Research Article

Achieving Data Truthfulness and Privacy Preservation in Data Markets over Cloud Computing

Siddavatam Lakshmi Datta Meghana

Mahindra University, Hyderabad, India
sld.meghana@gmail.com

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 4 June 2021

Abstract: As data plays an important role in any organization where data DE duplication is a data encoding approach which is used for deleting present duplicate copies of replicated data, as well as it is preferably used for storage purpose in cloud to conserve space and bandwidth. To preserve privacy laws with some allowing de-duplication, the heterogeneous encoding method has been proposed to secure communications before privatization. It is the first comprehensive effort to address the issue of permitted data de-duplication in addition to enhancing data security. In contrast to conventional de-duplication methods, the replicate check approach often discusses both the data and the users' differential rights. In a hybrid cloud architecture, we do demonstrate a number of new de-duplication structures that allow for duplicate check. Our scheme is secure in respect of the definitions identified in the proposed security model, thus according securing data. We provide a prototype of our proposed accepted duplicate check scheme as a proof of concept and perform experiments with it. As compared to conventional operations, we display that our proposed allowed replicate check schemes suffers reduced overlap.

Keywords: Hybrid Cloud, Data Duplication, Privacy Preserving, Security, Redundancy

1. Introduction

Redundancy seems to have a lot in common with words like dunce, stupid, and reductive, if only because of the similar sounds they make when spoken. The notion of being repetitive repels those who read books, keep up with current affairs, and strive to bring original, new material to the table on a regular basis. However, in the context of cloud computing, redundancy provides comfort to those who are concerned about the cloud's ongoing flaws in data privacy and security. Redundancy in cloud computing refers to the provision of duplicate copies of various data, services, processes, and in the event that a part of one's cloud computing system fails or is inaccessible. This redundancy is accomplished by replicating data several times inside the same data center using multiple machines or units.

Since cloud computing is designed with a fail-first approach, there is no need to construct an expensive "high available redundant infrastructure," as one might with a traditional IT operating system. The cloud was designed with the knowledge that certain device components would fail at some point.

Cloud computing is the most recent technical advancement in the computing industry, and it focuses on developing services that are delivered to consumers in the same way that basic necessities including- Food, water, gas, electricity, as well as telecommunications are all necessities. Providers are deployed and processed just on cloud using this platform (a network is also designed for storing data known as a datacenter), and then made available to users as much as they want. Customers can get pay-per-use, available on-demand, and in low-cost availability cloud hosted services. Cloud computing has increased in popularity as a result of the services listed above. A cloud service provider (CSP), which functions similarly to an ISP in internet computing, provides all of services offered by servers to users. Users' attention has been drawn to this technology by some groundbreaking advances in internet technology, such as virtualization as well as distributed computing, as well as low-cost with access to high-speed networks. This technology is based on a novel idea of delivering utilities to consumers without forcing them to buy them or store them locally.

The built environment

In the cloud technology provisioning architecture, there are essentially three parties required to deliver services to users:-

1. User/Client

The customer is the one that makes use of cloud computing resources in the cloud computing architecture. It may be a mobile or stationary client that makes a service request to the cloud infrastructure, and then from the Third-Party Auditor (TPA) fulfills the request by providing the Cloud Server's requested services to these users (CS). Data is stored in data centers in cloud computing, and it can be accessed whenever and wherever it is required. Digital servers are connected to the data centers.

2. Third Party Auditor (TPA)

TPA stands for Third Party Auditor, and it is an agent who ensures secure service provisioning between cloud users and cloud service providers. TPA helps to secures contact among users with their cloud servers, as shown in Figure 1.TPA conducts certain operations for security purposes, such as agreement and authentication between users and service providers.

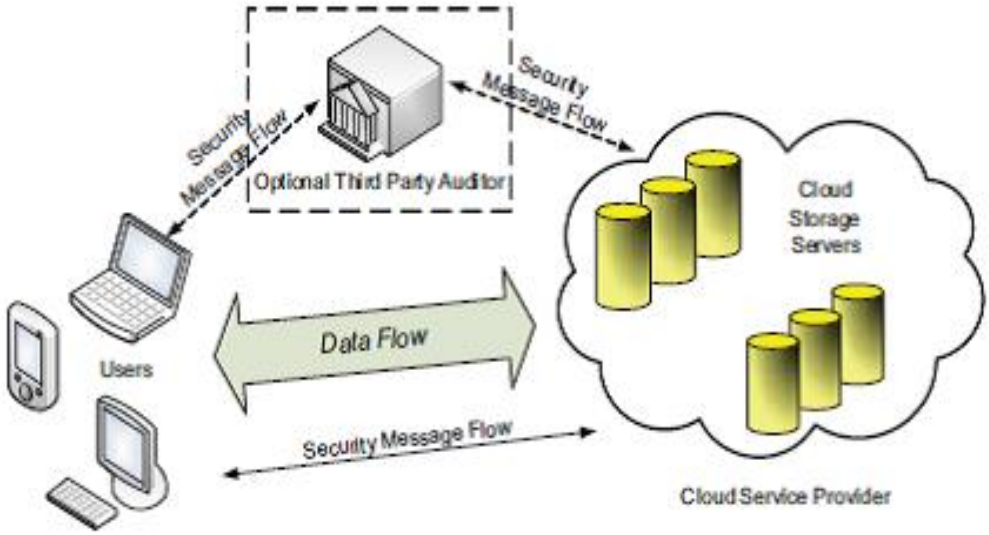

Figure 1 TPA architecture [1.

Cloud Service Provider (CSP)

These networks were provided by a cloud service provider with a good service-level agreement, higher customer loyalty, and lower costs. CSP provides services to customers in such a way that, if a service must be configured, the customer has the option of configuring the available services based on their needs and security concerns.

Models of Cloud Services

The three widely known categories for cloud computing services are

Below is the description of these three service models, in essence, are interconnected and have a three-tiered architecture. Figure 2 depicts the three-tier architecture of cloud computing.

IaaS: In a three-tier architecture, this is the first and most basic layer.

The middle or second layer of a three-tier architecture is PaaS (Platform-as-a-Service). In this model, users are given a structure that includes an operating system. PaaS applications include Force.com (a Salesforce.com spinoff) and GoogleApps. There are currently no guidelines for cloud interoperability or data portability, which developers should be aware of. Some service providers won't let their customers' apps leave their site.

The final level of the three-tier architecture is SaaS (Software-as-a-Service). Users may use "On-Demand software" without having to install, customize, or run them using this model. It must be paid for and used by a customer. The computer program, and communicates with the customer via a front-end platform. Software as a service (SaaS) is in high demand. Services provide email services along with inventory management. But since service is available from anywhere, the end user can use it from wherever.

Types of Cloud

From the point of view of the physical location of the user, Private cloud, public cloud, community cloud, and hybrid cloud are the four types of clouds [4].

In-home cloud computing: A cloud infrastructure is one that has been set up and services deployed by a single entity on its own data center. They create a virtual cloud infrastructure.

Cloud computing in the public domain: A Third-party cloud service providers provide public cloud services, that contains the resources that are not of the user's premises. Anyone on the Internet can buy services from a public cloud. Amazon Web Services is now the largest virtual server.

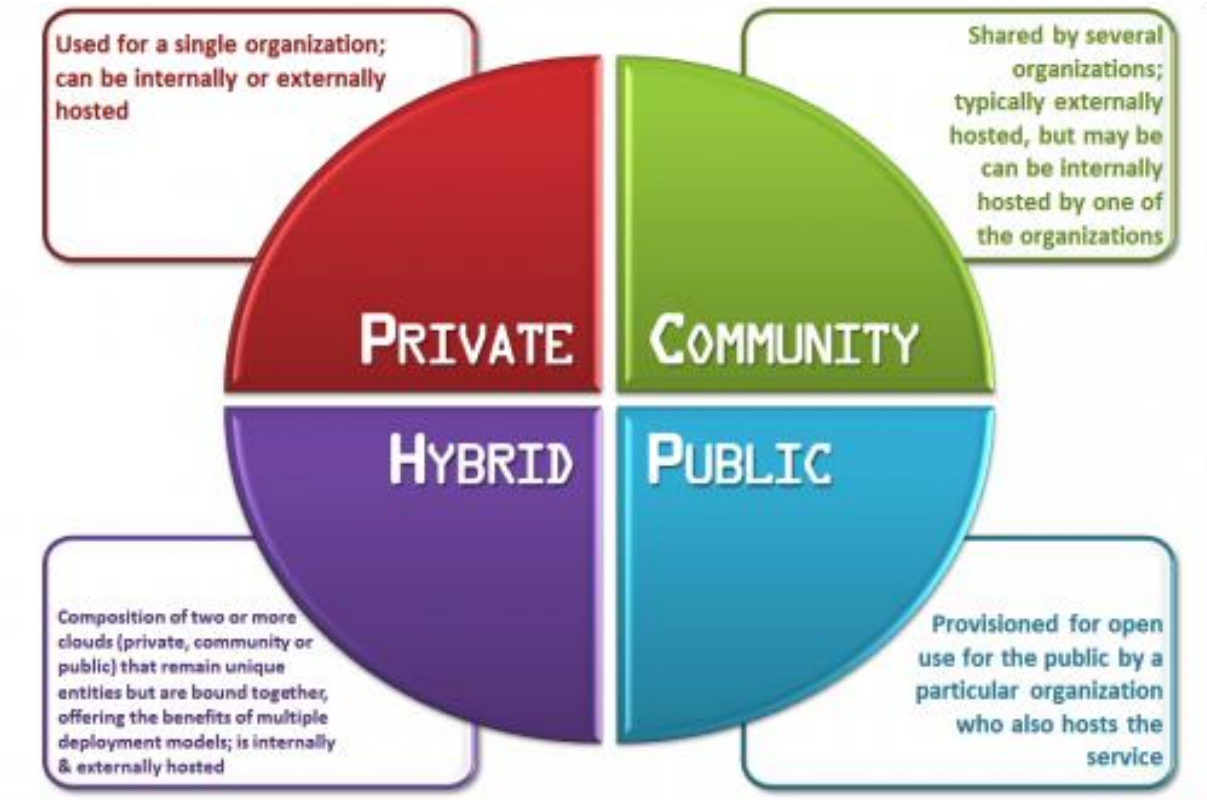

Figure 2 Types of clouds [2].

The Community [18] cloud is capable of providing services to a group of organizations.

Hybrid cloud: it is made up of two or more of the cloud types mentioned above.

A cloud system can be of any type, but its purpose is to make computing resources and IT services more accessible and scalable.

2. Literature Review Based On Privacy Preserving Of Data

In a paper [2] "Toward this Development of Efficient Redundant Data Schemes for Decentralized Cloud Based Infrastructures," Author look with how clustered redundant schemes can be implemented efficiently over heterogeneous infrastructures. They're especially interested in infrastructures with varying levels of online availability among nodes. They present a method for assessing data availability that is more reliable than current methods and takes these heterogeneities into account. They use this tool to determine the best data placement technique, which reduces the amount of duplication and associated overheads.

In a paper [9]-According to comprehensive security and performance review, the proposed schemes are both secure and highly successful. They've made it possible for an external auditor to review a user's cloud data without having to understand the data's content; they've also made it possible for the TPA to perform several distributed auditing tasks from different people in a privacy-preserving manner; they've set up a MAC-based setup; and they've made it possible for them to conduct several delegated auditing tasks from different people in a private information manner. This method utilizes the approximate numerical linear verification as well as random disguising to ensure that the TPA has no knowledge of the data content contained on the cloud server during the effective auditing phase, which somewhat relieves cloud users of the time-consuming as well as potentially expensive auditing mission, but also relieves their fears of external provider security breaches.

In this paper [3]-Algorithms such as RSA, DES, AES, and Blowfish have been used to ensure the security of data in the cloud, with a comparison review given. The symmetric key algorithms DES (Data Encryption Standard), AES, and Blowfish use a single key for both encrypting and decrypting messages. In cloud technology, user data is protected. The paper Used Cryptographic Techniques suggested a cloud-protection scheme that included a variety

of security techniques to address concerns about data loss, separation, and privacy using the cloud-based web services. Algorithms such as RSA, DES, AES, and Blowfish have been used to ensure the security of data in the cloud, with a comparison review given. The symmetric key algorithms DES (Data Encryption Standard), AES, and Blowfish use a single key for both encrypting and decrypting messages. The RSA algorithm uses a 1024-bit key length. As a result, the authors of this paper ran a number of algorithms and compared the results of each.

In this paper [4]-Implement a different random forest (rf combinations shorter digital signature that, unlike BLS, uses a general encryption algorithms like SHA-1 or MD5 rather than specialized hash functions. In addition, since it uses fewer matching processes than the BLS strategy, the strategy is more effective. A new negotiation form and a ring providing immediate are both built using this digital signature. In the random oracle model, we have exact security proofs for both the new and ring signature schemes. A modernized short signature scheme that replaces the BLS scheme.

In this paper [6]-They've worked with a variety of virtues, including confidentiality, honesty, availability, transparency, and privacy-preservability, as well as a variety of security concerns. Using an attribute-driven approach, the authors have specifically assessed the security and privacy problems in cloud computing. We defined the most descriptive security/privacy attributes (e.g., confidentiality, fairness, availability, transparency, and privacy-preservability) and investigated the various security concern issues from various perspectives.

Table 1: Comparison Among Previous Schemes.

ALGORITHMS	**ADVANTAGES**	**DISADVANTAGES**	**OUR SCHEME**
Attribute Based Encryption [1]	To provide a great-grained and comfortable access management, an ABE (Attribute Based Encryption) service is used to encrypt patient's knowledge.	Increases the complexity in the administration.	The scheme which we have used will provide reduce the complexity over data handling and will encrypt it for security.
Pushed Model [2]	It provides patients a management over the access of their information, a patient driven mannequin and an entry control framework to preclude unauthorized entry for the SPYSECURE knowledge.	It provides Dynamic entry manipulated framework which is difficult to maintain.	It uses the Boolean Search for the entry of the unauthorized entry.
Cloud-based SPYSECURE framework [5]	Results are exhibited which show the patient-driven cloud-based comfortable SPYSECURE framework is comfortable, versatile and productive [5].	For the man or woman area making use of mysterious multi-recipient personality centric encryption plan which is quite confusing.	The AES Encryption Technique which we have used provides clear-cut outputs.
A patient-pushed mannequin used [6]	Patients can access the information by the use of faraway virtual desktop.	Mannequin is used for all operations.	
TPA in a privacy-maintaining method. MAC [7]	The results and efficiency evaluation has been achieved in more than a few features similar to some sample blocks they've taken and computing of more than a few effect parameters.	TPA would now not be taught any advantage in regards to the knowledge content material saved on the cloud server for the period of the efficient auditing method.	TPA handles carefully in the AES Encryption.
BLS scheme [8]	An effective Signature Scheme from Bilinear Pairings and Its functions is used.	The protection of this symmetric cryptography is based on a new situation, namely adequate-CAA or okay + 1EP.	It focuses on providing security.
Privacy and security [9]	Security and Privacy in Cloud Computing provided.	Defence techniques and strategies are quite difficult to achieve.	Since, it provides the encryption of data so no chance of data misuse.

3. Objectives

Using multi-clouds, reduce the likelihood of cloud storage systems failing.

i) Reduce the risk of data failure while staying within a set budget by using several cloud service providers.

ii) To ensure the consumer data protection in the cloud by fragmenting data into fragments before replicating it on cloud service providers.

iii) Increase the values as per the expected level of data chunks even after replicating them across cloud service providers while staying within a budget.

4. Proposed System For Data Preserving

The user can only conduct a duplicate search on files that are labelled with the appropriate privileges.

By encrypting the file with differential privilege keys, we present an advanced scheme to support stronger protection.

Reduce the tag's storage space for integrity checks. To improve the protection of DE replication while maintaining data confidentiality.

5. Conclusion:

Here in this paper we proposed a technique in which we have reviewed different papers on auditing technique and presented the technique which is for verification for data redundancy or to verify the data duplication available with the cloud, here in the scheme we effectively apply the effective encryption algorithm and the integrity verification system in order to verify the cloud system as efficient while keeping the duplicate copy on the cloud storage data centre. A new multi-cloud architecture for enabling privacy-preserving outsourced data storage has been implemented, which is stable, cost-effective, and highly accessible. The approach is designed to assist and customer in making the best cloud file storage possible choice, taking into account the customer's budget as well as the optimal service quality (security, fast response, as well as data availability) offered by applicable cloud providers.

References

1. Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P. C. Lee, Wenjing Lou, “A Hybrid Cloud Approach for Secure Authorized De-duplication”, IEEE Transactions on Parallel and Distributed Systems, 2014.
2. Lluis Pamies-Juarez, Pedro Garc__a-L_opez, Marc S_anchez-Artigas, Blas Herrera, “Towards the Design of Optimal Data Redundancy Schemes for Heterogeneous Cloud Storage Infrastructures” ,” Computer Networks, Vol.55, 1100-1113, 2011.
3. Deyan Chen, Hong Zhao, “Data Security and Privacy Protection Issues in Cloud Computing”, International Conference on Computer Science and Electronics Engineering 2012.
4. Boyang Wang, Baochun Li, Hui Li,” Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud,” IEEE TRANSACTIONS ON Cloud Computing, VOL. 2, NO. 01, March 2014.
5. “The Notorious Nine - Cloud Computing Top Threats in 2013,” https://downloads.cloudsecurityalliance.org/initiatives/top_threats
6. “Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud,” IEEE Transactions on Services Computing, VOL. X, NO. X, XXXX 2014, accepted.
7. K. Ren, C. Wang, and Q. Wang, “Security Challenges for the Public Cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69–73,2012.
8. H. Shacham and B. Waters, “Compact Proofs of Retrievability,” Proc. 14th Int’l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT ’08),pp. 90-107, 2008.
9. Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li,” Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing”Proc. IEEE transactions on parallel and distributed systems, vol. 22, no. 5, may 2011
10. A. Juels and B.S. Kaliski Jr., “Pors: Proofs of Retrievability for Large Files,” Proc. 14th ACM Conf. Computer and Comm. Security (CCS ’07), pp. 584-597, 2007.
11. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, “Provable Data Possession at UntrustedStores,” Proc. 14th ACM Conf. Computer and Comm. Security (CCS ’07), pp. 598-609, 2007.
12. G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, “Scalable and Efficient Provable Data Possession,” Proc. Fourth Int’l Conf. Security and Privacy in Comm. Networks (SecureComm ’08), pp. 1-10,2008.
13. C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring Data Storage Security in Cloud Computing,” Proc. 17th Int’l Workshop Quality of Service (IWQoS ’09), 2009.
14. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,“Dynamic Provable Data Possession,” Proc. 16th ACM Conf.Computer and Comm. Security (CCS ’09), 2009.
15. K.D. Bowers, A. Juels, and A. Oprea, “Hail: A High-Availability and Integrity Layer for Cloud Storage,” Proc. 16th ACM Conf.Computer and Comm. Security (CCS ’09), pp. 187-198, 2009.

16. D. Boneh, B. Lynn, and H. Shacham, “Short Signatures from theWeil Pairing,” Proc. Seventh Int’l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT ’01), pp. 514-532, 2001