) 133203, 2010.

[14] Mladen A. Vouk, ―Cloud Computing – Issues,Research and Implementations‖,2008.