Data storage Security in Single to Multi-Clouds Using TPA (Third Party Auditor)

Vilas C. Rathod [#1], Nitin Mishra [*2]
Information Technology Department, RGPV University Bhopal, Madhya Pradesh, India
[1]vilasrathod18@gmail.com
[2]nitin.nriist@gmail.com

Abstract

Cloud Computing has been unreal as a result of the next-generation style of IT Enterprise. Cloud Computing could be a web process with great amount of resource. The user of the cloud will get the service thought network. It moves the applying software package and database bases to the centralized massive data centres, wherever the management of the data and services might not be absolutelytrustworthy.This distinctive paradig m brings concerning several new security challenges, that haven't been well understood. Guaranteeing the security of cloud computing may be a major think about the cloud surroundings, as users typically store sensitive data with cloud storage providers however these suppliers is also untrusted. Handling with "single cloud" suppliers is expected to calm down in style customers as a results of risks of service availableness failure and additionally the danger of malicious insiders inside the only cloud. A movement towards "multi-clouds", or in different words, "interclouds" or "cloud-of-clouds" has emerged recently. As we have a tendency to address 3 security factors that significantly have an effect on single clouds, specifically data integrity, data intrusion, and service availability.

So here we offer a framework to produce a secure cloud information which will guarantee to forestall security risks facing the cloud computing community. This framework can apply multi-clouds and therefore the secret sharing algorithmic program to cut back the chance data intrusion and therefore the loss of service accessibility within the cloud and guarantee data integrity victimization third party auditor (TPA). Third Party Auditor: An entity that has experience and capabilities that user don't have, is trusty to assess and expose risk of cloud storage services on behalf of the user upon request. Above all, we have a tendency to think about the task of permitting a third party auditor (TPA), on behalf of the cloud consumer, to verify the integrity of the dynamic information keep within the cloud.

1. Introduction

Several trends are gap up the age of Cloud computing which is an Internet-based development and use of computer engineering. The ever cheaper and additional powerful processors, at the side of the "software as a service" (SAAS) computing design, are remodelling knowledge centres into pools of computing service on a massive scale.

Concurrently, the increasing network Information measure and reliable but versatile network connections produce it even possible that user will currently subscribe more-quality services from data and program that reside only on remote data centres. Although visualized as a promising service platform for the web, this new data storage paradigm in "Cloud" brings regarding several troublesome vogue issues that have profound influence on the protection and performance of the system. One of the largest issues with cloud data storage is that of data integrity verification at untrusted servers. For example, the storage service provider, that experiences Byzantine failures sometimes, could conceive to hide the data errors from the user for the advantage of their own. What's additional serious is that for saving money and storage space the service provider would possibly neglect to stay or deliberately delete seldom accessed data files that belong to a normal client.

This project focuses on the problems associated with the data security facet of cloud computing. As information and data are going to be shared with a 3rd party, cloud computing users need to

avoid associatedegree untrustedcloud provider. Prote ctive personal and vital data or information, like MasterCard, visa card, credit card details or a patient's medical records from attackers or malicious insiders is of essential importance. In addition, the potential for migration from one cloud to a multi-cloud surroundings is examined and analysis associated with security problems in single and multi-clouds in cloud computing is surveyed.

As solution we offer a framework to produce a secure cloud info which will guarantee to stop security risks facing the cloud computing community. This framework can apply multi-clouds and also the secret sharing algorithmic program to scale back the risk of data intrusion (intervention) and also the loss of service convenience within the cloud and guarantee data integrity. This secret sharing is completed with facilitate of TPA In regard to knowledge intrusion and knowledge integrity, assume we would like to distribute the data into 3 completely different cloud suppliers, and that we apply the secret sharing algorithmic program on the keep data within the cloud supplier. An intruder must retrieve a minimum of three values to be ready to verify the important value that we wish to cover from the intruder.

2. Literature Survey

- In order to reduce the risk in cloud storage, Customers will use cryptologic strategies to guard the keep information within the cloud [6]. Employing a hash function [11] could be a smart answer for data integrity by keeping a brief hash in native memory. During this manner, authentication of the server responses is finished by recalculating the hash of the received information that is compared with the native keep information [6]. If the quantity of data is massive, then a hash tree is that the answer [11]. Several storage system prototypes have enforced hash tree functions, like SiRiUS [20] and TDB [10].
- Mykletun et al. [12] and Papamanthou et al. [13] claim that this can be an energetic space in analysis on cryptographic strategies for keep data authentication.
- Cachin et al. [6] argue that though the previous strategies enable shoppers to confirm the integrity of their information that has been came by servers, they are doing not guarantee that the server can answer a question while not knowing what that question is and whether or not the info is keep properly within the server or not.
- Proofs of Retrievability (PORs) and Proofs of data Possession (PDP) are rules introduced by Juels and Kaliski [9] and Ateniese et al.
- [4] To make sure high likelihood for the retrieval of the user's information. Cachin et al. [6] recommend exploitation multiple cloud suppliers to make sure knowledge integrity in cloud storage and running Byzantine-fault-tolerant protocols on them wherever every cloud maintains one reproduction [7], [8]. Computing resources square measure needed during this approach and not solely storage within the cloud, such a service provided in Amazon EC2, whereas if solely storage service is on the market, Cachin et al.
- [6] Recommend operating with Byzantine Quorum Systems [24] by using Byzantine Disk Paxos [1] and using a minimum of four completely different clouds so as to make sure users' atomicity operations and to avoid the chance of one cloud failure.
- Bessani et al. [5] use Byzantine fault-tolerant replication to store information on many cloud servers, thus if one in every of the cloud suppliers is broken, they're still ready to retrieve information properly. Data encryption is taken into account the answer by Bessani et al. [5] to deal with the matter of the loss of privacy. They argue that to safeguard the keep information from a malicious insider, users should to encrypt information before it's keep within the cloud. Because the information are going to be accessed by distributed applications, the DepSky system stores the cryptographic keys within the cloud by victimization the key sharing algorithm to hide the value of the keys from a malicious insider.
- In the DepSky system, information is replicated in four industrial storage clouds (Amazon S3, Windows Azure, Nirvanix and Rackspace); it's not relayed on one cloud, therefore, this avoids the matter of the dominant cloud inflicting the questionable trafficker lock-in issue [2].

3. Architectural View of Cloud Computing

In cloud computing Architecture consists of five characteristics. The 5 key characteristics of cloud computing is: broad network access, on-demand self-service, rapid elasticity resource pooling, measured Service [21]. The three key cloud delivery models are platform as a service (PAAS), software as a service (SAAS), infrastructure as a service (IAAS), and. A Commercial Services Salesforce.com, Emailcloud.in PAAS, is that the set of tools and services designed to create coding and deploying those applications fast and economical. Platforms are designed upon Infrastructure that is expensive. It provides some standard services like Storage, Database, and quantifiability. An example of PAAS is Google App Engine, Mosso, and AWS: S3. In SAAS Applications are designed for end-users, Service are delivered through a browser. Software Package is managed from a central location. No hardware or software to manage. Users not needed handling software upgrades and patches. An example of SAAS is CRM, Human Resources, Financial Planning, and Word processing. In infrastructure as a Service (IAAS) is also a provision model throughout that a corporation outsources the instrumentality accustomed support operations, at the side of storage, hardware, servers and networking elements. The service supplier owns the equipment and is accountable for housing, running and maintaining it. The client generally pays on a per-use basis. Access to infrastructure as a Full OS access, Servers, Storage, Networks, Firewalls, Routers, Load balancing. An example of IAAS is that the Amazon web service (AWS: EC2) and Flexiscale [18]. Architecture view shown in Figure 1.

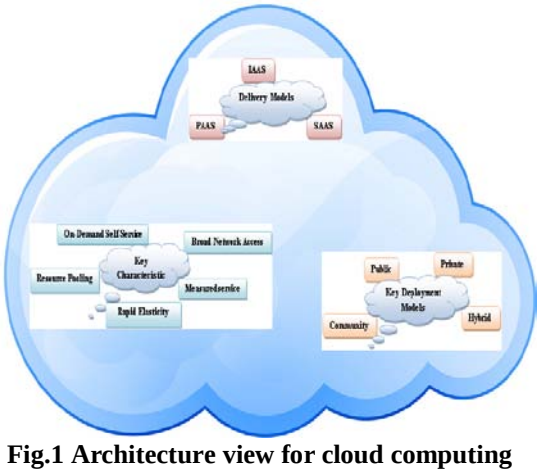

Fig.1 Architecture view for cloud computing

In cloud computing architecture include four key deployment models i.e. public, private, community, and hybrid clouds. In Public clouds the infrastructure and alternative cloud services are created obtainable to the overall public over the net. The cloud is owned and managed by a CSP WHO offers services to customers on a pay-per-use basis. Public cloud users are by default treated as untrustworthy. In private clouds the computing resources are operated completely by one organization. It should be managed by the organization itself. In hybrid clouds; the cloud infrastructure consists of a combination of two or more public, private or community cloud components. Community clouds are the same as private clouds however the cloud infrastructure and computing resources are shared by many organizations that have constant mission, policy and security necessities [17].This model represents the third layer in the cloud environment architecture.

3. Security Risks in Cloud Computing

The security model outlined in [4], we are saying that the checking scheme is secure if 1) there exists no polynomial time algorithmic program which will cheat the friend with non-negligible probability; and 2) there exists a polynomial time extractor which will recover the original information files by ending multiple challenges-responses. Although cloud service suppliers offers benefits to users, security risks play a significant role within the cloud computing surroundings [22]. Users of on-line information sharing or network facilities area unit responsive to the potential loss of privacy [15]. Protective personal and vital information like MasterCard or visa card details or patients' medical records from attackers or malicious insiders is of essential importance [19]. Moving databases to an outsized data centre involves several security challenges [23] like virtualization vulnerability, accessibility vulnerability, privacy and management problems associated with knowledge accessed from a third party, integrity, confidentiality, and information loss or stealing. In numerous cloud service models, the security responsibility between users and suppliers is totally different.

According to Tabakiet al. [21], the approach the responsibility for privacy and security in a very cloud computing atmosphere is shared between customers and cloud service suppliers differs between delivery models. In SAAS, cloud suppliers are more responsible for the protection and privacy of application services than the users. In PAAS, users are accountable for taking care of the applications that they build and run on the platform, whereas cloud suppliers are accountable or protective one user's applications from others. In IAAS, users are accountable for protective operative systems and applications, whereas cloud suppliers should offer protection for the users' data [21].

3.1 Data Integrity

One of the foremost vital problems associated with cloud security risks is data integrity. The info keep within the cloud might suffer from damage throughout transition operations from or to the cloud storage supplier. Cachin et al. [15] provides samples of the risk of attacks from each within and outdoors the cloud supplier, like the recently attacked Red Hat Linux's distribution servers [20]. Cachin et al. [15] argue that once multiple client use cloud storage or once multiple devices are synchronic by one user, it's troublesome to deal with the data corruption issue. Another example of broken data occurred in 2009 in Google Docs that triggered the Electronic Privacy data Centre for the Federal Trade Commission to open Associate in nursing investigation into Google's Cloud Computing Services [15].

3.2 Data Intrusion

According to Garfinkel [16], another security risk which will occur with a cloud provider, just like the Amazon cloud service, can be a hacked secret or data intrusion. If somebody gains access to associate degree Amazon account secret, they're going to be ready to access all of the account's instances and resources. So the taken secret permits the hacker to erase all the data within any virtual machine instance for the taken user account, modify it, or perhaps disable its services.

3.3 Service Availability

Another major concern in cloud services is service availability. Amazon [14] mentions in its contract that it's doable that the service may well be unavailable from time to time. The user's web service might terminate for any reason at any time if any user's files break the cloud storage policy. Additionally, if any damage happens to any Amazon web service and therefore the service fails, during this case there'll be no charge to the Amazon Company for this failure. Corporations seeking to shield services from such failure want measures like backups or use of multiple suppliers [19].

4. Problem Statement

Three completely different network entities may be known as follows: Client: an entity that has large data files to be keep within the cloud and depends on the cloud for data maintenance and computation, may be either individual customers or organizations; Cloud Storage Server (CSS): An entity, that is managed by Cloud Service provider (CSP), has important cupboard space and computation resource to keep up the clients' data, Third Party Auditor: an entity, that has experience and capabilities that shoppers don't have, is sure to assess and expose risk of cloud storage services on behalf of the shoppers upon request.

In the cloud paradigm, by putting the massive information files on the remote servers, the purchasers are often relieved of the burden of storage and computation. As purchasers not possess their information domestically, it's of vital importanc e for the purchasers to make sure that their information are being properly keep and maintained. That is, purchasers should be equipped with bound security suggests that so they will sporadically verify the correctness of the remote information even while not the existence of native copies. Just in case that shopper doesn't essentially have the time, feasibility or resources to watch their information, they will delegate the watching task to a sure TPA. During this paper, we have a tendency to solely contemplate verification schemes with public auditability: any TPA in possession of the general public key will act as a supporter. We have a tendency to assume that TPA is unbiased whereas the server is untrusted. For application functions, the purchasers could move with the cloud servers via CSP to access or retrieve their prestored information. A lot of significantly, in sensible eventualities, the shopper could oftentimes perform block-level operations on the info files. The foremost general styles of these operations we have a tendency to contemplate during this paper are modification insertion, and deletion.

5. The Proposed Scheme

This paper focuses on the problems associated with the information security side of cloud computing. As information and data are going to be shared with a third party, cloud computing users wish to avoid un-trusted cloud supplier. Protective personal and vital information, like Master Card, credit card or visa cards details or a patient's medical records from attackers or malicious insiders is of essential importance. Additionally, the potential for migration from one cloud to a multi- cloud environment is examined and analysis associated with security problems in single and multi-clouds in cloud computing is surveyed.

This framework can apply multi-clouds and therefore the secret sharing algorithm to reduce the risk of data intrusion and therefore the loss of service convenience within the cloud and guarantee data integrity. This secret sharing is finished with facilitate of TPA. Third Party Auditor: an entity, that has experience and capabilities that purchasers don't have, is trustworthy to assess and expose risk of cloud storage services on behalf of the purchasers upon

request. Especially, we tend to contemplate the task of permitting a third party auditor (TPA), on behalf of the cloud consumer, to verify the integrity of the dynamic data keep within the cloud. System Architecture shown in Figure 2.

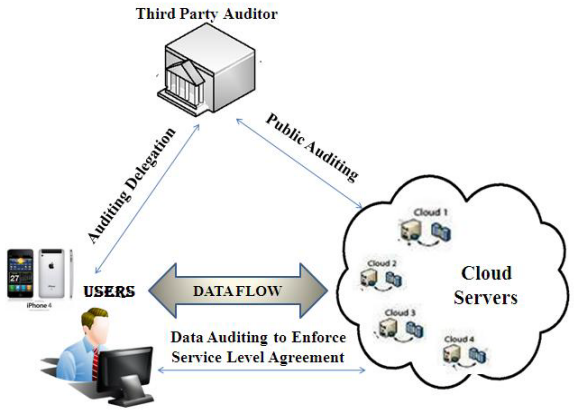

Fig.2 System Architecture

6. Objective

Our design objective will be summarized because the following:

1. Public auditability for storage correctness assurance: to permit anyone, not simply the client who originally hold on the file on cloud servers, to possess the potential to verify the correctness of the hold on information on demand.
2. Dynamic data operation support: to permit the clients to perform block-level operations on the info files whereas maintaining constant level of information correctness assurance. The design should be as economical as potential so on confirm the seamless integration of public auditability and dynamic data operation support.
3. Blockless Verification: No challenged file blocks should be retrieved by the verifier (e.g., TPA) throughout verification technique for efficiency concern.

7. Scope

The problem of the malicious insider within the cloud infrastructure that is that the base of cloud computing is taken into account by Rocha and Correia. IAAS cloud suppliers give the users with a collection of virtual machines from that the user will profit by running code on them. The standard resolution to make sure information confidentiality by data encryption isn't spare as a result of the very fact that the user's information has to be manipulated within the virtual machines of cloud suppliers that cannot happen if the info has been encrypted. Directors manage the infrastructure and as they need remote access to servers, if the administrator could be a malicious business executive, then he will gain access to the user's information. Van Dijk and Juels present some negative aspects of information encoding in cloud computing. Additionally, they assume that if the info is processed from completely different purchasers, encryption cannot guarantee privacy with in the cloud.

8. Methodology

To effectively support public auditability while not having to retrieve the info blocks themselves; we have a tendency to resort to the similarity authenticator technique. similarity authenticators are inexcusable data generated from individual data blocks, which might be firmly aggregative in such the simplest way to assure a supporter that a linear combination of data blocks is properly computed by confirmatory only the aggregative authenticator.

In relevancy data intrusion and data integrity, assume we wish to distribute the info into three totally different cloud suppliers, and that we apply the secret sharing algorithm on the keep information within the cloud supplier. An intruder needs to retrieve a minimum of three values to be ready to determine the real value that we wish to cover from the intruder. This relies on Shamir's secret sharing algorithm with a polynomial operate technique that claims that even with full information of (k – 1) clouds, the service supplier won't have any information of vs. (vs. is that the secret value). We've used this system in previous databases-as-a serves analysis [3]. In different words, hackers got to retrieve all the data from the cloud suppliers to understand the real value of the info within the cloud. Therefore, if the attacker hacked one cloud provider's secret or maybe two cloud provider's passwords, they still got to hack the third cloud provider (in the case wherever k = 3) to understand the key that is that the worst case state of affairs. Hence, replicating data into multi-clouds by employing a multi-share technique [3] might reduce the chance data intrusion and increase data integrity. In different words, it'll decrease the chance of the Hyper-Visor being hacked and Byzantine fault-tolerant data being taken from the cloud supplier. Relating to service accessibility risk or loss of information, if we have a tendency to replicate the info into totally different cloud suppliers, we have a tendency to might argue that the info loss risk are going to be reduced. If one cloud supplier fails, we will still

access our data live in different cloud suppliers. This truth has been discovered from this survey and that we can explore managing totally different cloud supplier interfaces and therefore the network traffic between cloud suppliers.

9. Conclusion

To ensure cloud data storage security, it's vital to modify a TPA to judge the service quality from associate objective and independent perspective. Public auditability also permits clients to delegate the integrity verification tasks to TPA whereas they themselves may be unreliable or not be ready to commit necessary computation resources acting continuous verifications. Additionally, the loss of service availableness has caused several issues for a large number of customers recently. Furthermore, data intrusion results in several issues for the users of cloud computing. The aim of this work is to survey the recent research on single clouds and multi-clouds to handle the security risks and solutions. We have a tendency to support the migration to multi-clouds as a result of its ability to decrease security risks that have an effect on the cloud computing user.

10. REFERENCES

[1] I. Abraham, G. Chockler, I. Keidar and D. Malkhi, "Byzantine disk paxos: optimal resilience with Byzantine shared memory", Distributed Computing, 18(5), 2006, pp. 387-408.

[2] H. Abu-Libdeh, L. Prince house and H. Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium on Cloud computing, 2010, pp. 229-240.

[3] M.A. AlZain and E. Pardede, "Using Multi Shares for Ensuring Privacy in Database-as-a-Service", 44th Hawaii Intl. Conf. on System Sciences (HICSS), 2011, pp. 1-9.

[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted stores", Proc. 14th ACM Conf. on Computer and communications security,2007, pp. 598-609.

[5] A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11:Proc. 6thConf. On Computer systems, 2011, pp. 31-46.

[6] C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.

[7] M. Castro and B. Liskov, "Practical Byzantine fault tolerance", Operating Systems Review, 33, 1998,pp. 173-186

[8] J. Hendricks, G.R. Ganger and M.K. Reiter, "Low overhead byzantine fault-tolerant storage", SOSP'07: Proc. 21st ACM SIGOPS symposium on Operating systems principles, 2007, pp. 73-86.

[9] A. Juels and B.S. Kaliski Jr, "PORs: Proofs of Retrievability for large files", CCS '07: Proc. 14thACM Conf. on Computer and communications

[10] U. Maheshwari, R. Vingralek and W. Shapiro, "How to build trusted database system on untrusted storage", OSDI'00: Proc. 4thConf. On Symposium on Operating System Design & Implementation, 2000, p. 10. Security, 2007, pp. 584-597.

[11] R.C. Merkle, "Protocols for public key cryptosystems", IEEE Symposium on Security and Privacy, 1980, pp. 122-134.

[12] E. Mykletun, M. Narasimha and G. Tsudik, "Authentication and integrity in outsourced databases", ACM Transactions on Storage (TOS), 2, 2006, pp. 107-138.

[13] C. Papamanthou, R. Tamassia and N. Triandopoulos, "Authenticated hash tables", CCS'08: Proc. 15th ACM Conf. on Computer and communications security, 2008, pp. 437-448.

[14] Amazon, Amazon Web Services. Web services licensing agreement, October3, 2006.

[15] C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.

[16] S.L. Garfinkel, "An evaluation of amazon's grid computing services: EC2, S3, and SQS", Technical Report TR-08-07, Computer Science Group, Harvard University, Citeseer, 2007, pp. 1-15.

[17] P. Mell and T. Grance, "The NIST Definition of Cloud Computing" Recommendation of NIST, Special Publication 800-145, 2011.http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[18] S. Kamara and K. Lauter, "Cryptographic cloud storage", FC'10: Proc. 14thIntl.Conf. on Financial cryptography and data security,2010, pp. 136-149.

[19] H.Mei, J. Dawei, L. Guoliang and Z. Yuan, "Supporting Database Applications as a Service", ICDE'09:Proc. 25thIntl.Conf. On Data Engineering, 2009, pp. 832-843.

[20] RedHat, https://rhn.redhat.com/errata/RHSA-2008-0855.html.

[21] H. Takabi, J.B.D. Joshi and G.-J.Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security & Privacy, 8(6), 2010, pp. 24-31.

[22] J. Viega, "Cloud computing and the common man", Computer, 42, 2009, pp. 106-108.

[23] C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuring data storage security in cloud computing", ARTCOM'10: Proc. Intl. Conf. on Advances in Recent Technologies in Communication and Computing, 2010, pp. 1-9.

[24] D. Malkhi and M. Reiter, "Byzantine quorum systems", Distributed Computing, 11(4), 1998, pp. 203-213.

[25] (NIST), http://www.nist.gov/itl/cloud/.

[26]Mohammed A. AlZain, Eric Parded, Ben Soh, James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds", 2012, IEEE CONFERENCE ON SYSTEM SCIENCES