Survey on reliable auditing services for multistorage clouds

P.Jeyaram[1], P.Ashly angel[2]

[1]*PG Scholar, Department of Computer Science and Engineering, Christian College of Engineering and Technology, Dindigul, Tamilnadu – 624619, India.*
jeyaram823@gmail.com

[2] *Assistant Professor, Department of Computer Science and Engineering, Christian College of Engineering and Technology, Dindigul, Tamilnadu - 624619, India.*
puppy.ashlyangel@yahoo.com

Abstract— **Cloud computing provides various resources for the client to perform the activities through internet. Outsourced storage is used to client store large amount data because client difficult to store entire data in personal system. Reliable auditing services for multi-storage clouds used to test out the quality of stored data. It is efficient method for check data integrity. Our audit system is used for make sure authenticate integrity of the untrusted and outsourced storage. Audit services based on techniques on index hash table, random sampling, cryptography, and fragment it is used in the dynamic operation. Our system used to check integrity of data without downloading the entire date. This paper describe dynamic link list method for updating index hash table and dynamic operation in multi-storage cloud this is used for retrieve data or archives quickly from cloud and reduce communication cost.**

Keywords—**Provable data possession, Audit service, Multistorage cloud, Storage security.**

I. INTRODUCTION

Cloud computing means storing, accessing data and programs over the Internet instead of computer's hard drive and it also provides scalable environment for storing large amount of data and works on various application. Cloud computing provide on-demand self-services and enables end user to provide computing power, network, software, storage, etc in a simple and flexible way based on the user request. Cloud computing invented by joseph carl robnett licklinder in the year for 1960s.he worked on APRANET and it useful for connect people and data sharing among anywhere, anyplace and any time. CC hosting services over the network. Cloud computing services are dividing into major three types such as Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS). Cloud outsourcing storage is new technology provide low-cost, location independent and scalable platform for storing large amount of client's data. Cloud Storage Services(CSS) useful for storing large amount of data in cloud and heavy load that is difficult to carry storage management and maintenance. Some of operations affect (attacks or failures) the client's data or archives. Software as a service is a model provides software and application based on demand user request. On-demand licensing contained in the SaaS and 30% of new software will be deliver via SaaS.

Platform as a Service is a SaaS application, software delivered in the PaaS model. PaaS model also known as cloudware and PaaS workflow for application design, application development, testing, deployment, hosting and offer many services. PaaS model all software or application entirely throw in internet without software downloads or installation.Infrastructure as a service is a model of computer infrastructure (virtualization environment) as a services. Purchasing servers, software, data center space, network equipment customer buy resource fully outsourced service.IT as a service said to be proposed model of IT infrastructure.

Seven security issues cloud computing model. They are as follows: first, Privileged user access - information transmit from the customer through the Internet poses a certain amount of hazard, because of issues of data ownership and inquire about who has specialized access to data. Second, Regulatory compliance - clients are responsible for the security of their clarification, as they can select connecting providers that allow to be auditing by third party auditing/security certification of organizations that ensure levels of security and providers t they don't know . Third, Data location – depending on contract, some customer might never know what country or what jurisdiction their data is located and provider control over the location of data. Fourth, Data Segregation – make sure encryption available at all the stages and encrypted information from various companies may be stored on the same hard disk, so a method to separate data should be deploy by the provider. Fifth, Recovery - each provider must enclose a disaster recovery protocol to save from harm user data and they offer complete restoration. Sixth, Investigative Support - if a client suppose faulty action beginning the provider, it might not cover many legal conduct pursue an investigation and vendor have the capacity investigation. Last, Long-term Viability - refers to the facility to withdraw a contract and all data if the present provider is bought out by another firm and company goes out of business how data will be return and what format.

The following reasons damage client's data: first, internal and external threads damage data. Second, Clients improper operation such as user can't control over dynamic operation in cloud. Therefore cloud service provider necessary to check integrity, availability of client's stored data. Reliable security auditing service important for analysis and trace the any activities client's operation such as data access, application and security activities. Further compare with common audit and reliable audit give more efficient method for check the integrity of the client's data. Our audit service is useful for data validation and user check the data integrity without downloading entire data. Technology and design in the security architecture design have authentication, authorization, availability, confidentiality, integrity, accountability, privacy. Cloud storage. Cloud service provider give space of clients store and retrieve data rather than local system and internet link used to access the data in the cloud. Currently number of different cloud storage system available in the world and each cloud provider give different storage method. First, niche-oriented store just email or digital pictures and the providers can copy the data onto DVDs and send to the client. Second, some providers give storage space of store any type of data in the cloud. Third, some providers are small and other providers are huge and fill an entire warehouse.

Providers- There are hundreds of cloud storage space providers on the network and further look to be added each day. Some examples of specialized cloud providers: Google Docs allow users to upload spreadsheets, documents and presentations to Google's data server. Customer files can then be edited using a Google application. Web email providers like Hotmail, Gmail and Yahoo Mail store email communication on their individual servers. Users can contact their email from computer and other devices coupled to the Internet. Picasa and Flickr host the digital photographs in the internet millions of amount. Users can create their own online photo albums. YouTube hosts the video files in the web and upload and download the video files. Hostmonster and GoDaddy store files and data for many client web sites. Facebook and MySpace are social networking sites and permit member to post image and other content. That content is stored on the company's servers. MediaMax and Strongspace provide storage space for any type of digital data. Numerous of these services are provided for free, but others charge you per stored gigabyte and by how much information is transferred to and from the cloud. As more and more providers offer their services, prices have tended to drop, and some companies offer a certain amount for free. Cloud audit-It is a control frameworks and specification for the manage information in cloud computing. Cloud service provider performs audit service for potential client to get data security and good performance. Standardized information makes comparison among providers easier, reducing the resources necessary to collect documentation and analyze the data. CloudAudit is planned to benefit cloud computing providers and clients. For example, the cost of respond to a possible customer's compliance controls may be very small for a large retailer. However, a small vendor may find it burdensome to provide that information to multiple prospective customers. Cloud Security Alliance is the cloud audit tools.

II. RELATED WORK

G. Ateniese and R.C. Burns at etl propose the Provable data possession(PDP)[2],first proposed by ateniese et al., method allows a verify to perform public auditing on the integrity of stored data in the unstrusted server and client check the integrity of stored data without retrieve data in the PDP method and this mechanism for only static data. Conventional cryptography technology for data integrity and availability based on hash function and signature schemes [hybrid grid] cannot effort on the outsourced data and not practical solution for large size files. In addition ,auditing services expensive for cloud customer. proof of retrievability(POR)[2] method used to public auditing and probabilistic proof technique used in the POR and this method for storage provider to prove the customers stored data.PDP/POR techniques work on a publicly verifiable method and anyone use this verification protocol and prove the availability of the clients stored data. Using remote-interface method clients prove the availability of stored data in the untrusted cloud storage.

C.C. Erway and A. Ku tells about the Dynamic provable data possession (DPDP) [3], is a framework and efficient construction for DPDP and this method extends the provable data possession and support dynamic operation in the cloud storage data. In addition, this technique used for the probability misbehavior detection used to find defects in the outsourced storage. The clients stored file F divide into n blocks and client define update operation for any insertion of new block, deletion of any data block, modification of any old block easy in the DPDP. Contributions work are, introduce framework for DPDP, Provide efficient fully dynamic PDP solution, logarithmic computation, Communication and same detection of PDP scheme, rank-based authentication dictionary using an RSA tree.

G. Ateniese and R.D. Pietro at etl propose the Scalable provable data possession (SPDP) [4] method construct for high efficiency and provable data possession based on symmetric key cryptography, outsourcing of dynamic data operation such as efficient of modify, delete, insert in the SPDP technique. SPDP provide security and reliability in the storage server. C. Wang and Q. Wang Privacy-preserving public auditing & data integrity for secure cloud storage [5], Enabling public auditable for cloud storage. Check the correctness of the stored data in the cloud. No new vulnerabilities towards user data privacy on-line burned. In this method audit service perform multiple users simultaneously. Privacy-preserving auditing protocol enable external auditor to check integrity without knows the data content. Batch auditing method used in protocol which is perform simultaneously audited by third party auditor. High Efficient and provable secure method is proposed in privacy-preserving.

Richard Chow and Philippe Golle at etl propose the Controlling data in the cloud: outsourcing computation without outsourcing control [6]. Major issue in the cloud, the cloud provider some control over the cloud client's data. Controlling data in the cloud provide tools supporting control o data and enable users to enhance business intelligence. Information-centric security extends control to data in the cloud. If data is enter into the cloud protection of data in enhanced and retrieve same protected data from the cloud. Self –protection technique is used for storing and retrieving data. High-Assurance Remote server Attestation, Privacy-Enhanced Business Intelligence techniques used in the controlling data in the cloud.

Cong Wang and Kui Ren propose the Toward public auditable secure cloud data storage services [7]. Computing as a utility, data owners can remotely store their data in the cloud to enjoy on demand first-class applications and services from a shared collection of configurable compute resources. Auditing service not only helps save data owners' computation resources but also provides a transparent yet cost-effective method for data owners to gain trust in the cloud**.** Desirable properties for public auditing services are minimizing auditing overhead, protect data, support data dynamic, batch auditing, data privacy.

Boyang Wang and Baochun Li2 at etl propose the Konx: privacy-preserving audit for shared data with large groups in the cloud [8], Cloud computing and storage services offer the data not only stored in the cloud storage but also shared between a huge number of users in a crowd. Knox, a privacy- preserving auditing mechanism for data stored in the cloud and shared among a large number of users in a group. knox means amount of data for verification at the same time auditing operation is performed. In addition, knox provide Homomorphic Macs to minimize storage space in verification process and efficiently audit the correctness of data that shared among a large group. Design goals are correctness, efficiency, identify privacy, and support large number of groups, traceability. Thread models are integrity, privacy threads affect the correctness of the data. Two threads in the integrity of the shared data that are improper sharing, hardware failure, human errors make corruption of data.

TABLE I
COMPARISON BETWEEN THE KNOX AND PREVIOUS WORK

	Previous work	Knox
Identify privacy	Yes	Yes
Public auditing	Yes	No
Traceability	No	Yes
Support large group	No	Yes

Jason Baker and Chris Bond at etl propose the Megastore- Providing Scalable and Highly Available Storage for Interactive Services [9], Megastore is a storage system developed for the needs of today's interactive online web services. Megastore blends the scalable of the NoSQL datastore provide long-established RDBMS, and provides both strong reliability guarantees and high availability. Replication methods provide high availability and fast read, writes, replica types provided in the megastore. Some drawbacks are full replication become unreliable, less connectivity, performance degraded, and storage space.

Nicoleta - Magdalena Iacob propose the Fragmentation and Data Allocation in the Distributed Environments [10], Fragmentation and data allocation in data base is an efficient way to improve reliability, availability and performance of a database system. Fragmentation design and replication methods: vertical fragmentation, horizontal fragmentation, mixed fragmentation. Effective way to improve reliability, availability and performance of a database system, minimize the cost and response time, allocation design, replication, cost analysis methods are cost analysis of fragmentation, replication, partition. Some draw backs are concurrency operation slow, extra storage space.

Naveen Palavalli and Shishir Bharathi at etl propose the concept Performance and Scalability of a Replica Location Service [11], Replica Location Service provides the Globus Toolkit Version 3.0 and Replica Location Service (RLS) provide the replicated information. RLS version includes support for a hierarchy of RLI servers that update one another as well as performance and reliability improvements. Technologies are Globus toolkit version 3.0, Replica location service, Soft state update protocols, RLS index scales. Advantages are bulk operations, performance and reliability improvement.

III. PROBLEM STATEMENT

Provable data possession at untrusted stores [2], verify the authenticity of data has critical problem for storing data on untrusted servers so issue arise in p-p storage system, network file system, web-service stores, database system. Significant I/O computation, large amount data is not available in the system. Scalable and efficient provable data possession [4] symmetric key cryptography method used for provide security and reliability in the storage server. Fragment structure not used so data availability is less. Local computations overhead for the client perform each verification and limited number of verification available in the SPSD. Dynamic provable data possession [3], client preprocess the data and sends it to an untrusted server. Small amount of meta-data stored in the server. Controlling Data in the Cloud and Outsourcing Computation without Outsourcing Control [5], Trusted computing in cloud. Encryption of the stored and retrieved data. Business intelligence stand point in the common life style. Security concern are vm-level attacks[monitor and firewalls],cloud provider vulnerabilities[rational appscan tool], - Phishing cloud provider, expanded network attack surface, Authentication and Authorization. single point of failure, assurance of computation integrity. Toward Publicly Auditable Secure Cloud Data Storage Services[6], Not enough for a public auditable secure cloud data storage system, accountability, multi-writer model, performance ,data security, recovery, privacy for clients data. Privacy-Preserving audit for Shared Data with Large

Groups in the Cloud [7] and knox- Cloud computing and storage services provide data is not only stored in the cloud and also shared among a huge number of client's in a group. Knox, a privacy- preserving audit mechanism for data stored in the cloud and shared among a large number of users in a group. Public auditing difficult in the knox. Megastore: Providing Scalable and Highly Available Storage for Interactive Services[8], mega storage full replication become unreliable, less connectivity, performance degraded are problem in the mega storage. Fragmentation and Data Allocation in the Distributed Environments [10], concurrency operation slow, extra storage space, concurrency operation slow, extra storage space.

IV.PROPOSED SYSTEM

Dynamic link list used to improve efficiency of index hash table while updating data in the storage sever. Reliable auditing services for multistorage cloud methodology for checking data integrity in the multistorage cloud. Auditing services based on the techniques of fragment structure, index-hash table, random sampling, dynamic operation and timely anomaly detection in the cloud. Following performance and security objectives are used to improve efficient for auditing services in the multistorage clouds: Third party auditor (TPA): To allow client or TPA to check the correctness of cloud data without retrieving entire data. Dynamic operations: To make sure no attack to compromise the security while dynamic operation such as update, delete, insert on the multi-storage cloud. Timely detection: To find errors or losses in timely detect the data operation in the outsourced storage. Efficient forensic: Third party auditor to apply strict audit and administration for outsourced client's data and offer efficient confirmation for anomalies. Lightweight: To permit audit tasks every data with minimum storage and less communication and computation cost.

Reliable audit service for reliability verification of outsourced storages and our audit system is useful for public auditing. User checks integrity without downloading raw data and keep privacy of the data. Reliable audit system provide dynamic data operation based on techniques, such that fragment structure, index hash table and random sampling. Our audit system for improve the efficiency of updating index hash table. Audit service contain three processes-first, Tag generation data owner use the secret key for each storing data and each file collection blocks in the index hash table. Second, periodic sampling audit third party auditing perform this auditing technique. Audit for dynamic operation data owner perform insert, delete, modification and update the data server and each operation store in the index hash table. Authentication application is user interface protocol for clients access the dynamic operation. Our protocol construction based on keygen, taggen, update, delete, insert algorithms used in the authentication application.

Fragment and secure tags providemaximize data availability and Performance in the audit system fragment technique used in the outsourced storage. Fragment techniques apply for file F and file is spilt into n blocks. Secure tags apply for each n blocks and secure signature tag added in the n blocks. Periodic sampling audit: Third party auditors periodically perform the sampling audit used to reduce the workload in the audit services and it is effective method finding misbehaviors. Index hash table: INT store all records of clients dynamic operation such as insert, delete, modify, update task stored in the INT. In addition dynamic link list method for increase efficiency in the index hash table. Stack and queues are easy to implement link list method and no need to set limits the size of stack. Link list method used to push, pop, enqueue and dequeue. The hash table is a fine modest data structure and it useful for storing and retrieves the data in quick time. Dynamic link list used for storing data any place in link list.

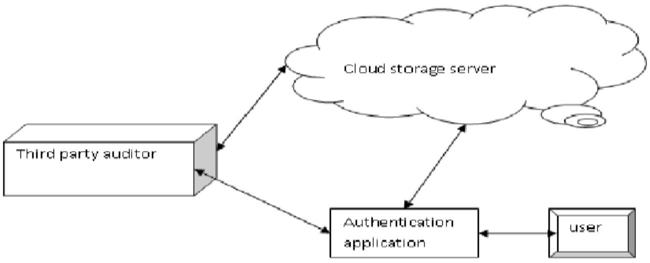

Fig.1 Audit System Architecture

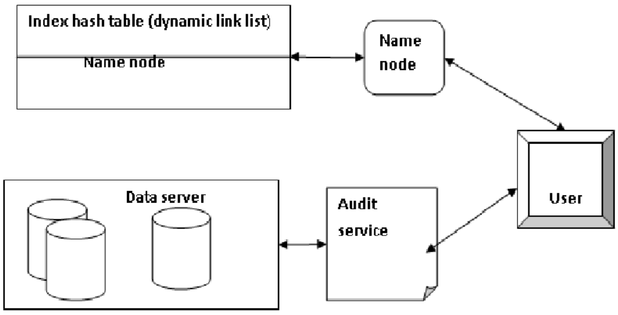

Fig. 1 Index Hash Table Records

V. CONCLUSION

Construction based on reliable auditing services in the multistorage cloud. Dynamic link list used to improve efficiency of index hash table while updating data in the storage servers. Cloud computing clients check the integrity of data without downloading entire data. These methods reduce the computation, communication cost.

REFERENCES

[1] "Dynamic Audit Services for Outsourced Storages in Clouds" Yan Zhu, Member, IEEE, Gail-Joon Ahn, Senior Member,

IEEE, Hongxin Hu, Member, IEEE, Stephen S. Yau, Fellow, IEEE, Ho G. An, and Chang-Jun Hu.

[2] G. Ateniese, R.C. Burns, R. Curtmola, J. Herring, L. Kissner, Z.N.J. Peterson, and D.X. Song, “Provable Data Possession at Untrusted Stores,” Proc. 14th ACM Conf. Computer and Comm. Security, pp. 598-609, 2007.

[3] C.C. Erway, A. Ku¨ pc¸u¨ , C. Papamanthou, and R. Tamassia,“Dynamic Provable Data Possession,” Proc. 16th ACM Conf.Computer and Comm. Security, pp. 213-222, 2009.

[4] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, “Scalable and Efficient Provable Data Possession,” Proc. Fourth Int’l Conf. Security and Privacy in Comm. Netowrks (SecureComm), pp. 1-10,2008.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Storage Security in Cloud Computing,” Proc. IEEE INFOCOM ’10, Mar. 2010.

[6] “Toward Publicly Auditable Secure Cloud Data Storage Services” Cong Wang and Kui Ren, Illinois Institute of Technology Wenjing Lou, Worcester Polytechnic Institute Jin Li, Illinois Institute of Technology.

[7] “Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control” Richard Chow, Philippe Golle, Markus Jakobsson, Ryusuke Masuoka, Jesus Molina Elaine Shi, Jessica Staddon.

[8] “Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud”Boyang Wang, Baochun Li2 and Hui Li1

[9] “Megastore: Providing Scalable, Highly Available Storage for Interactive Services” Jason Baker, Chris Bond, James C. Corbett, JJ Furman, Andrey Khorlin, James Larson, Jean Michel L´eon, Yawei Li, Alexander Lloyd, Vadim Yushprakh Google, Inc.

[10] “Fragmentation and Data Allocation in the Distributed Environments” Nicoleta - Magdalena Iacob (Ciobanu).

[11] “Performance and Scalability of a Replica Location Service” Ann L. Chervenak, Naveen Palavalli, Shishir Bharathi, Carl Kesselman, Robert Schwartzkopf University of outhern California Information Sciences Institute.