International Journal of Computer (IJC)

ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

Data Auditing and Security in Cloud Computing: Issues, Challenges and Future Directions

Geeta C M[a]*, Raghavendra S[b], Rajkumar Buyya[c], Venugopal K R[d], S S Iyengar[e], L M Patnaik[f]

[a,b,d]*Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University*

[c]*Cloud Computing and Distributed Systems (CLOUDS) Lab, School of Computing and Information Systems, The University of Melbourne, Australia*

[e]*Department of Computer Science and Engineering, Florida International University, USA*

[f]*INSA, National Institute of Advanced Studies, Indian Institute of Science Campus, Bangalore, India*

[a]*Email: geetacmara@gmail.com*

[b]*Email: raghush86@gmail.com*

[c]*Email: raj@csse.unimelb.edu.au*

[d]*Email: venugopalkr@gmail.com*

[e]*Email: iyengar@csc.lsu.edu*

[f]*Email: patnaiklm@iisc.ac.in*

Abstract

Cloud computing is one of the significant development that utilizes progressive computational power and upgrades data distribution and data storing facilities. With cloud information services, it is essential for information to be saved in the cloud and also distributed across numerous customers. Cloud information repository is involved with issues of information integrity, data security and information access by unapproved users. Hence, an autonomous reviewing and auditing facility is necessary to guarantee that the information is effectively accommodated and used in the cloud. In this paper, a comprehensive survey on the state-of-art techniques in data auditing and security are discussed. Challenging problems in information repository auditing and security are presented. Finally, directions for future research in data auditing and security have been discussed.

Keywords: Cloud Computing; User Revocation; Deduplication; Public Auditing; Consistency; Re-generating Codes; Key-Exposure Resilience.

---

* Corresponding author.

1. Introduction

The most recent utility oriented distributed computing model that has envisioned an immense transformation of Information Technology (IT), to increase capacities of the client access to a common pool of platforms, applications and infrastructures without having to really claim them in distributed computing. In the context of deployment, the cloud computing is grouped into four approaches: (i) public, (ii) private, (iii) hybrid and (iv) community clouds that are described below:

- *Public Cloud*: In public cloud, the service suppliers transfer various applications as service and encourage the customers by offering access to the resources by means of concentrated distributed servers over the Internet for example, Amazon Web Services, Google App Engine.
- *Private Cloud*: The services and framework are utilized and supervised absolutely by a performance institution.
- *Community Cloud*: The services and framework are distributed by an arrangement of institutions that are overseen either privately or by a dependable outsider.
- *Hybrid Cloud:* Hybrid cloud adopts a blend of on-premises, private cloud and third-party public cloud services with arrangement among the two platforms.

Liu and his colleagues [1] discusses about the cloud computing reference architecture and taxonomy of three service models i.e., Platform as a Service (PaaS), Software as a Service (SaaS), Infrastructure as a Service (IaaS). Fox and his colleagues [2] examine the impediments to and opportunities for selection and development of distributed computing and classes of utility computing. Buyya and his colleagues [3] proposed framework for market-oriented distribution of assets inside the clouds. It provides the attributes of cluster, grid and clouds and awareness on market-based assets administration procedures. Cloud service provider offers three types of service models, for example, Software as a Service (SaaS), Infrastructure as Service (IaaS) and Platform as Service (PaaS). Clients of SaaS layer are granted to adopt all sorts of programming from their relating cell phones. For example, Microsoft Live Mesh grants document and folder distribution between numerous reckoning gadgets. The PaaS framework gives designers with a runtime circumstance as indicated by their specific necessities.

The PaaS gives programming system, libraries and toolboxes for the designers to authorize them to create, convey and look after applications. Some prominent PaaS systems such as like Amazon Elastic MapReduce (EMR), Google App Engine are accessible in the business sector. The IaaS delivers reckoning, reposition and systems administration in a kind of versatile Virtual Machine (VM) to the trading customers for example, S3 (Simple Storage Service) and EC2 (Elastic Cloud Computing). Distributed computing provides cloud repository as one of the service in which information is maintained, managed, backed up remotely and made accessible to customers over a network (typically the Internet). The customer is worried about the integrity of information saved in the cloud as the customers information can be attacked or altered by external attacker. Therefore, a new concept called data auditing is introduced in Cloud Computing to deal with secure information storage. Auditing is a process of verification of customer information which can be carried out either by the customer himself (information proprietor) or by a TPA (Third Party Auditor). It helps to maintain the sincerity of data saved on

the cloud.

The two categories of verifier's role are: first one is private auditing, in which only customer or information proprietor is allowed to verify the honesty of the hoarded information. No other person has the authority to question the server regarding the data. But it tends to increase verification overhead of the user. Second is public auditability, which allows anyone, not just the customer, to challenge the server and performs information verification with the help of TPA. The TPA is an entity which is used so that it can act on behalf of the client. It has all the necessary proficiencies, intelligence and professional expertise that are needed to handle the work of integrity certification and it also decreases the overhead of the customer. It is necessary that TPA should efficiently verify the distributed information storage without requesting for the local copy of information. It should have zero knowledge about the information saved in the distributed server.

1.1 Data Storage Auditing Model

Blum and his colleagues [4] explored the auditing issue that empowers information proprietors to verify the honesty of remote information. Numerous conventions have been suggested: e.g., Remote Integrity Checking (RIC), Proof of Retrievability (POR) and Provable Data Possession (PDP) conventions. Systems comprising of information proprietor and distributed server is known as private verification framework. Role of two entities in private verifying framework is explained below: (a) Information proprietor: is the proprietor of information, consist of both individuals and administration. Information proprietor is relying on cloud service provider for proper sustentation of information. (b) Cloud Storage Server (CSS): maintains information repository space to information proprietor. Distributed service provider is authoritative for managing the distributed repository servers. This entity is considered to be semi-trusted. System framework for private auditing is shown in Fig. 1. The model consists of two entities- Information proprietor and Cloud service provider. This framework provides permission only to Information proprietor to interact with the distributed repository server to verify information sincerity and accomplish data structure operations on deployed information.

Figure 1: System Framework for private auditing.

The convention that acknowledges a third party other then information proprietor to verify information sincerity is termed as public verifying system. This framework consists of Information proprietor, CSS and a Third party auditor. Role of Third party auditor in public verifying framework is elucidated below: a. Third Party Auditor (TPA): is an accomplished individual possessing resources, and skills to access services administered by distributed repository server. Information proprietor may solicit TPA to verify the accomplishment of distributed repository server. The system framework for public auditing is shown in Fig. 2. It consists of two forms of communications. First communication is between information proprietor and TPA as shown in Fig. 2a.

The information proprietors create cryptographic keys, estimates metadata of their information to be hoarded on distributed server. Then information proprietor interchanges the cryptographic keys with the TPA and saves information on cloud and goes off line. Second communication is amidst TPA and CSS as shown in Fig. 2b. The sincerity verification is done via a challenge-response verifying convention. This feedback verifying convention has three phases: Challenge, Authentication, and Verification. At any time TPA wishes to verify ownership of information it throws a challenge to the distant server. The server provides a proof of possession of information that is acknowledged to the TPA. The TPA validates the proof for its correctness utilizing the cryptographic keys applicable and develops a statement of ownership of information. This statement is then conveyed to the information proprietor as shown in Fig. 2c. This verification report from TPA will guide the information proprietor to evaluate their registered cloud service provider.

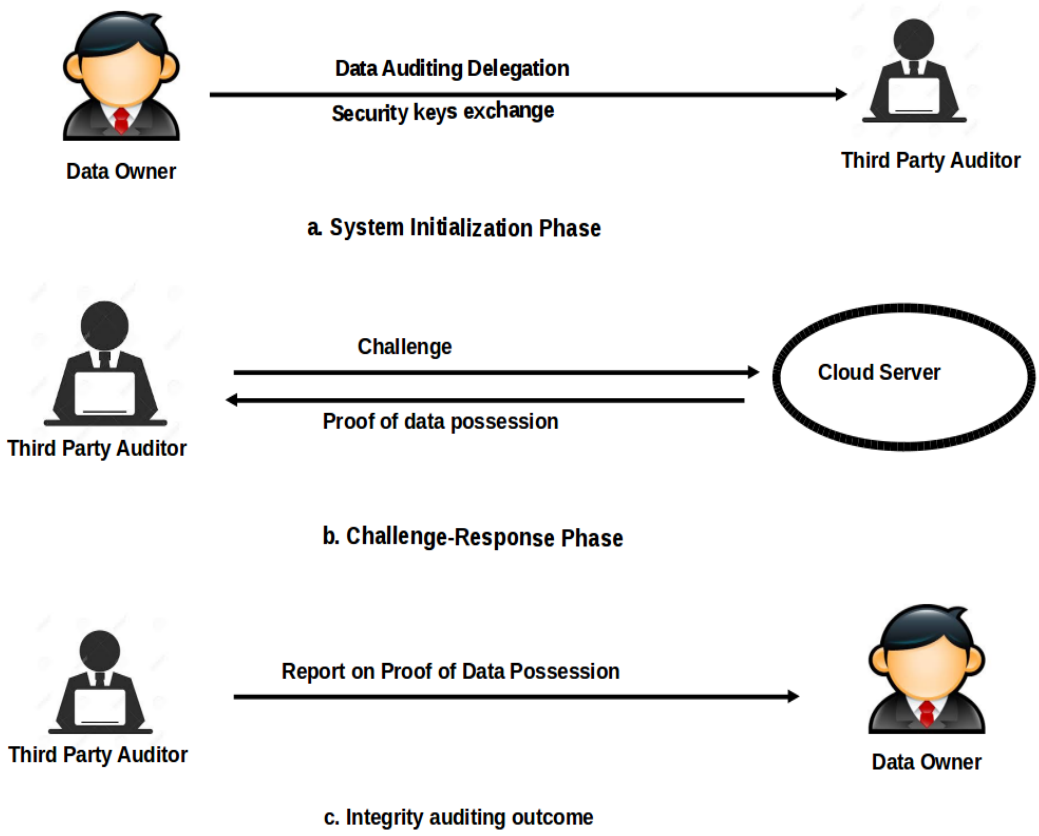

Figure 2: System framework for public auditing: a. System Initialization phase. b. Challenge-Response phase. c. Integrity auditing outcome.

1.2 Organization

The list of the paper is organised as follows: In Section 2 we have explained the challenging issues in

information storage auditing. Section 3 describes Public Honesty Verification with Group Client Repudiation. Section 4 outlines Public Verification for Collaborative Information in the Cloud. Section 5 discusses issues in Secure Verification and Deduplicating Information in Cloud. Section 6 and Section 7 presents issues on Auditing Cloud Consistency and Provable Verification for Deployed Database in Cloud. Section 8 emphasizes on Cloud Repository Auditing with Key-Disclosure Protection. Public Verification for Reconstructing-Code-Based Cloud Repository is given in Section 9. Conclusions are presented in section 10.

2. Challenging issues in information repository auditing

2.1 Dynamic auditing

As the outsourced information is dynamic by nature, it is essential to construct a verifying convention that supports for dynamic operations on outsourced information. Homomorphic authenticators are utilized in a public verification method to accomplish a constant transmission overhead. In the earlier homomorphic authenticated procedures, the chunk value was utilized in the course of authenticator estimation to prohibit distributed server to accomplish proof of possession of proprietor's information by adopting same authenticator. However the limitation of utilizing token value is that they develop complexity in chunk insertion operations. Insertion of an information chunk needs to update authenticated tags of all the subsequent information chunks, that is extremely idealistic in real cloud scenario. As a result, to thoroughly accomplish dynamic operations token value has to be prevented in tag estimation. To realize this condition, the classic Merkle Hash Tree (MHT) can be utilized. Leaf nodes of MHT are hashes of information file chunks. All of the information chunks can be validated by verifying root value and utilizing auxiliary information. Erway and his colleagues [5] introduced continued version of PDP framework namely vital provable information possession advocating updating on the owner's information. They discussed two mechanisms namely skiplist based and MHT based authenticated dictionary.

2.2 Collaborative auditing

Numerous information sincerity verifying conventions that are relevant for a single cloud scenario has been recently proposed (Ateniese and his colleagues [6]; Juels and Kaliski, [7]; Shacham and Waters, [8]) and they do not support multi cloud environments. Today's distributed repository frameworks support new Distributed File Systems (DFS) in order to offer low cost and location independence to proprietor's information. The benefit of such cooperative frameworks is the repository and processing of enormous amount of proprietor's information. Hence, highly efficient auditing mechanisms are required for such systems. Collaborative auditing is the verification of proprietor's information over multi clouds. The challenging problems for the collaborative verification are:

- The data transfer between distributed servers play an important role in cooperative verification. These homomorphic verifiable responses decreases transmission costs considerably and also reveals the tangible location of information outsourced in a multi-cloud surroundings. The advantage of using homomorphic verifiable responses is that it reduces transmission costs considerably and also reveal the

physical location of information deployed in a multi cloud neighborhood.

- Task assignment: The cooperative verifying conventions comprises of a TPA for verification and are appropriate to multi-cloud environment. For an adept cooperative verifying convention, a candid third party auditor is necessary.
- Security guarantee: information disclose assault and tag counterfeit assault are the two potential attacks in collaborative auditing. These assaults may also pose threat to secrecy of information and also to ownership of information. This verifying convention must present security guarantee for proprietor's information. In addition, in cooperative verification, the issues such as estimation complexity, repository overhead and system applicability need to be addressed.

2.3 Batch verification

The anticipation of cluster verification was initially introduced in Yamamoto's protocol [9]. The Batch auditing has several advantages over independent auditing:

- It can save the correspondence bandwidth, as the server just needs to forward the continuous sequence of all the tested information chunks whose size is identical to one information chunk.
- It can lower the reckoning intricacy for examination on both the public verifier and the distributed server. The group inspecting for various information chunks are used in numerous evaluating conventions, for instance, Ateniese's Provable Data Possession (PDP) [10], Juel's Proof of Retrievability (POR) [7] and Zhu's Cooperative Provable Data Possession (CPDP) [11] and so on.

Wang and his colleagues [12] presents a cluster verifying convention for several information chunks from various information proprietors. In spite of the fact that the cluster verifying can incredibly enhance the adeptness of verifying, while outlining the group verification protocol, it is important to study the data processing intricacy and transmission overhead for cluster operations. Yang and his colleagues [13] have performed a comprehensive review on repository examination approaches. Set of prerequisites of the reviewing mechanisms are presented for information repository in distributed computing.

2.4 Support for blockless verification

A verification scheme without the adoption of certification labels and signature aggregation mechanisms depends upon the server to send the challenged chunks to assure the integrity. The drawback of this scheme is that there is more transmission overhead at the server and also the effectiveness of verification scheme is affected. Although blockless verification can improve adeptness of verification scheme and lower transmission overhead considerably, it may also let the server to deceive. Assume the information proprietor desires to carry out any update operation say the information proprietor desires to alter a chunk. It is viable that after the update operation the server is preserving prior information and its signatures. As both the information and signatures are genuine, so the verifier may not be capable of recognizing whether the information is updated precisely or not.

2.5 Privacy preserving

When information proprietor deploy information to the distant cloud or delegate the verification job to the trustworthy third party, it is essential for them that the verifiers or cloud not be given the freedom to acquire intelligence of the information content or be able to create a duplicate of the primary information. That is, most of the information verification mechanisms for the cloud servers generally believe that the public verifier is a reliable delegate; however such an irrelevant inference additionally leads to information leakage. Randomization of information chunks and labels is a trivial mechanism to address the security problem to avoid label or information leakage throughout the auditing phase.

2.6 Error localization

As per the survey of existing mechanisms, most of them yields binary results about verification of information (Ateniese and his colleagues [6]; Juels and Kaliski, [7]; Shacham and Waters, [8]). The proprietor's information is appropriated over numerous servers; one realizes the repository status of information across multiple servers but no information about the misconducting server.

2.7 Accountability

Usually, the distributed server is considered as semi-trusted party. The public verifier discloses the sincerity of distributed server only. The verification record need to identify not only the correctness of information but also account for the entity that is authoritative if any complication arises, including information proprietor, public verifier and distributed server. There is a need to achieve accountability when all the entities are malignant.

2.8 Contribution

This summary presents a State of the Art work in Data Auditing and Security in Cloud Computing. We have compiled the techniques and algorithms with their performance, advantages and disadvantages. We have indicated the scope and issues that needs future research.

3. Public honesty verification with group client repudiation

With information repository and distribution administration supplied by the cloud, customers can conveniently work together as a cluster by distributing information with each other. For security reasons, when a customer quits the cluster or misbehaves, the customer ought to be repudiated from the cluster. As a result, this repudiated customer need no longer be able to retrieve and alter combined information, and the signatures created by this repudiated customer are no longer legitimate to the cluster. Therefore, even though the content of collective information is not modified during customer repudiation, the chunks, that were apriori signed by the repudiated customer, still needs to be re-signed by the current customer in the cluster. Hence the sincerity of the entire information can still be proved with the public keys of existent customers only. In this section we study the Public Honesty Verification with Group Client Repudiation.

3.1 System Framework

The system architecture includes: the distributed storage server, ensemble of clients and a public verifier (see Fig. 3.) Batch clients comprise of an information proprietor and various customers. Information repository services are given by the cloud storage server to the collection of clients. Third party auditor performs the information trustworthiness of the combined information saved in the distributed server. The information proprietor can encode and transfer the information to the distant distributed repository server. The information proprietor has the right to safely repudiate a batch client when the batch customer is discovered malignant or the agreement of the client is terminated.

Jiang and his colleagues [14] ensures public trustworthiness with group client repudiation. A collusion attack problem is considered where a renounced client can conspire with a malicious cloud server to change the group client's information. There is a possibility that one of the user in the group may behave maliciously. The data owner revokes the malicious user from the group. Security is of concern in the group users' data when a semi-trusted cloud server co-operates with the revoked user. The proposed mechanism supports the group information encoding and decoding during data repair process and achieves proficient and secure client renouncement. It is constructed using vector assurance scheme, Asymmetric Group Key Agreement (AGKA) scheme and verifier local revocation aggregate signature scheme. The system model is shown in Fig. 3. It has been debated that the most proficient technique is to safely outsource neighborhood repository to a distant distributed server. Ateniese and his colleagues [10] and Juels and his colleagues [7] introduced the mechanisms of Verifiable Information Ownership and Proofs of Retrievability (PoR). Homomorphic authentication approach has been used to reduce both the transmission and data processing cost.

Figure 3: Cloud Storage Model

Wang and his colleagues [15] introduced public inspecting system for the trustworthiness of transmitted data with effective customer denial. By using the notion of intermediary re-signatures, the cloud is permitted to re-sign chunks for existent clients in the course of client repudiation, so that current clients need not download and

re-sign chunks. In addition, an auditor continually examines the candidness of assembled data without retrieving the complete data from the cloud. The scheme improves cluster reviewing by examining varied reviewing jobs at the same period. The mechanism can be extended to implement collusion-resistant intermediary re-signature approaches while also supporting public verification.

Reference [16] also achieves secure batch client elimination along with their vital public forthrightness analyzing mechanism. The scheme depends on polynomial confirmation and adopts intermediary label update procedures which endorse public reviewing and dynamic user revocation. This scheme does not support cipher text store. Raghavendra and his colleagues [17] proposed a Most Significant Index Generation Technique (MSIGT) that improves safe and effective token creation period adopting a Most Significant Digit (MSD) radix sort. An analytical framework is refined to encode the indexed keywords for safe token creation. The advantage of the scheme is that it reduces the cost to the data owner.

Further considering the verification of outsourced database, Bennabbas and his colleagues [18] discussed the realistic testable database mechanism established on the rigidity of the subbatch association issue in bilinear groups with complex order. This mechanism does not bolster the feature of public validation. While Catalano and Fiore [19] achieves improved public validation along with their provable database from vector commitment mechanism. The mechanism presumes that the client can learn apriori the outsourcing function and the dimension of the outsourced fixed database. Backes and his colleagues [20] address the problem of verifiable delegation of computations on outsourced data. The solution works for computations over integers and supports the evaluation of arithmetic circuits. It also solves the security problem of Catalano-Fiore MAC completely.

Key management issue arises when various clients are repudiated from the group. This problem is addressed by Bruhadeshwar and Kulkarni [21], they discussed on a family of key management algorithms for productively disseminating the new group key when various clients are repudiated from the group. The storage at the group controller is linear and the storage at the clients is logarithmic to the size of the group. Techniques are illustrated to decrease the number of keys stored by the clients and the group manager. Algorithms are suited for overlay multicast applications. In heterogeneous frameworks, the algorithms can be used to enhance battery life span of wireless systems. Energy consumption is dominated by the amount of transmitted data. Raghavendra and his colleagues [22] introduced an effective procedure for keyword inquiry over encoded cloud information. In this scheme token creation procedure for keywords is constructed by utilizing split factor. The keywords are saved in wildcard based method within the token tree that is saved safely with little repository cost. The mechanism is adept in terms of index creation and repository cost.

Li and his colleagues [23] proposed a convertible Identity Based Encryption (IBE) scheme in the server-assisted framework. It discharges the vast majority of the key generation associated procedure to a Key Update Cloud Service Provider. This objective is accomplished by using a novel collusion-resistant technique. The disadvantage is that key-issuing stage in the proposed scheme is relatively longer than that in the IBE scheme. To support an adaptable encryption of assets in RBAC frameworks, Zhu and his colleagues [24] presents a generic role-based encryption over Role-Based Access Control (RBAC) model. The proposed design enhances completely collusion security and implements the renouncement at minimal cost. Hao and Nenghai [25]

suggested remote information honesty checking convention for distributed storage. The convention is appropriate for giving honesty assurance of client's information and improves the operations on information at the chunk level, and enhances public testability. The mechanism is safe against the semi-trusted server. It is effective in terms of data processing, calculation and storage costs. Data level dynamics at minimum costs is yet to be achieved.

Li and his colleagues [26] introduced an effective verifiable information ownership mechanism that utilizes a SN (sequence number)- BN (chunk number) vector to support information chunk modification. The mechanism is adept with reduced estimation, repository and correspondence overhead. An extensive PDP mechanism that has huge proficiency and fulfils every fundamental specification is provided. The limitation is that public verifiability, secrecy protection, legitimacy and multiple-duplicate inspecting are not supported. Ni and his colleagues [27] designed a privacy-protection reviewing convention for the distributed storage as discussed in [28]. A dynamic attacker can change the evidence of verification to deceive the verifier and the data possessor such that the distant cloud documents are uncorrupted, but the documents are impaired.

Extending the work from single data proprietor to multi-proprietor, Wang and his colleagues [29] presents a public auditing mechanism to review the righteousness of multi-proprietor information in a semi-trusted cloud by taking the benefit of multisignatures. The confirmation period and capacity overhead of signatures on multi-proprietor information in the cloud are independent with the quantity of proprietors. The limitation is that it has high communication cost and verification time when the number of elements increase. Xue and Hong [30] proposed a vital immune batch allocating system in public distributed computing. In the proposed system, the administration authority is permitted to few particular cluster individuals. Shared records are securely stored in cloud servers. TGDH mechanism is built to dynamically update the group key pair. Though the group individuals are online together, the proposed mechanism performs well. Forward secrecy and reverse secrecy are given by upgrading computerized envelopes in view of intermediary re-encryption. The scheme accomplishes the design objective and maintains a lower data processing intricacy and transmission overhead for every individuals of the cluster.

Luo and his colleagues [31] presents a public verification mechanism for the honesty of combined information with effective and collusion resistant client repudiation. Polynomial-based validation labels are developed which supports secure and effective public auditing. The mechanism is protected and effective, the aggregate overhead of the auditing mechanism is relatively small. Dong and his colleagues [32] achieves information privacy against untrusted cloud. They proposed a secure, effective and versatile information coordinated mechanism. Security examination demonstrates that the proposed mechanism is safe against versatile chosen ciphertext attacks. Experimental analysis demonstrated that it is exceptionally productive and has small overhead on estimation, communication and storage. The scheme does not achieve data consistency.

Huang and his colleagues [33] presents a quality based secure information sharing mechanism with efficient revocation in distributed computing. The design ensures information security and accomplishes fine-grained access control. The mechanism accomplishes prompt attribute repudiation which ensures forward and backward security and brings about low data processing cost on clients. Park and his colleagues [34] proposed Revocable

Identity-Based Encryption (RIBE) schemes with a consistent number of private key components. It is constructed in three-levelled multilinear maps. The proposed scheme possesses a consistent number of group components in private key and update key. Another Revocable Identity-Based Encryption (RIBE) scheme is built with decreased public parameters and short keys are generated by consolidating the Hierarchical Identity-Based Encryption (HIBE) mechanism. Constraint of the second Revocable Identity-Based Encryption (RIBE) scheme is that it requires high-levelled multilinear maps.

Confidentiality-protecting public auditing convention is proposed by Zhang and his colleagues [35] that uses opportunist assortment work. It comprises of the following features: (1) the individuality protection of information client is saved for distributed server; (2) the legitimacy of the transferred information is confirmed; (3) information security is safeguarded for the examiner in evaluating process; (4) calculation cost to create information label is small. The disadvantage is that the cloud server has high computation cost. Hwang and his colleagues [36] outlined a group signature mechanism advocating the controllable linkability. The considerable benefit of this scheme is that the signature length is short. The proposed scheme bolsters security features for example, secrecy, traceability, nonframeability, and linkability under a random oracle model. Privacy is not preserved by global linkability. Hong and his colleagues [37] revisited the proposed design by Yang i.e., a multi-authorization ciphertext-approach, feature established encryption-based data access regulation for distributed repository. It embraces a bidirectional re-encoding strategy in ciphertext restoring. An attack technique is proposed that uses a unidirectional re-encoding mechanism.

Among the various existing efficient public auditing for shared data mechanisms, Yaun and Yu [38] proposed an effective verifying mechanism for cloud information sharing services portrayed by multiuser changes, public verification, large fault location likelihood, effective client revocation and pragmatic computational/communication inspecting performance. The scheme overcomes client impersonation attack and permits the customer to review the honesty of a combined record with a steady estimation overhead and a limited communication cost. The drawback is that it does not accomplish reliability and error detection. Li and his colleagues [39] presents two confidentiality conserving public verifying conventions for secure stockpiling in cloud. Both conventions depend on the online/offline signatures, through which a client just requires to accomplish low estimation. They bolster batch auditing and information dynamics. The disadvantage is that time cost increases continuously as the number of chunks increases at the user side.

Cryptographic approaches are used in few of the verifying schemes such as, Hur and his colleagues [40] proposed a cryptographic approach to deal with fragile access control on the outsourced information, that is double encryption convention utilizing the combined attributes of the ciphertext-approach encryption and group key administration algorithm. The proposed mechanism permits an information proprietor to characterize the access control strategy and authorize on his outsourced information. It also features a system that empowers more fine-grained access control with effective characteristic and customer repudiation capability. It is proficient and scalable to safely deal with the outsourced data. The drawback of the scheme is that the revoked client can access the outsourced information with other attributes that he holds.

Dong and his colleagues [41] presents a privacy safeguarding and secure information sharing strategy in

distributed computing by employing Ciphertext Policy Attribute-Based Encoding (CPABE) and the strategy of Identity-Based Encryption (IBE). The technique assures fine-grained information admission control, in backward secrecy and protection against collusion of customers with the cloud and supports user addition, revocation and attributes modifications. The scheme does not reveal any attributes of clients to the cloud. It has low overhead and efficient. The scheme needs to be implemented in real Cloud Service Provider (CSP) platform. Wu and his colleagues [42] presents a generic construction, which uses two Ciphertext Policy Attribute-based Encoding (CPABE) schemes as building blocks. The scheme can revoke on attribute per encryption. The model of CP-ABE supports

the attribute revocation under the direct revocation model, in which the repudiation record is inserted in the ciphertext and none of the clients secret keys are influenced by the renouncement procedure.

Muthi Reddy and his colleagues [43] discuss on secure information sharing in distributed computing. They have analyzed different issues in data security and reviewed on various schemes that provide secure information sharing in distributed computing. Lu and Li [44] proposed a certificate-based agent re-encoding mechanism (CB-PRE) deficient of bilinear pairings. It demonstrates safe under the computational Diffie-Hellman expectation in the arbitrary prediction model. The mechanism essentially reduces the computation cost by avoiding tedious bilinear matching operations. In contrast with the previous mechanisms with bilinear pairings, it has improvement in the calculation proficiency. The CB-PRE mechanism requires to be developed in the standard model without bilinear pairings.

Both, Identification privacy and trackability for cluster individuals are protected by a proficient public verifying solution that is suggested by Yang and his colleagues [45]. The scheme accomplishes information security during authenticator generation by using blind signature. In this scheme, the identification of cluster individuals are unknown to the auditor and the cluster administrator can reveal the identification of untruthful customer in case of controversy. Identity traceability is accomplished through the group manager. The scheme has low overhead to implement both identification privacy and trackability. The data processing cost on the cluster manager needs to be reduced while lightweight authenticator creation has not been addressed.

A safe way for key distribution has been discussed by Zhu and his colleagues [46] where the clients can safely acquire their secret keys from cluster administrator. The scheme likewise fulfils fragile admission control, and repudiated customers cannot approach the cloud once they are repudiated. The scheme is protected from collusion attack. By utilizing the polynomial function, the mechanism accomplishes a secure user revocation. It is efficient as clients need not modify their secret keys else either a client participates in the cluster or a user is eliminated from the cluster. A revision on works on secrecy and protection problem in cloud information repository has been performed by Selvamani and Jayanthi [47]. They have examined about encryption based strategies and auditability schemes. Public verifier cannot acquire any information details at the time of public inspecting and hence integrity is ensured. Furthermore, it is observed that the auditing jobs can be carried out concurrently. A detailed review of various information trustworthiness strategies for cloud computing has been performed by Garg and Bawa [48]. They have observed that most of the current conventions focus on honesty checks to different information storage frameworks.

Xu and his colleagues [49] propose Multi-authorization Proxy Re- Encoding method based on ciphertext-policy attribute-based encryption (MPRE-CPABE) for distributed repository frameworks. The Weighted Access Structure (WAS) is introduced that reduces the estimation overhead of granting the keys. MPRE-CPABE utilizes intermediary re-encryption to minimize the estimation overhead of access revocation. This scheme enormously minimizes the estimation overhead of the creation of key elements and the withdrawal of customers access right.

The impediment of the mechanism is that it requires longer computational time for setup. Raghavendra and his colleagues [50] presents a safe multi-owner information distribution for vital cluster in the cloud with RSA Chinese Remainder Theorem (RSA-CRT) encode approach and substring token creation procedure. RSA-CRT effectively handles repudiation list, key administration, with decreased repository and reckoning cost. The substring token creation algorithm decreases the repository space and Search algorithm reduces the time to search files from the cloud. The limitation is that the protocol does not support multi-media files.

Further, More and Chaudhari [51] presents a secure and effective privacy preserving auditing scheme. The mechanism utilizes TPA (Third Party Auditor), performs the inspection without retrieving the data copy, subsequently security is preserved. The data is divided into blocks and then stored in the encoded format in the distributed storage, thus maintaining the privacy of data. The information uprightness is confirmed by TPA on demand of the customer by checking both the signatures.

The proposed scheme does not support information dynamic operations, for example, updation, deletion and insertion of data. Wang [52] proposed proxy provable information ownership (PPDP) convention. In public clouds, PPDP is a phenomenon of important significance while the customer cannot achieve the distant information ownership auditing. An effective PPDP convention is outlined by utilizing bilinear pairings. The convention counteracts mischievous customers and has small transmission overhead. The comparison of schemes for Public Honesty Verification with Group Client Repudiation is shown in Table 1.

4. Public auditing for collaborative information in the cloud

Cloud service suppliers offer customers adept and extensible information repository benefits. Sharing information among various customers is one of the highest appealing features that inspires distributed repository.

Therefore, it is also essential to guarantee the honesty of combined information in the cloud is legitimate. Currently, many schemes [10,8,53,54] have been suggested to grant not only a information proprietor itself but also a public examiner to regularly carry out honesty examination without downloading the complete information from the cloud, that is referred to as public reviewing.

However, an advanced compelling secrecy problem introduced in the case of combined information is the leakage of personality secrecy to public auditors. In this section we present an extensive survey on public verification for Collaborative Information in the cloud.

Table 1: Comparison of schemes for public honesty verification with group client repudiation

Authors	**Concept**	**Algorithm**	**Advantages**	**Disadvantages**
Jiang and his colleagues 2016 [14]	Efficient public integrity verification with secure group client repudiation.	vector commitment, Asymmetric Group Key Agreement, verifier-local revocation group signature.	Secure against the collusion attack.	More computation cost.
Wang and his colleagues 2015 [15]	Public verification for combined information with effective client repudiation.	Homomorphic Authenticable Proxy Resignature Scheme (HAPS), Panda mechanism.	Secure User Revocation, Public auditing.	Collusion of repudiated customer and cloud.
Xue and Hong, 2014 [30]	Dynamic secure group data sharing.	Group Initialization, Batch Regulation Authority Administration, Cluster customer addition and elimination.	Lower computational complexity and communication overhead.	The complexity of encryption and communication is linear with the length of the file.
Luo and his colleagues 2015 [31]	Honesty examining for combined information with safe customer repudiation	Public auditing scheme, Polynomial-based authentication tags	Total overhead is small	User revocation takes longer time
Dong and his colleagues 2015 [32]	Protected and adaptable information collaboration assistance in distributed computing	Secure and Scalable Data Collaboration service (SECO) scheme.	Secure against ciphertext attacks	Data consistency is not achieved.
Zhang and his colleagues 2016 [35]	Efficient chameleon hashing-based privacy preserving auditing	Identity privacy-preserving public auditing protocol	Identity privacy preserved, low computation cost.	Cloud server has large computation cost.
Dong and his colleagues 2014 [41]	Privacy-preserving and secure data sharing in cloud.	System initialization, Encryption, Key generation, Decryption.	Fragile information access control, safe against conspiracy attack.	Scheme has to be implemented in real cloud platform.
Hwang and his colleagues 2015 [36]	Short dynamic group signature supporting controllable linkability.	PS-OL scheme.	Yields short signature, proves the security features.	Privacy is not preserved by global linkability.
Yaun and Yu, 2015 [38]	Public honesty examining for vital information distribution with multicustomer modification.	System setup, challenge, prove, validation, customer repudiation.	Large error revelation probability, effective customer repudiation.	Scheme does not achieve reliability and error detection Probability.
Li and his colleagues 2016 [39]	Secrecy-Conserving Public Inspecting Convention for Low-Accomplishment	Secrecy-Conserving Public Inspecting Convention.	Lightweight computation, supports batch auditing.	Additional time cost as the number of chunks increases at the user side.

	End Appliances in Cloud.			
Xu and his colleagues 2016 [49]	Multi-authority proxy reencryption based on CPABE for cloud storage system.	MPRE-CPABE scheme and WAS scheme.	Low computational cost of key distribution.	Longer computational time of setup.

4.1 System Model

The system architecture consists of three entities: the distributed server, a cluster of clients and auditor (see Fig. 4). Batch customers consist of an information possessor and a number of batch clients. The data owner generates combined information in the cloud and allocates it to the batch clients. Each customer of the batch is authorized to retrieve and alter the combined information. The distributed server stores both the combined information and its confirmation metadata (i.e., endorsements) authorized to retrieve and alter the combined information. The distributed server stores both the combined information and its confirmation metadata (i.e., endorsements).

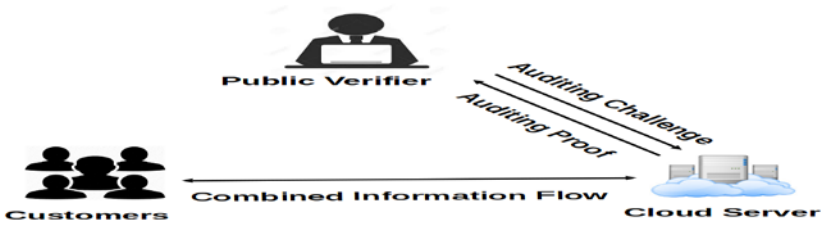

Figure 4: System framework consists of the distributed server, a cluster of clients and a public auditor.

Public auditor offers proficient information examining administration or an information client foreign to the batch expecting to utilize the combined data, can freely prove the honesty of joint data cached in the distributed server. When an auditor verifies the sincerity of the combined information, he initially transmits an inspecting challenge to the distributed server. After accepting the inspecting challenge, the distributed server acknowledges to the auditor with a reviewing evidence of the ownership of collective information. Then, the auditor examines the imperativeness of the complete information by proving the accuracy of the verifying proof. Wang and his colleagues [55] introduced a security protecting public evaluating framework for combined information in cloud by the scheme of One Ring to Rule them All (Oruta). Ring signatures are exploited to accomplish validation metadata anticipated to examine the accuracy of combined data. In the proposed protocol, the individuality of the endorser on every chunk in the combined information is maintained unrevealed from the public auditors, who can adequately verify combined data respectability without fetching the complete file. The scheme performs numerous reviewing jobs simultaneously. Limitation of the scheme is that the identity privacy is not preserved and does not support traceability. They have used the system model that is shown in Fig. 4. Shacham and Waters [8] composed two enhanced scheme. The main mechanism is constructed using Boneh-Lynn-

Shacham short signatures (BLS) and the second depends on spurious-haphazard functions. Recently, research on network catalogue-based cloud repository systems is performed, namely Chen and his colleagues [54] introduced Remote Data Checking (RDCNC), a protected and effective Remote Data Checking (RDC) mechanism for network catalogue-based cloud repository systems. RDC-NC alleviates current attacks and is able to preserve low correspondence expense of the repair element. The mechanism is computationally reasonable for both customers and servers. The drawback of the mechanism is that the correspondance rate increases directly with the document size. Venugopal and his colleagues [56] use soft computing techniques for data mining applications. A safe distributed storage maintenance is designed by Cao and his colleagues [53] that addresses the issue of fidelity. The scheme supports public honesty confirmation. To totally release the information proprietor from the burden of being on the web after information deployment, a correct repair result is outlined so that no metadata should be produced on the fly for reconstructed information. The analysis shows that the convention has less capacity cost, significant speedy information recovery and similar transmission cost. The scheme does not detect decodability efficiently. Wang [57] proposed an innovative procedure, Uncertainty, to ensure both existence security and cooperative protection with small data deficit. The secrecy model is characterized and the security certification of Uncertainty against both existence leakage and cooperative leakage is measured. It isdemonstrated that the data damage of Ambiguity is lower than the exemplary generality-based anonymization system. An enhanced mechanism *PriView* is built that can accomplish preferable data loss over Ambiguity. The scheme does not include dynamic datasets. One can design tools and approaches which address all aspects of cloud responsibility by using the Cloud Accountability Life Cycle (CALC) and three deliberation layers, proposed by Ko and his colleagues [58]. They have examined responsibility and auditability as an essential viewpoint towards expanding trust in distributed computing. Logging and mapping of virtual machines to physical machines in CALC has not been achieved. A cryptographic construct namely the hourglass schemes [59], empowers customers to check remotely if a server stores documents in a specific target format. Hourglass schemes influence server resource limits to accomplish their security confirmations. Three primary hourglass developments are discussed; two draw on storage-access times as an asset bound, and another on hardness presumptions on the RSA cryptosystem. Xu and his colleagues [60] introduced a Certificateless Proxy Re-encoding mechanism (CL-PRE) for cloud-established information sharing. CL-PRE exceptionally coordinates identification based public key into intermediary re-encryption, and dispenses with the key insurance issue in customary identification based encryption; the certificates are not used to ensure the legitimacy of public keys. The overhead of arbitrary re-encryption keys is high. Further Qin and his colleagues [61] introduced a firmly safe and proficient Certificateless Proxy Re-encoding mechanism (CLPRE) lacking pairings for cloud based information distribution scenario. The mechanism is inferably IND-CCA reliable in a more robust protected framework. It is observed that the scheme is firmly protected and applicable for cloud positioned information distribution in terms of estimation and transmission overhead for information proprietor, Cloud Service Provider (CSP) and information receiver. Provable information ownership model [62] gives trustworthiness and originality in a vital, multi-client context. By utilizing reliable hardware on the server, Forking and rollback assaults are eliminated. The proposed constructions eliminate client-side storage costs and are relevant for situations in which various users work cooperatively on deployed information. It does not support load-balancing across multiple servers. Considering vital groups in a semi-trusted cloud, Liu and his colleagues [63] designed a protected data distribution

mechanism, Mona. Customer repudiation is effectively accomplished through a repudiation record without refreshing the private keys of the rest of the customers. The magnitude and calculation overhead of encoding are consistent and resilient with the number of relinquished clients. The drawback is that it has high estimation overhead. Rasheed and Hassan [64] analyzed the verification of cloud computing in terms of client inspecting prerequisites, standard procedures for secure reviewing and current cloud assistance provider facilities for satisfying review requisites. Client verifying requisites are classified into infrastructure secure evaluation and information safety verification. *TimePRE* framework [65] achieves small-grained fetch control and adaptable client repudiation. Every client's right to retrieve is successful in a pre-decided timeframe and empower the CSP to re-scramble encoded texts. The drawback of the mechanism is that it requires the powerful time periods to be the same for all features related with a client. Yu and his colleagues [66] revised triple verifying systems for collective information in the distributed systems, including two identity secrecy-maintaining reviewing schemes and cloud storage uprightness inspecting system. It is observed that if the distributed server does not authorize its acknowledgement, a dynamic attacker can instigate an assault to breach the repository accuracy. In particular, the attacker can immediately change the cloud information without being distinguished by the reviewer in the auditing stage. A protected digital signature mechanism is proposed to settle this issue. Abbas and Khan [67] have surveyed the methodologies and techniques that are at present being utilized to manage the imperative issue of secrecy. The authors have detailed the scientific classification of the systems that have been utilized to safeguard the security of the current information. There is a need to set up an effective verifying and liability mechanisms. There is a compelling need to construct more adaptable and proficient information examination procedures without trading off on security of the cloud. Considering the issue of identification security and trackability, Yang and his colleagues [68] designed a state-of-the-art structure for information distribution in cloud and formalized the meaning of public verification mechanism for combined cloud information advocating identification security and trackability. The mechanism ensures individuality protection and trackability. The constraint of the mechanism is that there is high computational weight on the group administrator and lightweight authenticator generation has not been addressed. Further to resolve the issue of information honesty confirmation (by an intermediary verifier), Singh and Pasupuleti [69] proposed a convention to perform proficient chunk-level and fragile effective information refresh process on information saved on cloud utilizing a variant Opportunist Certification Tree. The proposed conventions are productive and can resist replay, replace and forge attacks. Overall computation time per task allows the increase in number of auditing tasks. Li and his colleagues [70] proposed a key-revising and authorization developing scheme with void-intelligence protection of the stored documents for safe cloud information examination, which includes void learning evidence frameworks, intermediary re-signature and homomorphic direct endorser. The scheme has low communication and computation cost while maintaining attractive security. The time complexity of key update is linear with the updating times. In order to decrease the workloads of information clients caused due to group client revocation, Cui and his colleagues [71] proposed Server-Aided Revocable Attribute-Based Encryption (SR-ABE) mechanism in which the data client's workloads are delegated to an untrusted server and the client just needs to store a key of constant size. A security framework for SR-ABE is designed. This does not require any protected channels for key transmission. In the decryption stage, information client just needs to perform one exponentiation calculation to decrypt a cipher-text. A Novel and Efficient Public Auditing mechanism [72] for cloud information (NaEPASC), checks the trustworthiness of the information saved in the

cloud. NaEPASC adopts an identity-based aggregate signature, to develop real-time and homomorphic verifiable labels, and the TPA can review the accuracy in favor of the clients. The mechanism eliminates the burden on cloud users of inspecting tasks, and in addition reduces the clients fear of losing their keys. This mechanism is adept and secure in verifying the uprightness of the information stored in the cloud. It has a considerable estimation overhead on the server side and TPA has increased verification time. Raghavendra and his colleagues [73] present most significant single keyword inquiry over encoded cloud information that supports effective and precise search. The scheme supports a considerable number of information documents, decreases token creation time, token repository space and keyword inquiry time. Limitation is that the mechanism does not support index storage space on multimedia. The comparison of schemes for Public Verification of Combined Dynamic Cloud Information is summarized in Table 2.

Table 2: Comparison of schemes for public verification of combined dynamic cloud information.

Authors	**Concept**	**Algorithm**	**Advantages**	**Disadvantages**
Cao and his colleagues 2012 [53]	Secure and Reliable Cloud Storage Service.	LT codes-based cloud storage service (LTCS).	Low storage cost, Faster data retrieval	Decodability detection need to be achieved.
Xu and his colleagues 2012 [60]	Secure information Sharing with Public Cloud.	Certificateless Proxy Re-Encryption Scheme, multi-proxy CL-PRE and randomized CL-PRE.	Eliminates the key escrow problem.	Overhead of arbitrary re-encryption keys is high.
Liu and his colleagues 2013 [63]	Safe multi-owner information sharing for effective clusters in the cloud.	Multi-owner data sharing scheme.	Constant storage Overhead.	High estimation overhead.
Liu and his colleagues 2014 [65]	Time-based agent re-encryption line mechanism.	Time-based Proxy Re-Encryption (*TimePRE*) scheme.	Scalable, Fine-grained access control, Data confidentiality.	Effective time periods is same for all attributes of the user.
Wang and his colleagues 2014, [55]	Safety-protecting public verification for combined information in the cloud.	Oruta and Homomorphic Authenticable Re-signature (HARS) mechanisms.	Identity of the signer is kept private, supports batch auditing.	Data freshness is not proved.
Qin and his colleagues 2015, [61]	Reliable information sharing in public cloud by using Agent Re-encryption.	Certificateless Proxy Re-encoding (CLPRE) scheme.	Low computation cost and communication overhead.	High storage overhead at data owner.
Yang and his colleagues 2016 [68]	Public verification for shared information in distributed storage.	Key generation (KeyGen), Proof, Verify, Revoke member phase.	Data privacy is achieved.	High computational burden on the batch administrator.
Singh and Pasupuleti, 2016, [69]	Public Auditing and Data Dynamics for Data Storage Security	Public auditing and dynamic data update scheme.	Resistant to replace, replay and forge attacks.	More computation cost at the client side.

5. Secure verification and deduplicating information in cloud

Though distributed repository system has been extensively accepted, it is unsuccessful to furnish some substantial arising needs such as the capabilities of verifying honesty of cloud documents by cloud customers and identifying corresponding documents by distributed servers. In this section we have performed survey based on the problem of honesty verifying and protected deduplication on cloud information.

5.1 System Framework

As shown in Fig. 5. the SecCloud framework has three objects: Cloud customers, distributed servers and verifier. Cloud Customers possess large documents to be hoarded and depend on the cloud for information conservation and estimation. Distributed servers virtualize the assets as determined by the prerequisites of customers and present them as repository pools. Customer achieves the identical checkup with the distributed server to validate if such a document is saved in cloud repository or not before transferring a document. If there is a matching document, another convention called Proof of Ownership is executed among the customer and the distributed repository server. Distributed server acknowledges the customer that it has the same copy of the document and hence does not permit the customer to upload the document. The verifier provides users certain support with uploading and assess their deployed data, and acts like authentication supremacy.

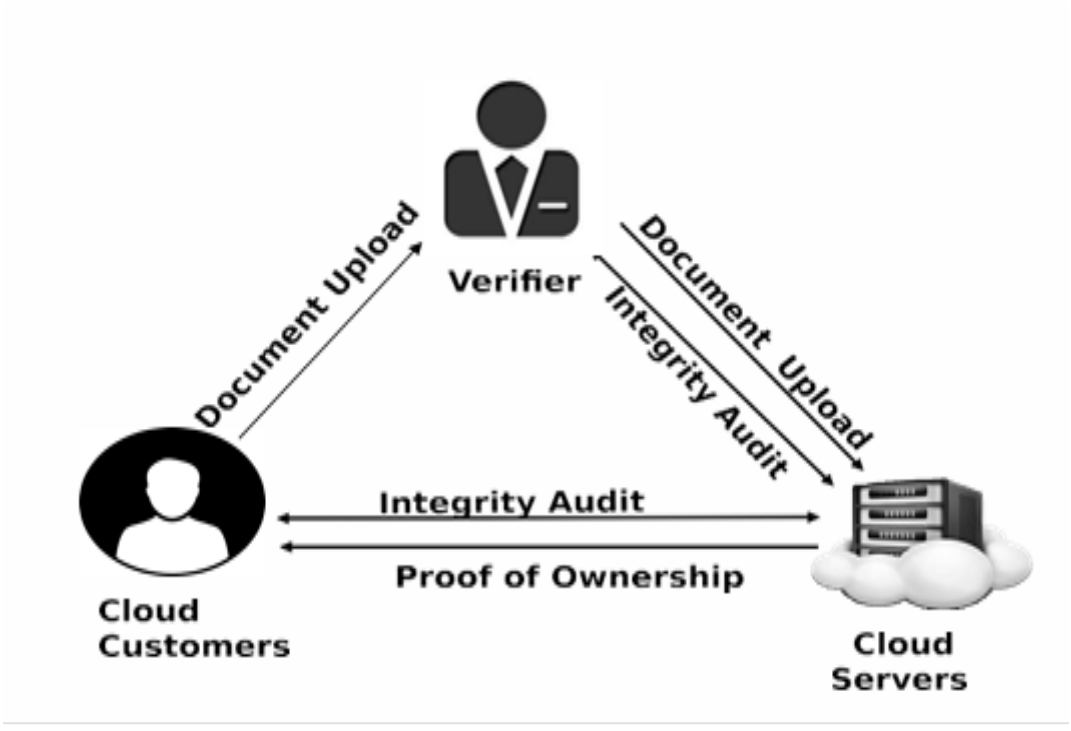

Figure 5: Cloud data auditing and deduplication framework.

Li and his colleagues [74] proposed two secure frameworks, SecCloud and SecCloud+ where these two frameworks accomplish both information sincerity and deduplication in cloud. SecCloud considers a verifying object with a provision of a MapReduce cloud, that provides customers some assistance with generating data

tags and in addition examine the sincerity of information that have been saved in cloud. The computation by customer in SecCloud is considerably decreased during the record transferring and evaluating stages. SecCloud+ encodes user's information before deploying, empower honesty verification and safe deduplication on encoded information.

The Seccloud architecture is shown in Fig. 5. Various researchers worked on the issue of integrity and deduplication of information in the cloud. They have proposed efficient deduplication mechanisms, few of them are discussed in this section. Li and his colleagues [75] proposed an approved information deduplication mechanism. They also displayed a few novel deduplication mechanisms encouraging approved duplicate verification in the hybrid cloud architecture. The mechanisms are safe in terms of internal and foreign assaults. Proof generation phase incurs little overhead.

The cloud deduplication frameworks [76], enhance the authenticity of information in the time of accomplishing the secrecy of the clients' deployed information without an encoding convention. The deduplication frameworks are implemented utilizing the Ramp secret allocation mechanism with little encrypting/decrypting cost. Wang and Chen [77] have performed survey on the methods of provable information repository and protected information deduplication.

They have examined systems for verifiable database deploying and the security challenges and solutions. Further, research direction recommended is publicly verifiable ODB, privacy-protecting VDB, user-revocable deduplication. Hur and his colleagues [78] examined server-side deduplication mechanism for encoded information. The procedure grants the distributed server to restrict access to deployed information even when the proprietorship renews actively. This counteracts information spillage to revoked clients and distributed storage server. Further, the proposed mechanism ensures information honesty against any tag irregularity assault. It involves extra computational overhead. Dekey [79], is a proficient and solid focalized key administration conspire for safe deduplication. Dekey employs deduplication among confluent keys and disseminates convergent key portions over various key servers, while safeguarding syntactic protection of convergent keys and secrecy of deployed information. Dekey is implemented utilizing the Ramp secret distribution mechanism with encrypting/decrypting overhead.

In order to accomplish record level and chunk level deduplication, Chen and his colleagues [80] proposed Block-Level Message-Locked Encryption (BL-MLE) scheme. The scheme also accomplishes chunk key administration and verification of possession utilizing a small set of metadata. It does not support proof of storage and is not computationally efficient.

In order to counteract deduplication of unpopular information, Stanek and Kencl [81] introduced intrinsic pressure between storage streamlining techniques and end-to-end encryption. It is resilient to client collusion assaults and never deduplicates unpopular files. The limitation of the scheme is that it has low space-saving efficiency. Extending the work to multi-server scenario, Miao and his colleagues [82] proposed multi-server supported deduplication mechanism using blind signature. The protocol can successfully oppose the conspiracy assault between the distributed server and different key servers. The scheme is secure and successfully opposes

the off-line brute force intrusion. It is expensive to record uploading. Zheng and his colleagues [83] proposed secure deduplication system that supports secure deduplication with strong video protection against malicious clients and untrusted cloud.

The algorithm is implemented utilizing RSA-OPRF convention and Threshold RSA-OPRF convention. It supports secure deduplication with resistance to limited information leakage and with guard against brute-force assaults over predictable videos. Computation overhead is high in case of decentralized servers. Yao and his colleagues [84] proposed a secure hierarchical deduplication framework to enhance privilege-based duplicate checks and privilege-based client profiling by the storage server. The framework depends on a novel Hierarchical Privilege-Based Predicate Encryption (HPBPE) protocol. HPBPE is used to create the cryptographic document tokens for copy checks without revealing the clients privilege data to the storage server. An improved mechanism called HPBPE-R is built to support dynamic privilege changes. Min and his colleagues [85] present fingermark administration mechanism called LRU-positioned Token Segregation and Incremental Modulo-K(INC-K) method. LRU-positioned Token Segregation utilizes the idea of tablet and employs admission conditions of the fingermark lookup in organizing fingermarks. It is observed that there is an increase in chunking time and decrease in deduplication ratio. Christian [86] discusses a study of twelve varieties of six ordering systems. It is suggested to implement the Febri model using indexing approaches and examination of learning systems for proficient and precise registering.

Xia and his colleagues [87] have reviewed various approaches of data deduplication. A detailed scientific categorization of the new information deduplication methods is explored that gives thought to significant issues of deduplication-based repository frameworks. As the volume of digital information progress to advance exponentially, there is a requirement for everlasting repository maintenance. Wang and his colleagues [88] proposed I-sieve, a formidable achievement of inline deduplication framework for use in distributed repository. I-sieve has incredible foreground performance contrasted with Internet Small Computer Systems Interface (iSCSI) applications. Moreover, I-sieve is suitable for deduplication in small storage situations, particularly with virtual machine applications.

The limitation of the scheme is that it has extra computational overhead. Considering the security of sensitive data, Raghavendra and his colleagues [89] introduce the Domain and Range Specific Multi-keyword Search (DRSMS) approach that minimizes the inquiry period and token repository space. The technique decreases token repository space and searchable time for top-*k* multi-keyword retrieval. It prevents sensitive data leakage and hence better privacy of keywords is achieved. The drawback of the scheme is that it requires more search time on the image data set. A public verifying mechanism [90] for distributed depository frameworks, achieves deduplication of encoded information and information trustworthiness examination inside the system. The distributed server can effectively examine the possession for original proprietors and the reviewer can accurately verify the trustworthiness of deduplicated information. The protocol enhances deduplication of encoded information by utilizing the strategy for intermediary re-encryption and achieves deduplication of information label by combining the labels from various proprietors. The comparison of schemes for Protected Auditing and Deduplicating Information in Cloud is shown in Table 3.

Table 3: Comparison of schemes for protected auditing and deduplicating information in cloud

Authors	Concept	Algorithm	Advantages	Disadvantages
Li and his colleagues 2014 [79]	Safe Deduplication with Efficient and Consistent Convergent Key administration.	Dekey, convergent key management scheme, Ramp secret sharing scheme	Provides secure deduplication, semantic protection of convergent keys.	Incurs encoding/ Decoding overhead.
Wang and his colleagues 2015 [88]	An Inline High Performance Deduplication System used in Cloud Storage	A novel Index table	Suitable for deduplication in small storage situations	High computation overhead.
Li and his colleagues 2015 [75]	Hybrid Cloud Approach for protection of approved Deduplication	Authorized data deduplication scheme.	Protected in terms of internal and external assaults.	Label creation introduces cost in the upload procedure.
Li and Jin, 2015 [74]	Secure auditing and deduplicating data in cloud.	SecCloud and SecCloud+.	Secure deduplication on encrypted data.	Increased time cost Response.
Hur and his colleagues 2016 [78]	Protected information deduplication with active ownership administration in cloud repository.	Deduplication scheme for encrypted data.	Prevents data leakage, assures information truthfulness.	Incurs additional computational overhead.
Stanek and Kencl, 2016 [81]	Secure Thresholded Data Deduplication for Cloud Storage.	Thresholded Data Deduplication Scheme.	Prevents deduplication of unpopular data.	Low space-saving efficiency.
Chen and his colleagues 2015 [80]	Block-Level Message-Locked Encoding for Safe huge Document Deduplication	Block-Level Message-Locked Encoding (BLMLE) scheme	Scheme achieves document-level and chunk-level deduplication.	Proposed scheme does not support proof of storage and is less computational efficient.
Zheng and his colleagues 2016 [83]	Encrypted Cloud Media Center with Secure Deduplication	The RSA-OPRF protocol, Threshold RSA-OPRF protocol	Guard against bruteforce assaults	High computation overhead.

6. Auditing cloud consistency

A cloud is a huge-scale distributed system where every chunk of information is duplicated on diversified geographically-distributed servers to accomplish high availability and high performance. Actually, mandated by the Consistency, Availability and Partition tolerance (CAP) principle, many cloud service providers (e.g., Amazon S3) only guarantee weak consistency, such as eventual consistency, for performance and high availability, where a customer can read stale information for an epoch of time. The Domain Name System (DNS) is a popular application that implements eventual consistency. But interactive applications need stronger

consistency assurance. Various applications have distinctive consistency requisites. For example, mail services need monotonic read consistency and read-your-write consistency, but social network services need causal consistency. In this section we present a review on auditing cloud consistency.

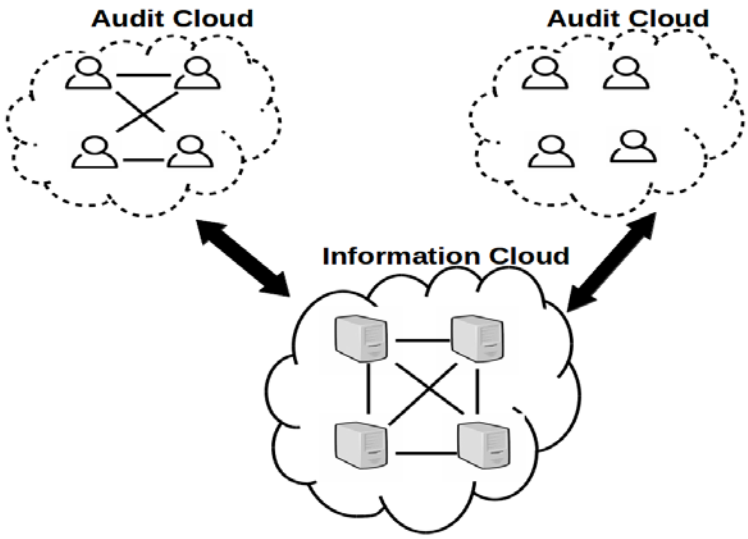

Figure 6: Auditing Cloud Consistency Framework.

6.1 Auditing Cloud Consistency Framework

As shown in Fig. 6, Auditing Cloud Consistency framework comprises of an information cloud, various verification clouds. The information cloud, managed by the cloud assistance supplier, is a key-esteem information repository framework, where every bit of information is distinguished by a particular key. To afford consistency-on services, the cloud service provider duplicates the entire information on numerous geographically allocated distributed servers. A verification cloud comprises of a cluster of clients that co-operate on a task, e.g., a file or a program. It is assumed that every client in the verification cloud is distinguished by a particular ID. Before deploying the task to the information cloud, the verification cloud and the information cloud participates in a service level agreement (SLA), which specifies the guaranteed level of firmness that ought to be given by the information cloud. The verification cloud checks whether the information cloud follows the SLA and evaluates the seriousness of infringement. Liu and his colleagues [91] presented an innovative model called Consistency as a Service framework. It incorporates a wide information cloud and many tiny verification clouds that are unique. The information cloud is hosted and monitored by the cloud service providers, while verification cloud is accessed by individual users for the purpose of verification and checking its consistency without any failure. A dual auditing architecture has been built in for effective functioning of the system model. In turn, it depends on a loosely coordinated clock in the auditing cloud. It monitors and measures the number of misbehaviors and its severity. The staleness of significance of a read is also verified and has been designed to expose as many misbehaviors as feasible. Simulations and real cloud implementations have been performed for validation of Heuristic Auditing Strategy (HAS). They have used the system model shown in Fig. 6. Golab and his colleagues [94] have addressed a few issues identified with the confirmation of firmness

features in histories of read/write register procedures. Instructions to perform consistency check online are additionally considered. Quantifying the seriousness of infringement empowers clients and assistance providers to arrange repayments equivalent to the seriousness of infringements. The limitation of the scheme is that it has not addressed *k*-atomicity verification problem. Raghavendra and his colleagues [95] present a technique called Rapid Similarity Search on Metric Space Object Stored in Cloud Environment (RSSMSO) that has build phase, inquiry phase, information transformation and search phase. The RSSMSO method ensures improved inquiry correctness with low communication cost. GentleRain [92] is a convention proposed for executing causal consistency for geo-reduplicated distributed information cache. For an assortment of workloads *GentleRain* gives very good throughput. The drawback of the protocol is that there is an increase in computation and storage overhead. Phansalkar and Dani [93] discusses on versatile certifications of particular information consistency model. The inconsistency detection logic ensures a prescient and tunable consistency metric with consistency index (CI). Consistency Index based Consistency Tuner (CICT) deals with the guideline of procrastinating the contradictory read procedures to cease it off dropping in the insecure duration. CICT is effectively exploited as workload scheduler. Acknowledgement period is high with a large number of duplicates and huge costs of desired CI. A 3-level security design [96] accomplishes better security improvement of cloud security. Various security challenges, vulnerabilities, assaults and threats that hamper the appropriation of distributed computing are examined. They have investigated different cloud services and also analyzed the security concern of every supplier. Jeevitha and his colleagues [97] have performed review on information storage security and privacy in distributed computing. Different techniques are discussed along with security challenges, advantages and disadvantages. They have performed analysis on information protection issues and secrecy preserving affairs related to distributed computing. The comparison of schemes for Auditing Cloud Consistency is shown in Table 4.

Table 4: comparison of schemes for auditing cloud consistency

Authors	**Concept**	**Algorithm**	**Advantages**	**Disadvantages**
Du and his colleagues 2014 [92]	Scalable Causal Consistency with Physical Clocks.	GentleRain protocol	Good throughput.	Increase in computation and storage overhead.
Phansalkar and Dani, 2015, [93]	Tunable consistency guarantees of selective data consistency model.	CI based selective data consistency Model.	Efficiently exploited as work-load scheduler.	High response time.
Liu and Wang, 2014, [91]	Auditing cloud consistency.	Local and Global consistency auditing, Heuristic Auditing Strategy (HAS).	Users assess and select an appropriate Cloud Service Provider (CSP).	Heuristic Auditing Strategy worsens when threshold value increases.

7. Provable verification for deployed database

The concept of database deploying allows the information proprietor to authorize the database management to a cloud service provider (CSP) that provides numerous database services to various customers. The outsourced database paradigm suffers from security challenges such as secrecy of outsourced data and verifiability of results. In this section we present a review on Provable Verification for Deployed Database.

7.1. System Model

The provable verifying mechanism of deployed database has four objects: the information proprietor, the clients, the cloud service provider (CSP) and the *Arbitration* Center (AC). The construction of provable verifying mechanism is as shown in Fig. 7.

- *Information Proprietor*: The information proprietor is an object who desires to deploy database to the CSP. Besides, he creates a confirmation format utilizing the Bloom filter and Merkle hash tree for checking the honesty of deployed database.
- *Client*: The client is an object that desires to access database services, who may acquire constrained repository volume and estimating capability.
- *Cloud Service Provider (CSP)*: The CSP is incharge of saving the encoded information and gives different database services to clients (e.g., searching).
- *Arbitration Center (AC)*: The AC performs as an unbiased observer to manage the conflict within the customer and the Cloud Service Provider (CSP).

The primitive of database outsourcing has been well studied in the past decades. In this section we have performed review on the existing database outsourcing schemes. Wang and his colleagues [98] present provable verifying mechanism of deployed database that can accomplish the validation of inquiry event regardless of the possibility of the result being null set. In addition, the mechanism provides customary database operations, for e.g., selection and projection. The drawback of the scheme is that it does not support dynamic database. The system model is shown in Fig. 7. Zhu and his colleagues [99] proposed an effective review service for confirming the trustworthiness of an untrusted and deployed repository. The verification service is developed on the methods: chunk constitution, arbitrary sampling and index hash table, assisting verifiable restoration to deployed information and recognition of inconsistency regularly. The audit framework checks the respectability with low computation cost and requires small additional repository to examine metadata.

Figure 7: The Deployed Database Architecture

A flexible and verifiable search mechanism [100] is designed using invertible Bloom filter to accomplish provability of search result. The proposed mechanism empowers the information proprietor to upload information tuple without the procedure of pre-counting. In this manner, it can improve dynamic information update and is suitable for dynamic deployed database situation. A verifiable search mechanism is developed for multi-client setting by combining multi-party searchable encoding that overcomes conspiracy assault between the distributed server and malignant clients. The proposed mechanism achieves desired security objectives and is cost effective in both data processing and repository overhead. In order to fulfil the prerequisites for cryptographic protocols, Yu and his colleagues [101] proposed verifiable secure outsourcing convention. The secret parameters in these secure computation conventions are well protected. It is demonstrated that these protocols are secure against some known assaults on secret data. A new strategy is exhibited for solving differential equations by integral computation protocol. The limitation of these methods is that they cannot be applied for all differential equations.

When the outsourced database undergoes repeated while small modifications, the customer must re-compute and update the encoded version (ciphertext) on the server at all times. For very huge information, it is remarkably expensive for the resource-constrained customer to perform both operations from scratch. Hence, Chen and his colleagues [102] presented the idea of Verifiable Database with Incremental upgrades (Inc-VDB). Inc-VDB mechanism has enormous proficiency gain when the database experiences repeated while little updations. An extensive Inc-VDB system is introduced by using the naive vector commitment and the encode then-additive MAC method of encoding. A solid Inc-VDB mechanism is presented established on the Computational Diffie-Hellman (CDH) presumption. The Inc-VDB mechanism improves public certifiability and also fulfils the property of accountability. The disadvantage is that the server has high computational overhead.

Working on the outsourced spatial information, Ku and his colleagues [103] introduced a procedure that guarantees both security and uprightness for outsourced spatial information. A restricted spatial transformation technique is utilized based on Hilbert trajectories that encodes dimensional information before deploying and guarantees security.

The mechanism is applied for both *k*-closest neighbor inquiries and dimensional range queries. Solutions are also designed to ensure the freshness of outsourced spatial databases. A comprehensive survey on NoSQL and NewSQL information stores is performed by Grolinger and his colleagues [104] with the goal of giving direction to professionals and investigators to select proper repository and recognizes challenges and opportunities in this field. They have addressed on the storage aspect of distributed computing frameworks, specifically, NoSQL and NewSQL information stores.

Kiran and his colleagues [105] introduced a distributed effective video transfer utilizing LAN caching. The scheme reduces Internet bandwidth by caching frequently accessed cloud server streamed video content with in LAN peers, and uses it for subsequent viewing by itself or other peers in same LAN. It improves the quality of media streaming by multiple folds.

By exploiting the computation capability of Graphics Processing Units (GPU), Jo and his colleagues [106]

proposed the mechanism and implementation of a database framework that encodes and decrypts information by utilizing GPU. The proposed component is fundamentally intended for database frameworks that require information encryption and decoding to improve high security level.

The performance of the database framework is higher by offloading computation to GPU. It demonstrates that encryption and decoding on GPU is better compared with that on CPU and the performance gain is relative to the data size. The framework alleviates the use of CPU, and the overall performance of the database framework is enhanced by offloading substantial encoding and decrypting computation to GPU.

Using database model remodelling, a model [107] is introduced for safeguarding cloud clients information security. The database model is altered utilizing cryptographic and comparative secrecy conserving procedures. Uniform access to database documents is guaranteed for the cloud supplier utilizing effective rebuilding of metadata for the recovery of initial database model.

The scheme does not provide cloud customers presence privacy in private cloud environments. Kohler and his colleagues [108] presents a scientific classification of requirements that Confidentiality Preserving Indexing (CPIs) approaches need to fulfil in classification scenarios along with the essential serviceability and the prescribed level of safety against different attacks. The scientific classification's hidden standards provide techniques to survey CPIs, essentially by connecting attack framework to CPI protection attributes.

Doelitzscher and his colleagues [109] have revised cloud-specific security issues and cloud audits. Conventional reviews need to change to address cloud-specific attributes is discussed. The agent based *Security Audit as a Service* construction has been presented as a solution for the recognized issues. The drawback is that the hash function cannot be applied for too big numbers. Krendelev and his colleagues [110] discuss on procedure-conserving encoding mechanism in view of computation coding. Standards of arithmetic coding are examined which form the basis of the algorithm.

Noise behavior approach is executed that builds the algorithm cryptographically substantially and modifications are performed to acquire order protecting hash function. A Verifiable Database (VDB) structure [111] is implemented using vector commitment in view of the binding commitment.

The development is publicly verifiable as well as secure under the Forward Automatic Update (FAU) assault. The mechanism utilizes the bilinear pairing clusters of prime order and hence is additionally effective than Benabbas-Gennaro-Vahlis's mechanism. The public verification has more overhead in this scheme.

A Collaborative Provable Data Possession (CPDP) mechanism [112] is constructed using homomorphic provable acknowledgement and hash token ranking. The security of the mechanism is demonstrated based on multi-prover zero information evidence frameworks. A proficient strategy is presented for choosing optimal specification features to decrease the estimation expenses of users and repository assistance providers. The accomplishment of CPDP mechanism is influenced by the bilinear mapping procedures because of its large complexity. The comparison of schemes for Verifiable Auditing for Outsourced Database is as shown in Table 5.

Table 5: comparison of schemes for verifiable auditing for outsourced database.

Author	Concept	Algorithm	Advantages	Disadvantages
Chen and his colleagues 2014 [102]	Provable Estimation over substantial Database with Cumulative Updates.	Incremental Verifiable Updates (Inc-VDB) Scheme.	Huge efficiency gain, supports public verifiability.	Server has more Computational overhead.
Wang and his colleagues 2015 [98]	Provable Verification for Outsourced Database.	Verifiable Auditing Scheme.	Achieves correctness and completeness of search results.	Does not support dynamic Database.
Yu and his colleagues 2015 [101]	Secure outsourcing of scientific Computations.	Verifiable secure outsourcing protocol.	Parameters in abstract and linear equations are protected.	Methods cannot be applied for all differential equations.
Wang and his colleagues 2016 [100]	Verifiable search for outsourced Database.	Flexible and verifiable search scheme, Verifiable search scheme for multiuser.	Supports efficient data update, cost efficient.	More computation overhead at the client side.
Chen and his colleagues 2015 [111]	Publicly Verifiable Databases with Efficient Updates.	Setup, Query, Verify, Update.	Secure under the Forward Automatic Update (FAU) Assault.	More auditing time.

8. Cloud repository auditing with key-disclosure protection

Existing auditing conventions are all based on the supposition that the client's private key for verifying is certainly protected. Nevertheless, such supposition may not continually be retained, due to the possibility of weak sense of security settings at the customer. If such a private key for verification is disclosed, most of the existing verification conventions would surely become inefficient to work. Therefore, how to deal with the client's private key disclosure for cloud repository verification is really a critical issue. In this section, we review Cloud Repository Auditing with Key-Disclosure Protection.

8.1 System model

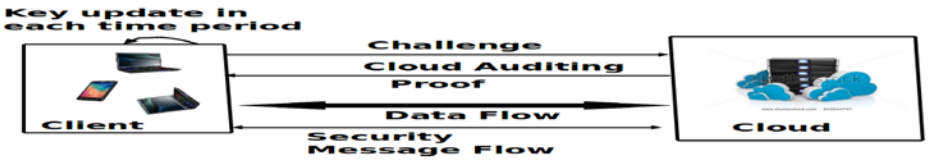

Figure 8: The system architecture of cloud repository auditing.

A verifying framework for safe cloud repository is shown in Fig. 8. The framework includes two entities: the customer (documents proprietor) and the cloud. The customer creates documents and transfers these documents along with relating proofs to the cloud. Every document is additionally isolated into different chunks. The customer can occasionally verify the honesty of his documents saved in cloud. The duration of documents saved in the cloud is separated into (T + 1) time duration (from 0-th to T^{th} time durations). In this framework, the customer upgrades his private keys for distributed repository examining toward the termination of every session, yet public key is dependably unaltered. The cloud is permitted to obtain the customer's private key for distributed repository verification in one assured time duration. It implies the private key disclosure can take place in this scheme.

Yu and his colleagues [113] proposed a verifying convention with key disclosure flexibility. In this convention, the sincerity of the information already saved in cloud is checked regardless of the fact that the customer's present private key for cloud repository verification is revealed. The impairment of the customer's key disclosure in cloud repository verification is addressed. An appraiser system is built to improve the advancing security and the feature of blockless provability. The system model is shown in Fig. 8. Identification based Cloud Information Uprightness verifying convention (ID-CDIC) [114] preserves irregular-sized document blocks and public verification. It is secure under the RSA presumption with considerable public advocators in the random oracle framework. The drawback is that the protocol has little cost of tag generation.

An online/offline signcryption mechanism provides confidentiality and authentication simultaneously, hence considering these benefits, Yan and his colleagues [115] presents a key-disclosure free online/offline signcryption mechanism. In the random oracle framework, the protocol is verified to be alike in contrast to versatile selected ciphertext assaults and existentially unforgeable contrary to selected information assaults. An enhanced protocol is constructed, that needs none of the recipient's public knowledge in the offline stage. The limitation is that the protocol sacrifices performance while needing none of the recipient's public information in the offline stage. Yu and his colleagues [116] proposed an enhanced Remote Data Possession Checking (RDPC) convention by using few methods involving the document name and the chunk series numbers in producing a label. It uses spurious arbitrary behavior to alter the computative signature algorithm. The arbitrary sampling method is used to give probabilistic auditing. The proposed convention is secure and efficient. The drawback is that the protocol has very high tag generation cost.

Software-based attacks (e.g., malware) pose a huge threat to cryptographic software as they can compromise the related cryptographic keys in their totality. Hence, Dodis and his colleagues [117] proposed Key-protected Symmetrical Key scheme. The practicality of the protocol is outlined with an evidence-of approach implemented in the Kernel-based Virtual Machine (KVM) domain. The scheme is built utilizing five algorithms: Key Generation, Device Key-Update, Computer Key-Update, Encryption and Decryption. It mitigates the catastrophe created by repeated attacks contrary to cryptographic software. Limitation of the scheme is that it has more communication cost due to the Device Key-Update module to the Computer Key-Update module.

Considering batch applications and mitigating the effect of key disclosure, Lin and his colleagues [118] presents an identification based key-isolated multi-signature mechanism. Every customer can intermittently refresh his

secret key and at the same time the public key remains unaltered. The mechanism has the features of absolute time durations and arbitrary approach key-restores. Performance analysis shows that it has better proficiency and demonstrates its protection of unforgeability in contrast to empirical fabrication under versatile chosen information assaults in the random oracle framework. A problem-free, steady rate and task established Software as a Service cloud framework [119] is discussed along with the trustworthiness checking schemes, with specific target convex optimization issue. In the security model, the inherent structures of the streamlining issues are utilized to accomplish productive integrity certification. The suggested configuration gives generous data processing preservations on the customer side and presents negligible cost on the cloud side. The system guarantees strong honesty confirmation with immense proficiency on both the customer and the cloud sides. The protocol introduces marginal overhead on the customer side.

To ensure the information repository security in distributed computing, Sookhak and his colleagues [120] presents an effective remote information examination plan. The divide and conquer table permits the examiner to review the huge scale information and accomplish a substantial number of insert and erase operations with least calculation cost on the examiner and server. The scheme is not applicable for distributed servers. The advantage of the protocol is that it incurs least data processing overhead on the verifier and server. The scheme does not perform optimized number of divisions in the divide and conquer table. Forward-secure signatures diminish the damage of key exposure, hence Yu and his colleagues [121] presents a mechanism to incorporate forward-secure and personality established primitives into untrusted restore situations. The proposed plan is demonstrated to be forward-protected and update protected in the random oracle framework supporting the CDH supposition. The limitation is that the key update time and verifying time have logarithmic complexities.

Zhang and his colleagues [122] proposed a Safe Certificateless Public Sincerity Verification (SCLPV) mechanism. The SCLPV concurrently supports certificateless public confirmation and protection against vindictive evaluators to confirm the trustworthiness of deployed information in Cyber-Physical-Social Framework (CPSS). The transmission overhead bounded by the evaluator and the distributed server of the SCLPV is independent of the volume of the refined information, the examiner need not manage certificates. TPA cannot concurrently manage numerous confirmation jobs from distinct CPSS customers and diverse distributed servers. In order to preserve the confidentiality, honesty, and authenticity of the information, Zhou and his colleagues [123] presents an Efficient and Secure Data Repairing (ESDR) paradigm. ESDR is constructed by utilizing regenerating code and certificateless signcryption technique. The signcrypt preprocessing advances security and proficiency remarkably. The scheme is feasible and productive to secure information repairing in distributed storage. The disadvantage of the scheme is that the data stored on every other data center is slightly more than the size of the original data.

Liu and his colleagues [124] suggests a new two-element information security preservation scheme for distributed repository framework, in which an information owner is permitted to encode the information with learning of the identification of a recipient just in the time the recipient is prescribed to employ both his/her private key and a safety gadget to fetch the information. The proposed mechanism upgrades the privacy of the information, as well as handles the repudiability of the gadget. The drawback of the protocol is that it does not support multiple revocability for device and revocability for identity factor. Wang and his colleagues [125]

designed a framework of Identity-Based Remote Data Possession Checking (ID-RDPC) conventions. It eliminates certification administration and confirmation. IDRDPC convention surpasses current RDPC conventions in the PKI context in terms of estimation and intelligence.

An unique solution of routing stereoscopic 3D video stream encoded using H.264/MVC algorithm [126] is discussed for multiple network paths using multiple RTP sessions.

The scheme transmits 3D video without any latency or jitter. The comparison of schemes for Cloud Repository Auditing with Key-Disclosure Protection is shown in Table 6.

Table 6: comparison of schemes for cloud repository auditing with key-disclosure protection

Authors	**Concept**	**Algorithm**	**Advantages**	**Disadvantages**
Sookhak *et al.,* 2014 [120]	Dynamic remote data auditing in computational clouds.	Remote data auditing scheme.	Low computation overhead on the client, server and verifier.	Not applicable for distributed cloud servers.
Xu and his colleagues 2014 [119]	Software as a service cloud framework along with the honesty certification.	Integrity verification Scheme.	Low computation cost, strong integrity assurance.	High overhead on client side.
Zhang and his colleagues 2015 [122]	Certificateless public authentication for cloud positioned cyber-tangible public schemes .	Safe Certificateless Public Sincerity Verification (SCLPV) scheme.	Supports certificateless public verification and resistance against malicious auditors.	Cannot handle multiple verification tasks.
Zhou and his colleagues 2016 [123]	Dynamic and safe data repairing model in cloud repository.	Efficient and Secure Data Repairing (ESDR) scheme.	Secures data repairing, data availability.	High communication cost overhead.
Yu and his colleagues 2016 [113]	Cloud Repository Verification with provable deploying of Key Updates.	SysSetup, EkeyUpdate, VerESK, DecESK, ProofGen, ProofVerify.	Minimal key update burden on the client.	High overhead to accomplish extra key exposure resilience.
Yu and his colleagues 2016 [114]	Cloud data integrity checking.	Setup, Extract, TagGen, Challenge, ProofGen and ProofVerify.	Supports variable sized file blocks and public verification.	Little cost of tag generation.
Yu and his colleagues 2015 [116]	Remote information possession checking with enhanced security for distributed repository.	Setup, TagBlock, Challenge, ProofGen and ProofVerify.	Secure against replay attack and deletion attack	Very high tag generation cost.
Yu and his colleagues 2016 [121]	Integrating forward-secure and identity-based primitives into standard applications.	Key, Extract, Update, Sign, Verify.	Proven to be forward-secure and update-secure.	Key update time and verifying time have logarithmic complexities.

9. Public verification for reconstructing-code-based cloud repository

To preserve deployed information in cloud repository contrary to exploitation, adding fault tolerance to distributed repository together with information honesty verifying and failure reparation becomes critical. There are various redundancy mechanisms, such as replication, erasure codes, and reconstructing codes. Reconstructing codes excellently trade the bandwidth required for restoration of failed node with the volume of information saved per node of the network. Reconstructing codes have decreased restoration bandwidth while administering fault tolerance. We review the cloud storage based on regenerating codes in this section.

9.1 System Model

The auditing framework for Reconstructing-Code-based distributed repository is shown in Fig. 9, that consists of four objects: (i) The data owner, who have a huge number of information documents to be saved in the cloud; (ii) The cloud, provides repository services and have noteworthy data processing assets; (iii) The public verifier, has ability and proficiency to accomplish public verification on the coded information in the cloud; (iv) The public verifier is trustworthy and its review outcome is impartial for information proprietors and distributed servers; An intermediary specialist, who is semi-trusted and follows up in support of the information possessor to repair proofs and data chunks on the collapsed servers throughout the restoration process.

Liu and his colleagues [127] introduced a public verifying mechanism for the reconstructing-code-based cloud repository. To take care of the reconstruction problem of fizzled certifications in the nonappearance of information proprietors, an intermediary is introduced, that is required to repair the certifications, into the customary public verifying model. A public irrefutable certification is designed, which is produced by two or three keys and can be repaired employing partial keys. This mechanism can completely discharge information proprietors from on-line accountability. In addition, the cipher coefficients are randomized with a pseudorandom behaviour to conserve information confidentiality. The system model is shown in Fig. 9.

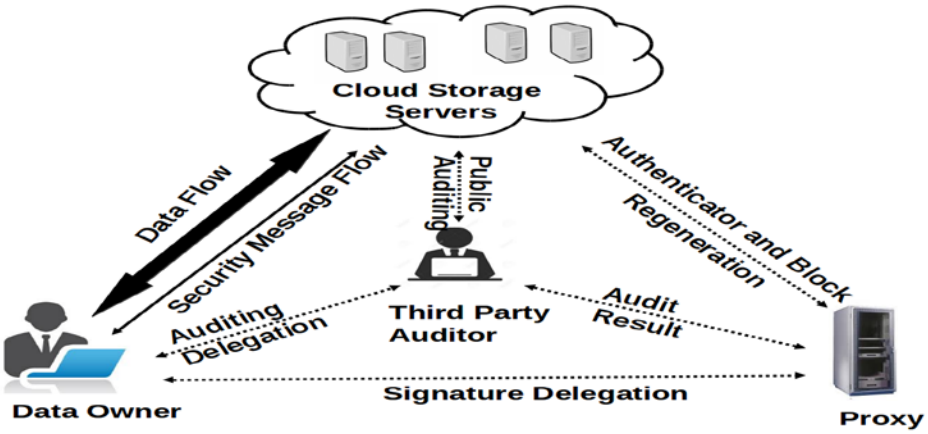

Figure 9: The system model.

A comprehensive review [128] is performed on the analysis of the current results of coding methods for cloud

storage frameworks. These coding systems are exhibited into two classes, specifically reconstructing codes and regionally replacement codes. These codes satisfy the prerequisites of distributed repository along two distinct axis: optimizing transmission capacity and I/O cost. Erasure coding, is able to tolerate the disk failures, and has better storage efficiency. Chen and his colleagues [129] outlined Functional Minimum-Storage Reconstructing-Data Integrity Protection (FMSR-DIP) codes, which empowers trustworthiness security, adaptation to internal failure, and conducive restoration for cloud storage. Data Integrity Protection (DIP) is planned in a versatile Byzantine adversarial scheme, and authorizes the customer to practically confirm the honesty of arbitrary subsets of deployed data against general or malicious dishonesty. The drawback of the scheme is that storage overhead is increased due to appending the MACs of all blocks to the metadata.

Utilizing the idea of the Fractional Repetition (FR) code, Yu and his colleagues [130] proposed the Irregular Fractional Repetition (IFR) code. The IFR code reduces the restore transfer speed and the disk access transfer capacity at the same time, with no computational cost. The MDS-IFR code and the recovery sets are intended to minimize the framework repair cost. Maximum Distance Separable-Irregular Fractional Repetition (MDS-IFR) code affords little restore rate at the loss of high depository overhead. To ensure the straightforwardness of distributed storage frameworks, Corena and Ohtsuki [131] presents a productive framework utilizing network-coding-based regenerating codes. It is additionally conceivable to confirm in polynomial period that the encrypted segments can recreate the primary document. As far as the exhibited limited-benefit vs unlimited benefit PORs, the limited-benefit development has improved cost over the unlimited-benefit one, it likewise causes in low cost per challenge. The drawback of the scheme is that it has large repository overhead.

Network-Coding-based Storage system (NCCloud) [132], addresses the soundness of cloud reinforcement storage. NCCloud is fault tolerant in repository; additionally, permits cost-effective reconstruction when a cloud forever fails. NCCloud constructs an efficient version of the Functional Minimum-Storage Reconstructing (FMSR) codes. The drawback is that the scheme does not support effective restoration of simultaneous node failures and degraded reads are not considered. Yang and his colleagues [133] exhibited a piggybacking plan that provides Minimum-Storage Regenerating (MSR) codes with practically ideal restore transmission capacity of parity correspondence hubs. MSR codes with uniform download are built in the course of hub reconstruction. Piggybacking is utilized to accomplish little normal restore data transfer capacity of correspondence hubs of MSR codes. The limitation is that the scheme has additional complexity and the receiver can jam the service if it has nothing to send.

Silberstein and his colleagues [134] introduced concatenated coding mechanism for cloud storage framework. The mechanism uses rank-metric codes, specifically, Gabidulin codes. In the encoding procedure, MDS ideal repair array codes are utilized. This development guarantees flexibility against static adversarial mistakes. The scheme does not support optimal error correcting Minimum Storage Regenerating-Locally Repairable Codes (MSR-LRCs) and also for optimal error-correcting Minimum Bandwidth Regenerating-Locally Repairable Codes (MBR-LRCs). Huang and Udaya [135] discusses about the secrecy limit of Minimum Storage Cooperative Regenerating Codes (MSCR). A stable MSCR codes are presented where the repair information is independent of the repair groups and the sets of assistant hubs. The MSCR codes has preferable secrecy limit over the original one. The disadvantage is that the characterization of secrecy capacity of MSCR codes is not

considered.

Many existing verifying mechanisms always assume TPA is trustworthy and independent. Huang and his colleagues [136] reviews the issue what if certain public verifiers are semi-trusted or even possibly malevolent in some situations, and hence they proposed a powerful and trivial convention where client himself processes the concluding confirmation job and TPA assumes the responsibility of preparing evidence and combining inputs. Multi-TPAs are embraced to implement the equivalent estimation review and allows client to verify the last confirmation condition for anticipating frame attack and conspire attack, separately. The performance analysis demonstrates that the mechanism is secure and lightweight under the supposition that TPA is malevolent in a few circumstances. Raghavendra and his colleagues [137] have performed survey on keyword searches that are analyzed on the basis of miscellaneous criterion like security, adeptness, scalability, query efficiency, architecture and performance. They also examined on numerous aspects of information sharing on basis of customer repudiation, competency, encoding methods, identity privacy and key distribution.

Chen and his colleagues [138] discussed on the attributes of restoration matrices for MSR codes with correct repair. The properties of MSR codes are useful in building MSR codes with least restoration disk I/O and in addition in creating lower limits for the restoration disk I/O. Inquiring MSR codes with restore-by-exchange property has not been addressed. A provable information exchange mechanism [139], accomplish the information uprightness, accessibility and secure deletion in data movement between two clouds. In particular, by combining the Provable Data Possession (PDP) and provable information deletion, the mechanism permits the cloud to create a succinct proof to convince the information proprietor that the outsourced information are transferred to the server with no debasement. Additionally, it empowers the cloud from which the information is relocated to demonstrate the deletion of the exchanged data. Provable information deletion strategy is built for taking care of secure information erasure after the outsourced information is migrated.

Kiran and his colleagues [140] presents cloud enabled 3D Tablet model for medical applications. They have discussed the hardware and software architecture for 3D Tablet design. They have also explored how combining the cloud capabilities into the Tablet can enhance the accomplishment of the mobile cloud computing and provide profitable services. The comparison of schemes for Public Verification for Reconstructing-Code-Based Cloud Repository is shown in Table 7.

10. Future directions

In this section, new future research directions in the context of Data Auditing and Security in Cloud Computing are presented as shown in Fig. 10.

Group Client Repudiation: Various efficient public honesty verification with group client repudiation schemes have been developed. But the proposed schemes have their own limitations. Security is of concern in the group clients' information when a semi-trusted distributed server co-operates with the revoked client. Therefore, it is necessary to develop unique and secure information auditing with efficient client repudiation mechanisms that provide integrity and confidentiality of shared information and is collusion resistant. Group signatures schemes

have to be constructed that preserves privacy. Auditing mechanisms for cloud information sharing services need to be designed that accomplishes reliability, information recovery and error detection. Collusion resistant proxy resignature approach must be implemented that also supports public verification. In some of the existing schemes it is found that the revoked customer can access the outsourced information with the attributes that he holds. Hence there is a need to implement the auditing mechanisms that are totally secure from the revoked user. Further researchers must develop data auditing mechanisms that support data dynamics and has low computation, communication, and storage costs.

Table 7: comparison of schemes for public verification for reconstructing-code-based cloud repository

Authors	**Concept**	**Algorithm**	**Advantages**	**Disadvantages**
Chen and his colleagues 2014 [129]	Data integrity protection in reconstructing-code-based distributed repository.	Functional Minimum-Storage Reconstructing-Data Integrity Protection (FMSR-DIP) codes	Integrity protection, fault tolerant, and efficient recovery.	Transmission time is more during upload process.
Yu and his colleagues 2014 [130]	Irregular fractional repetition code optimization for heterogeneous cloud storage.	Maximum Distance Separable-Irregular Fractional Repetition (MDS-IFR) code	Minimizes repair bandwidth and the disk access bandwidth.	High storage overhead.
Liu and his colleagues 2015 [127]	Secrecy-conserving public verification for Reconstructing-Code-Based Cloud Repository.	Setup, Audit, Repair.	Clients relieved from online burden.	High bandwidth cost.
Yang and his colleagues 2015 [133]	Piggybacking design for minimum storage regenerating codes.	Model of Minimum-Storage Regenerating (MSR) codes.	Small average repair Bandwidth.	For repair of a failed parity node, MSR codes have to download all the data.
Corena and Ohtsuki, 2014 [131]	Pollution-Free Reconstructing Codes with Fast Reconstruction Verification.	Unbounded-Use Proof of Retreivability (POR) and bounded-use POR.	Bounded use has better Overhead.	Large storage overhead.
Chen and his colleagues 2014 [132]	An agent-based repository system for fault-tolerant multiple-cloud repository.	Network-Coding-based Cloud storage (NCCloud) Scheme.	Fault tolerant in repository, cost-effective reconstruction.	Does not support effective restoration of simultaneous node failures.
Silberstein and his colleagues 2015 [134]	Enabling error resilience in distributed storage.	Concatenated coding mechanism using rank metric codes.	Ensures resilience against static adversarial.	Does not support optimal error correcting codes.
Huang and Udaya, 2015 [135]	Security Concerns in Minimum Storage Cooperative Regenerating Codes.	Stable MSCR codes.	Better secrecy capacity.	Characterization of secrecy capacity of MSCR codes is not considered.

Collaborative Information in Cloud: Sharing information among diversified customers is an appealing feature that inspires cloud repository. The sincerity of cloud information is susceptible to apprehension due to the hardware/software failures and human mistakes. Various mechanisms have been constructed to allow information owner and TPAs to effectively verify cloud information. These mechanisms have their own limitations and there is a need to design an effective public audit schemes with the proficiency of sustaining identity secrecy of customers and supporting traceability. Re-encryption keys in few of the existing mechanisms have high overhead and has increased time complexity for key updates. To enhance the remote information checking, mechanisms need to be implemented that support dynamic datasets, decodability, low computation and communication costs. There is a compelling need to construct more adaptable and efficient information examination procedures without trading off on security of the cloud.

Data Deduplication in Cloud: Deduplication is an approach where the server maintains only a distinct copy of every document, regardless of how many customers have asked to save that document such that the disk space

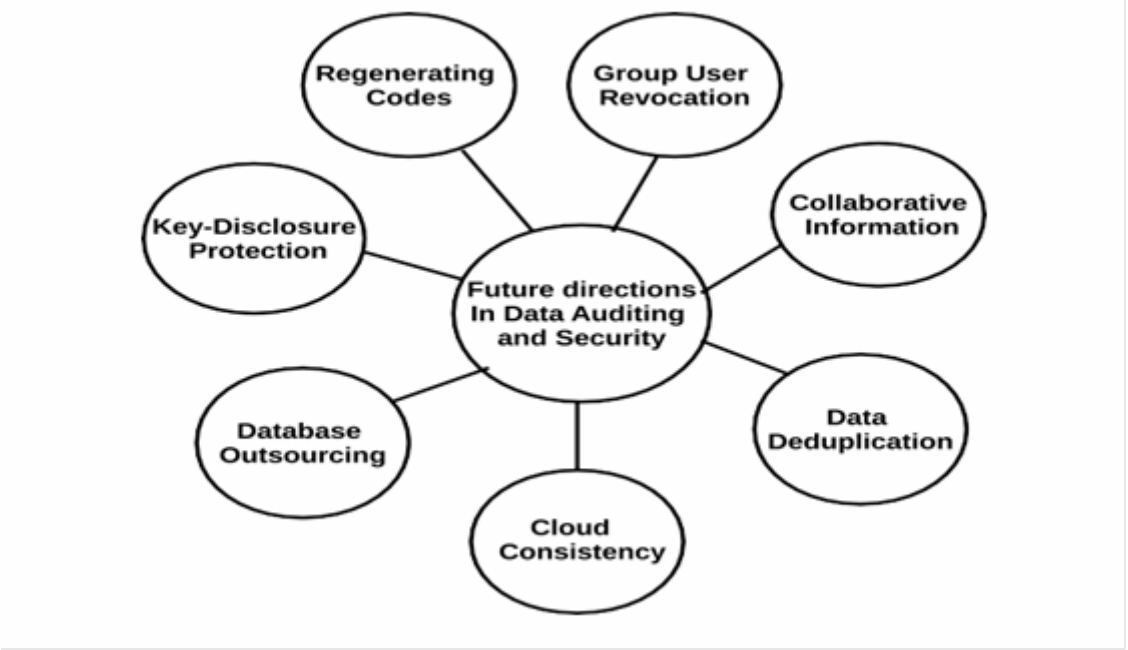

Figure 10: Future directions for Data Auditing and Security.

of distributed servers and network bandwidth are saved. It is necessary to design secure and efficient deduplication techniques that reduces computational cost, communication cost, storage cost, and encoding/decoding overhead. It is suggested to develop customer revocable deduplication. In multi-server supported deduplication there is a need to design a scheme that reduces the cost of record uploading. Everlasting repository maintenance is required for digital information storage.

Cloud Consistency: Mandated by the Consistency, Availability and Partition tolerance (CAP) principle, many cloud service providers (e.g., Amazon S3) only guarantee weak consistency, such as eventual consistency, for

performance and high availability, where a customer can read stale information over an epoch of time. But interactive applications needs stronger consistency assurances as various applications have different consistency requirements. For example, mail services need monotonic- read consistency and read-your-write consistency, but social network services need causal consistency. There is a necessity to design consistency auditing protocol that addresses *k*-atomicity verification problem while Heuristic Auditing Strategy can be improved by decreasing threshold value.

Database Outsourcing: The concept of database deploying allows the information proprietor to delegate the database administration to a Cloud Service Provider (CSP) that supports numerous database services to various customers. Research work is required to develop an efficient verifiable database outsourcing mechanism that addresses the security challenges such as secrecy of outsourced information and verifiability of results. Cloud customers privacy is not preserved in private cloud environment. There is a requirement to develop the mechanism that uses hash functions for big numbers and also supports differential equations.

Key-Disclosure Protection: Existing auditing conventions are all based on the supposition that the client's private key for verifying is certainly protected. Nevertheless, such supposition may not continually be retained, due to the possibility of weak sense of security settings at the customer. If such a private key for verification is disclosed, most of the existing verification conventions would surely become inefficient to work. Therefore, it is essential to establish a unique and safe scheme that deal with the client's private key disclosure for cloud repository verification. There is a need to construct a protocol that has low tag generation cost, low key updating cost and verifying cost. Few mechanisms do not support multiple revocability for devices and revocability for identity factor. The size of the information stored on every other data center is slightly more than the size of the original information.

Regenerating Codes: To preserve deployed information in cloud repository contrary to exploitation, adding fault tolerance to distributed repository together with information honesty verifying and failure reparation becomes critical. There are various redundancy mechanisms, such as replication, erasure codes, and, reconstructing codes. Reconstructing codes excellently trade the bandwidth required for restoration of failed node with the volume of information saved per node of the network. Reconstructing codes have decreased restoration bandwidth while administering fault tolerance. It is necessary to design an efficient scheme that supports effective restoration of simultaneous node failures and consider the degraded reads. Further, it is required to design protocols that support optimal error correcting codes that must consider the characterization of secrecy capacity of Minimum Storage Cooperative Regenerating (MSCR) codes. Inquiring Minimum Storage Regenerating (MSR) codes with restore-by-exchange property has not been addressed.

10. Conclusions

This paper presents an extensive survey on data auditing and security in distributed computing. With data storage and shared data, auditor performs efficient auditing with group user revocation. Existing mechanisms provide efficient integrity auditing of shared data, user revocation and supports batch auditing. Mechanisms need to be implemented to reduce the overhead introduced by a huge number of customers in the cluster. In

public auditing for collaborative information, the auditor performs efficient auditing and also preserves confidentiality of the shared information saved in cloud. The schemes preserve the privacy of the identity of the customer and supports batch auditing. The disadvantage is that they do not justify information freshness and not support traceability.

In secure verification and deduplicating information in cloud, secure systems are implemented to achieve data deduplication and verifier achieves efficient integrity auditing on the data. The advantages of the protocol are secure deduplication on encrypted information is achieved and are protected from internal and external attacks. The drawback is that the schemes do not support user revocable deduplication. In auditing cloud consistency, the clients perform auditing of cloud storage consistency to verify whether the cloud storage service is consistent or not. Efficient auditing of cloud consistency is achieved and the users can precisely choose the cloud service provider. Efficient algorithms need to be designed that improve the storage and computation overhead of the existing algorithms.

In verifiable outsourced database, Cloud Service Provider (CSPs) provides various database services and also manages the database saved in it. Here clients perform provable auditing for deployed database. The mechanisms accomplish accuracy and integrity of search results. Efficient protocols need to be designed that support dynamic database and improves computation cost. Distributed repository verifying protocols with builtin key disclosure resilience is designed that reduces the damage of the customer's secret key disclosure. The algorithms support forward security and property of blockless verifiability which incurs high overhead to accomplish extra key disclosure resilience. Public verification for reconstructing code based distributed repository achieves protection of stored data against exploitation and adds fault tolerance to distributed repository. The mechanism relieves clients from online burden. There is a need to design protocols that support optimal error correcting codes.

References

[1] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, "Nist Cloud Computing Reference Architecture," NIST Special Publication, vol. 500, no. 2011, pp. 1–28, 2011.

[2] A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "Above the Clouds: A Berkeley View of Cloud Computing," Department of Electrical Engg. And Computer Sciences, University of California, vol. 28, no. 13, pp. 1–42, 2009.

[3] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility," Future Generation Computer Systems, vol. 25, no. 6, pp. 599–616, 2009.

[4] M. Blum, W. Evans, P. Gemmell, S. Kannan, and M. Naor, "Checking the Correctness of Memories," Algorithmica, vol. 12, no. 2-3, pp. 225–244, 1994.

[5] C. C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession,"

ACM Transactions on Information and System Security (TISSEC), vol. 17, no. 4, pp. 213–222, 2015.

[6] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," in Proceedings of the 4th International Conference on Security and Privacy in Communication Networks, pp. 1–9, ACM, 2008.

[7] A. Juels and B. S. Kaliski Jr, "PORs: Proofs of Retrievability for Large Files," in Proceedings of the 14th ACM Conference of Computer and Communications Security, pp. 584–597, 2007.

[8] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Journal of Cryptology, vol. 26, no. 3, pp. 442–483, 2013.

[9] G. Yamamoto, S. Oda, and K. Aoki, "Fast Integrity for Large Data," in Proceedings of ECRYPT Workshop Software Performance Enhancement for Encryption and Decryption, pp. 21–32, 2007.

[10] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, pp. 598–609, 2007.

[11] Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231–2244, 2012.

[12] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in INFOCOM Proceedings, pp. 1–9, IEEE, 2010.

[13] K. Yang and X. Jia, "Data Storage Auditing Service in Cloud Computing: Challenges, Methods and Opportunities," World Wide Web, vol. 15, no. 4, pp. 409–428, 2012.

[14] T. Jiang, X. Chen, and J. Ma, "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation," IEEE Transactions on Computers, vol. 65, no. 8, pp. 2363–2373, 2016.

[15] B. Wang, B. Li, and H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," IEEE Transactions on Services Computing,, vol. 8, no. 1, pp. 92–106, 2015.

[16] J. Yuan and S. Yu, "Efficient Public Integrity Checking for Cloud Data Sharing with Multi-User Modification," in INFOCOM Proceedings, pp. 2121–2129, IEEE, 2014.

[17] S. Raghavendra, C. M. Geeta, R. Buyya, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik, "MSIGT: Most Significant Index Generation Technique for Cloud Environment," in Proceedings of the Annual IEEE India Conference (INDICON), pp. 1–6, 2015.

[18] S. Benabbas, R. Gennaro, and Y. Vahlis, "Verifiable Delegation of Computation Over Large

Datasets," in Advances in Cryptology–CRYPTO, pp. 111–131, Springer, 2011.

[19] D. Catalano and D. Fiore, "Vector Commitments and their Applications," in Public-Key Cryptography–PKC, pp. 55–72, Springer, 2013.

[20] M. Backes, D. Fiore, and R. M. Reischuk, "Verifiable Delegation of Computation on Outsourced Data," in Proceedings of ACM SIGSAC Conference on Computer & Communications Security,, pp. 863–874, 2013.

[21] B. Bruhadeshwar and S. S. Kulkarni, "Balancing Revocation and Storage Trade-offs in Secure Group Communication," IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 1, pp. 58–73, 2011.

[22] S. Raghavendra, S. Girish, C. M. Geeta, R. Buyya, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik, "IGSK: Index Generation on Split Keyword for Search over Cloud Data," in Proceedings of International Conference on Computing and Network Communications (CoCoNet), pp. 374–380, 2015.

[23] J. Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity-Based Encryption with Outsourced Revocation in Cloud Computing," IEEE Transactions on Computers, vol. 64, no. 2, pp. 425–437, 2015.

[24] Y. Zhu, H.-X. Hu, G.-J. Ahn, H.-X. Wang, and S.-B. Wang, "Provably Secure Role-Based Encryption with Revocation Mechanism," Journal of Computer Science and Technology, vol. 26, no. 4, pp. 697–710, 2011.

[25] Z. Hao, S. Zhong, and N. Yu, "A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability," IEEE Transactions on Knowledge and Data Engineering, vol. 23, no. 9, pp. 1432–1437, 2011.

[26] C. Li, Y. Chen, P. Tan, and G. Yang, "Towards Comprehensive Provable Data Possession in Cloud Computing," Wuhan University Journal of Natural Sciences, vol. 18, no. 3, pp. 265–271, 2013.

[27] J. Ni, Y. Yu, Y. Mu, and Q. Xia, "On the Security of an Efficient Dynamic Auditing Protocol in Cloud Storage," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 10, pp. 2760–2761, 2014.

[28] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 9, pp. 1717–1726, 2013.

[29] B. Wang, H. Li, X. Liu, F. Li, and X. Li, "Efficient Public Verification on the Integrity of Multi-Owner Data in the Cloud," Journal of Communications and Networks, vol. 16, no. 6, pp. 592–599, 2014.

[30] K. Xue and P. Hong, "A Dynamic Secure Group Sharing Framework In Public Cloud Computing,"

IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 459–470, 2014.

[31] Y. Luo, M. Xu, S. Fu, D. Wang, and J. Deng, "Efficient Integrity Auditing for Shared Data in the Cloud with Secure User Revocation," in Trustcom/BigDataSE/ISPA, IEEE, vol. 1, pp. 434–442, 2015.

[32] X. Dong, J. Yu, Y. Zhu, Y. Chen, Y. Luo, and M. Li, "SECO: Secure and Scalable Data Collaboration Services in Cloud Computing," Computers & Security, vol. 50, pp. 91–105, 2015.

[33] Q. Huang, Z. Ma, Y. Yang, J. Fu, and X. Niu, "EABDS: Attribute- Based Secure Data Sharing with Efficient Revocation in Cloud Computing," Chinese Journal of Electronics, vol. 24, no. 4, pp. 862–868, 2015.

[34] S. Park, K. Lee, and D. H. Lee, "New Constructions of Revocable Identity-Based Encryption from Multilinear Maps," IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1564–1577, 2015.

[35] J. Zhang and X. Zhao, "Efficient Chameleon Hashing-Based Privacy-Preserving Auditing in Cloud Storage," Cluster Computing, vol. 19, no. 1, pp. 47–56, 2016.

[36] J. Y. Hwang, L. Chen, H. S. Cho, and D. Nyang, "Short Dynamic Group Signature Scheme Supporting Controllable Linkability," IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1109–1124, 2015.

[37] J. Hong, K. Xue, and W. Li, "Comments on DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems/ Security Analysis of Attribute Revocation in Multiauthority Data Access Control for Cloud Storage Systems," IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1315–1317, 2015.

[38] J. Yuan and S. Yu, "Public Integrity Auditing for Dynamic Data Sharing with Multiuser Modification," IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1717–1726, 2015.

[39] J. Li, L. Zhang, J. K. Liu, H. Qian, and Z. Dong, "Privacy-Preserving Public Auditing Protocol for Low-Performance End Devices in Cloud," IEEE Transactions on Information Forensics and Security, vol. 11, no. 11, pp. 2572–2583, 2016.

[40] J. Hur and D. K. Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214–1221, 2011.

[41] X. Dong, J. Yu, Y. Luo, Y. Chen, G. Xue, and M. Li, "Achieving an Effective, Scalable and Privacy-Preserving Data Sharing Service in Cloud Computing," Computers & Security, vol. 42, pp. 151–164, 2014.

[42] Q. Wu, "A Generic Construction of Ciphertext-Policy Attribute-Based Encryption Supporting Attribute Revocation," China Communications, vol. 11, no. 13, pp. 93–100, 2014.

[43] M. Reddy, S. H. Manjula, and K. R. Venugopal, "Secure Data Sharing in Cloud Computing: A Comprehensive Review," International Journal of Computer (IJC), vol. 25, no. 1, pp. 80–115, 2017.

[44] Y. Lu and J. Li, "A Pairing-Free Certificate-Based Proxy Re-Encryption Scheme for Secure Data Sharing in Public Clouds," Future Generation Computer Systems, vol. 62, pp. 140–147, 2016.

[45] G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, "Enabling Public Auditing for Shared Data in Cloud Storage Supporting Identity Privacy and Traceability," Journal of Systems and Software, vol. 113, pp. 130–139, 2016.

[46] Z. Zhu and R. Jiang, "A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 1, pp. 40–50, 2016.

[47] K. Selvamani and S. Jayanthi, "A Review on Cloud Data Security and its Mitigation Techniques," Procedia Computer Science, vol. 48, pp. 347–352, 2015.

[48] N. Garg and S. Bawa, "Comparative Analysis of Cloud Data Integrity Auditing Protocols," Journal of Network and Computer Applications, vol. 66, pp. 17–32, 2016.

[49] X. Xu, J. Zhou, X. Wang, and Y. Zhang, "Multi-Authority Proxy Reencryption Based on CPABE for Cloud Storage Systems," Journal of Systems Engineering and Electronics, vol. 27, no. 1, pp. 211–223, 2016.

[50] S. Raghavendra, P. A. Doddabasappa, C. M. Geeta, R. Buyya, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik, "Secure Multi-Keyword Search and Multi-User Access Control over an Encrypted Cloud Data," International Journal of Information Processing, vol. 10, no. 2, pp. 51–61, 2016.

[51] S. More and S. Chaudhari, "Third Party Public Auditing Scheme for Cloud Storage," Procedia Computer Science, vol. 79, pp. 69–76, 2016.

[52] H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Transactions on Services Computing, vol. 6, no. 4, pp. 551–559, 2013.

[53] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, "Lt Codes-Based Secure and Reliable Cloud Storage Service," in INFOCOM Proceedings IEEE, pp. 693–701, 2012.

[54] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-Based Distributed Storage Systems," in Proceedings of ACM workshop on Cloud Computing Security Workshop, pp. 31–42, 2010.

[55] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud,"IEEE Transactions on Cloud Computing, vol. 2, no. 1, pp. 43–56, 2014.

[56] K. R. Venugopal, K. G. Srinivasa, and L. M. Patnaik, "Soft Computing for Data Mining Applications," Springer, 2009.

[57] H. Wang, "Privacy-Preserving Data Sharing in Cloud Computing," Journal of Computer Science and Technology, vol. 25, no. 3, pp. 401– 414, 2010. [58] R. K. Ko, B. S. Lee, and S. Pearson, "Towards Achieving Accountability, Auditability and Trust in Cloud Computing," in International Conference on Advances in Computing and Communications, pp. 432– 444, Springer, 2011.

[58] R. K. Ko, B. S. Lee, and S. Pearson, "Towards Achieving Accountability, Auditability and Trust in Cloud Computing," in International Conference on Advances in Computing and Communications, pp. 432–444, Springer, 2011.

[59] M. Van Dijk, A. Juels, A. Oprea, R. L. Rivest, E. Stefanov, and N. Triandopoulos, "Hourglass Schemes: How to Prove that Cloud Files are Encrypted," in Proceedings of ACM Conference on Computer and Communications Security, pp. 265–280, 2012.

[60] L. Xu, X. Wu, and X. Zhang, "CL-PRE: A Certificateless Proxy Reencryption Scheme for Secure Data Sharing with Public Cloud," in Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, pp. 87–88, 2012.

[61] Z. Qin, S. Wu, and H. Xiong, "Strongly Secure and Cost-Effective Certificateless Proxy Re-Encryption Scheme for Data Sharing in Cloud Computing," in Proceedings of the International Conference on Big Data Computing and Communications, pp. 205–216, Springer, 2015.

[62] S. R. Tate, R. Vishwanathan, and L. Everhart, "Multi-User Dynamic Proofs of Data Possession using Trusted Hardware," in Proceedings of the Third ACM Conference on Data and Application Security andPrivacy, pp. 353–364, 2013.

[63] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182–1191, 2013.

[64] H. Rasheed, "Data and Infrastructure Security Auditing in Cloud Computing Environments," International Journal of Information Management, vol. 34, no. 3, pp. 364–368, 2014.

[65] Q. Liu, G. Wang, and J. Wu, "Time-Based Proxy Re-Encryption Scheme for Secure Data Sharing in a Cloud Environment," Information Sciences, vol. 258, pp. 355–370, 2014.

[66] Y. Yu, L. Niu, G. Yang, Y. Mu, and W. Susilo, "On the Security of Auditing Mechanisms for Secure

Cloud Storage," Future Generation Computer Systems, vol. 30, no. 1, pp. 127–132, 2014.

[67] A. Abbas and S. U. Khan, "A Review on the State-of-the-Art Privacy-Preserving Approaches in the E-Health Clouds," IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 4, pp. 1431–1441, 2014.

[68] G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, "Enabling Public Auditing for Shared Data in Cloud Storage Supporting Identity Privacy and Traceability," Journal of Systems and Software, vol. 113, pp. 130– 139, 2016.

[69] A. P. Singh and S. K. Pasupuleti, "Optimized Public Auditing and Data Dynamics for Data Storage Security in Cloud Computing," Procedia Computer Science, vol. 93, pp. 751–759, 2016.

[70] Y. Li, Y. Yu, B. Yang, G. Min, and H. Wu, "Privacy Preserving Cloud Data Auditing with Efficient Key Update," Future Generation Computer Systems, 2016.

[71] H. Cui, R. H. Deng, Y. Li, and B. Qin, "Server-Aided Revocable Attribute-Based Encryption," in Proceedings of the European Symposium on Research in Computer Security, pp. 570–587, Springer, 2016.

[72] S. Tan and Y. Jia, "NaEPASC: A Novel and Efficient Public Auditing Scheme for Cloud Data," Journal of Zhejiang University Science, vol. 15, no. 9, pp. 794–804, 2014.

[73] S. Raghavendra, C. M. Geeta, K. Shaila, R. Buyya, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik, "MSSS: Most Significant Single- Keyword Search over Encrypted Cloud Data," in Proceedings of the 6th Annual International Conference on ICT: BigData, Cloud and Security, 1–6, 2015.

[74] J. Li, J. Li, D. Xie, and Z. Cai, "Secure Auditing and Deduplicating Data in Cloud," IEEE Transactions on Computers, vol. 65, no. 8, pp. 2386–2396, 2016.

[75] J. Li, Y. K. Li, X. Chen, P. P. Lee, and W. Lou, "A Hybrid Cloud Approach for Secure Authorized Deduplication," IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 5, pp. 1206–1216, 2015.

[76] J. Li, X. Chen, X. Huang, S. Tang, Y. Xiang, M. M. Hassan, and A. Alelaiwi, "Secure Distributed Deduplication Systems with Improved Reliability," IEEE Transactions on Computers, vol. 64, no. 12, pp. 3569–3579, 2015.

[77] J. Wang and X. Chen, "Efficient and Secure Storage for Outsourced Data: A Survey," Data Science and Engineering, vol. 1, no. 3, pp. 178–188, 2016.

[78] J. Hur, D. Koo, Y. Shin, and K. Kang, "Secure Data Deduplication with Dynamic Ownership Management in Cloud Storage," IEEE Transactions on Knowledge and Data Engineering, vol. 28, no.

11, pp. 3113–3125, 2016.

[79] J. Li, X. Chen, M. Li, J. Li, P. P. Lee, and W. Lou, "Secure Deduplication with Efficient and Reliable Convergent Key Management," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 6, pp. 1615–1625, 2014.

[80] R. Chen, Y. Mu, G. Yang, and F. Guo, "BL-MLE: Block-Level Message-Locked Encryption for Secure Large File Deduplication," IEEE Transactions on Information Forensics and Security, vol. 10, no. 12, pp. 2643–2652, 2015.

[81] J. Stanek and L. Kencl, "Enhanced Secure Thresholded Data Deduplication Scheme for Cloud Storage," IEEE Transactions on Dependable and Secure Computing, 2016.

[82] M. Miao, J. Wang, H. Li, and X. Chen, "Secure Multi-Server-Aided Data Deduplication in Cloud Computing," Pervasive and Mobile Computing, vol. 24, pp. 129–137, 2015.

[83] Y. Zheng, X. Yuan, X. Wang, J. Jiang, C. Wang, and X. Gui, "Towards Encrypted Cloud Media Centre with Secure Deduplication," IEEE Transactions on Multimedia, pp. 1–16, 2016.

[84] X. Yao, Y. Lin, Q. Liu, and Y. Zhang, "A Secure Hierarchical Deduplication System in Cloud Storage," in Proceedings of the IEEE/ACM 24th International Symposium on Quality of Service (IWQoS), pp. 1– 10, 2016.

[85] J. Min, D. Yoon, and Y. Won, "Efficient Deduplication Techniques for Modern Backup Operation," IEEE Transactions on Computers, vol. 60, no. 6, pp. 824–840, 2011.

[86] P. Christen, "A Survey of Indexing Techniques for Scalable Record Linkage and Deduplication," IEEE Transactions on Knowledge and Data Engineering, vol. 24, no. 9, pp. 1537–1555, 2012.

[87] W. Xia, H. Jiang, D. Feng, F. Douglis, P. Shilane, Y. Hua, M. Fu, Y. Zhang, and Y. Zhou, "A Comprehensive Study of the Past, Present, and Future of Data Deduplication," Proceedings of the IEEE, vol. 104, no. 9, pp. 1681–1710, 2016.

[88] J. Wang, Z. Zhao, Z. Xu, H. Zhang, L. Li, and Y. Guo, "I-sieve: An Inline High Performance Deduplication System used in Cloud Storage," Tsinghua Science and Technology, vol. 20, no. 1, pp. 17–27, 2015.

[89] S. Raghavendra, C. M. Geeta, R. Buyya, K. R. Venugopal, S. S.Iyengar, and L. M. Patnaik, "DRSMS: Domain and Range Specific Multi-Keyword Search over Encrypted Cloud Data," International Journal of Computer Science and Information Security, vol. 14, no. 5, pp. 69–78, 2016.

[90] K. He, C. Huang, H. Zhou, J. Shi, X. Wang, and F. Dan, "Public Auditing for Encrypted Data with Client-Side Deduplication in Cloud Storage," Wuhan University Journal of Natural Sciences, vol. 20,

no. 4, pp. 291–298, 2015.

[91] Q. Liu, G. Wang, and J. Wu, "Consistency as a Service: Auditing Cloud Consistency," IEEE Transactions on Network and Service Management, vol. 11, no. 1, pp. 25–35, 2014.

[92] J. Du, C. Iorgulescu, A. Roy, and W. Zwaenepoel, "Gentlerain: Cheap and Scalable Causal Consistency with Physical Clocks," in Proceedings of the ACM Symposium on Cloud Computing, pp. 1–13, 2014.

[93] S. P. Phansalkar and A. R. Dani, "Tunable Consistency Guarantees of Selective Data Consistency Model," Journal of Cloud Computing, vol. 4, no. 1, pp. 1–12, 2015.

[94] W. Golab, X. Li, and M. A. Shah, "Analyzing Consistency Properties for Fun and Profit," in Proceedings of the 30th Annual ACM SIGACTSIGOPS Symposium on Principles of Distributed Computing, pp. 197–206, 2011.

[95] S. Raghavendra, K. Nithyashree, C. M. Geeta, R. Buyya, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik, "RSSMSO Rapid Similarity Search on Metric Space Object Stored in Cloud Environment," International Journal of Organizational and Collective Intelligence (IJOCI), vol. 6, no. 3, pp. 33–49, 2016.

[96] S. Singh, Y.-S. Jeong, and J. H. Park, "A Survey on Cloud Computing Security: Issues, Threats, and Solutions," Journal of Network and Computer Applications, vol. 75, pp. 200–222, 2016.

[97] B. K. Jeevitha, J. Thriveni, and K. R. Venugopal, "Data Storage Security and Privacy in Cloud Computing: A Comprehensive Survey," International Journal of Computer Applications, vol. 156, no. 12, pp. 16–27, 2016.

[98] J. Wang, X. Chen, X. Huang, I. You, and Y. Xiang, "Verifiable Auditing for Outsourced Database in Cloud Computing," IEEE Transactions on Computers, vol. 64, no. 11, pp. 3293–3303, 2015.

[99] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds," in Proceedings of the 2011 ACM Symposium on Applied Computing, pp. 1550–1557, 2011.

[100] J. Wang, X. Chen, J. Li, J. Zhao, and J. Shen, "Towards Achieving Flexible and Verifiable Search for Outsourced Database in Cloud Computing," Future Generation Computer Systems, 2016.

[101] J. Yu, X. Wang, and W. Gao, "Improvement and Applications of Secure Outsourcing of Scientific Computations," Journal of Ambient Intelligence and Humanized Computing, vol. 6, no. 6, pp. 763–772, 2015.

[102] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, "Verifiable Computation over Large Database with

Incremental Updates," in Proceedings of the European Symposium on Research in Computer Security, pp. 148–162, Springer, 2014.

[103] W.-S. Ku, L. Hu, C. Shahabi, and H. Wang, "A Query Integrity Assurance Scheme for Accessing Outsourced Spatial Databases," Geoinformatica, vol. 17, no. 1, pp. 97–124, 2013.

[104] K. Grolinger, W. A. Higashino, A. Tiwari, and M. A. Capretz, "Data Management in Cloud Environments: NoSQL and NewSQL Data Stores," Journal of Cloud Computing: Advances, Systems and Applications, vol. 2, no. 1, pp. 1–24, 2013.

[105] S. V. Kiran, S. Raghuram, J. Thriveni, and K. R. Venugopal, "Efficient Video Transfer using LAN Caching Assisted by Cloud Computing," in Proceedings of the TENCON Region 10 Conference, pp. 1–5, IEEE, 2015.

[106] H. Jo, S.-T. Hong, J.-W. Chang, and D. H. Choi, "Offloading Data Encryption to GPU in Database Systems," The Journal of Supercomputing, vol. 69, no. 1, pp. 375–394, 2014.

[107] A. Waqar, A. Raza, H. Abbas, and M. K. Khan, "A Framework for Preservation of Cloud Users Data Privacy using Dynamic Reconstruction of Metadata," Journal of Network and Computer Applications,vol. 36, no. 1, pp. 235–248, 2013.

[108] J. K¨ohler, K. J¨unemann, and H. Hartenstein, "Confidential Database-as-a-Service Approaches: Taxonomy and Survey," Journal of Cloud Computing, vol. 4, no. 1, pp. 1–14, 2015.

[109] F. Doelitzscher, C. Reich, M. Knahl, and N. Clarke, "Understanding Cloud Audits," in Privacy and Security for Cloud Computing, pp. 125–163, Springer, 2013.

[110] S. Krendelev, M. Yakovlev, and M. Usoltseva, "Secure Database using Order-Preserving Encryption Scheme Based on Arithmetic Coding and Noise Function," in Proceedings of the Information and Communication Technology-EurAsia Conference, pp. 193–202, Springer, 2015.

[111] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, "New Publicly Verifiable Databases with Efficient Updates," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 5, pp. 546–556, 2015.

[112] Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231–2244, 2012.

[113] J. Yu, K. Ren, C. Wang, and V. Varadharajan, "Enabling Cloud Storage Auditing With Key-Exposure Resistance," IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1167–1179, 2015.

[114] Y. Yu, L. Xue, M. H. Au, W. Susilo, J. Ni, Y. Zhang, A. V. Vasilakos, and J. Shen, "Cloud Data

Integrity Checking with an Identity-Based Auditing Mechanism from RSA," Future Generation Computer Systems, vol. 62, pp. 85–91, 2016.

[115] F. Yan, X. Chen, and Y. Zhang, "Efficient Online/Offline Signcryption without Key Exposure," International Journal of Grid and Utility Computing, vol. 4, no. 1, pp. 85–93, 2013.

[116] Y. Yu, Y. Zhang, J. Ni, M. H. Au, L. Chen, and H. Liu, "Remote Data Possession Checking with Enhanced Security for Cloud Storage," Future Generation Computer Systems, vol. 52, pp. 77–85, 2015.

[117] Y. Dodis, W. Luo, S. Xu, and M. Yung, "Key-Insulated Symmetric Key Cryptography and Mitigating Attacks Against Cryptographic Cloud Software," in Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, pp. 57–58, 2012.

[118] H.-Y. Lin, T.-S. Wu, M.-L. Lee, and C.-K. Yeh, "New Efficient Identity-Based Key-Insulated Multisignature Scheme," International Journal of Machine Learning and Computing, vol. 3, no. 1, pp. 117–120, 2013.

[119] Z. Xu, C. Wang, K. Ren, L. Wang, and B. Zhang, "Proof-Carrying Cloud Computation: The Case of Convex Optimization," IEEE Transactions on Information Forensics and Security, vol. 9, no. 11, pp.1790–1803, 2014.

[120] M. Sookhak, A. Akhunzada, A. Gani, M. Khurram Khan, and N. B. Anuar, "Towards Dynamic Remote Data Auditing in Computational Clouds," The Scientific World Journal, vol. 2014, pp. 1–12, 2014.

[121] J. Yu, H. Xia, H. Zhao, R. Hao, Z. Fu, and X. Cheng, "Forward-Secure Identity-Based Signature Scheme in Untrusted Update Environments," Wireless Personal Communications, vol. 86, no. 3, pp. 1467–1491,2016.

[122] Y. Zhang, C. Xu, S. Yu, H. Li, and X. Zhang, "SCLPV: Secure Certificateless Public Verification for Cloud-Based Cyber-Physical- Social Systems Against Malicious Auditors," IEEE Transactions on Computational Social Systems, vol. 2, no. 4, pp. 159–170, 2015.

[123] S. Zhou, R. Du, J. Chen, D. He, and H. Deng, "ESDR: An Efficient and Secure Data Repairing Paradigm in Cloud Storage," Security and Communication Networks, vol. 9, no. 16, pp. 3646–3657, 2016.

[124] J. K. Liu, K. Liang, W. Susilo, J. Liu, and Y. Xiang, "Two-Factor Data Security Protection Mechanism for Cloud Storage System," IEEE Transactions on Computers, vol. 65, no. 6, pp. 1992–2004, 2016.

[125] H. Wang, Q. Wu, B. Qin, and J. Domingo-Ferrer, "Identity-Based Remote Data Possession Checking in Public Clouds," IET Information Security, vol. 8, no. 2, pp. 114–121, 2014.

[126] S. V. Kiran, S. Raghuram, J. Thriveni, and K. R. Venugopal, "Efficient Stereoscopic 3D Video Transmission over Multiple Network Paths," International Journal of Computer Science and Information Security (IJCSIS), vol. 14, pp. 50–66, 2016.

[127] J. Liu, K. Huang, H. Rong, H.Wang, and M. Xian, "Privacy-Preserving Public Auditing for Regenerating- Code-Based Cloud Storage," IEEE Transactions on Information Forensics and Security, vol. 10, no. 7, pp. 1513–1528, 2015.

[128] J. Li and B. Li, "Erasure Coding for Cloud Storage Systems: A Survey," Tsinghua Science and Technology, vol. 18, no. 3, pp. 259– 272, 2013.

[129] H. C. Chen and P. P. Lee, "Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage: Theory and Implementation," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 407–416, 2014.

[130] Q. Yu, C. W. Sung, and T. H. Chan, "Irregular Fractional Repetition Code Optimization for Heterogeneous Cloud Storage," IEEE Journal on Selected Areas in Communications, vol. 32, no. 5, pp. 1048–1060, 2014.

[131] J. C Corena and T. Ohtsuki, "Pollution-Free Regenerating Codes with Fast Reconstruction Verification for Verifiable Cloud Storage," Journal of Networks, vol. 9, no. 11, pp. 2892–2904, 2014.

[132] H. C. Chen, Y. Hu, P. P. Lee, and Y. Tang, "NCCloud: a Network- Coding-Based Storage System in a Cloud-of-Clouds," IEEE Transactions on Computers, vol. 63, no. 1, pp. 31–44, 2014.

[133] B. Yang, X. Tang, and J. Li, "A Systematic Piggybacking Design for Minimum Storage Regenerating Codes," IEEE Transactions on Information Theory, vol. 61, no. 11, pp. 5779–5786, 2015.

[134] N. Silberstein, A. S. Rawat, and S. Vishwanath, "Error-Correcting Regenerating and Locally Repairable Codes via Rank-Metric Codes," IEEE Transactions on Information Theory, vol. 61, no. 11, pp. 5765 –5778, 2015.

[135] K. Huang, U. Parampalli, and M. Xian, "Security Concerns in Minimum Storage Cooperative Regenerating Codes," arXiv preprint arXiv: 1509.01324, vol. 62, no. 11, pp. 6218–6232, 2015.

[136] K. Huang, M. Xian, S. Fu, and J. Liu, "Securing the Cloud Storage Audit Service: Defending Against Frame and Collude Attacks of Third Party Auditor," IET Communications, vol. 8, no. 12, pp. 2106–2113, 2014.

[137] S. Raghavendra, S. R. Chitra, C. M. Geeta, R. Buyya, K. R. Venugopal, S. S. Iyengar, and L. M.

Patnaik, "Survey on Data Storage and Retrieval Techniques over Encrypted Cloud Data," vol. 14, no. 9, pp. 1–28, 2016.

[138] Y. Chen and Y. Wang, "On the Non-Existence of Minimum Storage Regenerating Codes with Repair-by-Transfer Property," IEEE Communications Letters, vol. 19, no. 12, pp. 2070–2073, 2015.

[139] L. Xue, J. Ni, Y. Li, and J. Shen, "Provable Data Transfer from Provable Data Possession and Deletion in Cloud Storage," Computer Standards and Interfaces, 2016.

[140] S. V. Kiran, R. Prasad, J. Thriveni, K. R. Venugopal, and L. M. Patnaik, "Cloud Enabled 3D Tablet Design for Medical Applications," in Proceedings of the 9th International Conference on Industrial and Information Systems (ICIIS), pp. 1–6, IEEE, 2014.