



JOURNAL ON COMMUNICATIONS

ISSN:1000-436X

Scopus®

REGISTERED

www.jocs.review

A LITERATURE REVIEW ON PRIVACY PRESERVING AND SECURITY PUBLIC AUDITING FOR CONTENT STORAGE IN CLOUD ENVIRONMENT

Dr. D. SRUJAN CHANDRA REDDY[1], Mr. JANARDHAN[2], Mr. G VENU GOPAL[3]
Professor[1], Assoc. Professor[2]
Department of CSE[1,2,3]
PBR VISVODAYA INSTITUTE OF TECHNOLOGY & SCIENCE, KAVALI, AP, INDIA.[1,2,]

Abstract: -Cloud storage is the means of exchanging over the internet different services. As a service customer, the storage may be used to store and transfer data remotely. Data management in the cloud has many advantages over local data storage. Without thinking about the need to check its accuracy, consumers should be allowed to access the data in cloud storage as though the knowledge were local. But providing data transparency is a problem. Cloud storage public audit functionality enables users to ask third-party auditor (TPA) to validate data honesty. This paper addresses numerous privacy-related problems as consumers store data in the cloud. We would examine the methods of supplying cloud service privacy and protection here. Safe cloud computing services may be introduced by delivering privacy-preserving public auditing using ring signature processes.

Keywords: -Cloud Computing, integrity, public auditing, privacy preserving.

I. INTRODUCTION

Cloud infrastructure is one of the fastest evolving innovations commonly embraced by many small IT companies as the cloud allows them to boost their industries as appropriate, without the need for a lot of money and time.

Cloud computing relates to the method of exchanging services over the internet, such as hardware, applications and production platforms. It provides On-Demand network access to dynamically configurable computing services in a pooled pool. All aspects in the as-a-service paradigm are supported by cloud infrastructure.

Storage as a Service is a business concept in which a big organization leases space to a smaller company or entity in their storage infrastructure. As per their use, the smaller business or individual consumers compensate for the storage room. The requirement for manual backup is totally minimized by utilizing cloud storage. It also lowers the expense of hardware, applications and personal repair expenditure [1]. Users may access data from anywhere, over the internet, at any time. They're more effective than computers for personal computing. So, the way the data is processed has been altered. Instead of being processed and managed by consumers, the data is either either consolidated or outsourced to cloud service companies. It introduces daunting security risks to the outsourced data of customers, in addition to these benefits.

It can be cheap and powerful to access from anywhere while the data is processed in the cloud, however the data can face several problems such as confidentiality, safety, and transparency due to attacks or failures. This can often contribute to an irretrievable failure of user details. The integrity of data in the cloud can be challenging for consumers to verify. So, they depend on the providers of cloud services. But cloud service providers cannot have full confidentiality, data accuracy [2] when processing massive volumes of information. They can also exploit the data of users which may place details at risk. Inside the cloud service, certain privacy and protection threats on customer data exist when they typically have full access to stored data and can steal the data to offer to external parties in order to obtain benefit. Users will not be conscious of their data misuse, because users may not be told about it by cloud service providers. In order to verify the quality and correctness of data, cloud service providers must allow users to inspect their data. User data auditing could also allow users to monitor and evaluate any actions that threaten the integrity of the data [3]. The audit should report on security violations, access to records, etc. Users have to choose the best stable cloud storage provider and encrypt data to protect data from others before saving it in the cloud.

II. SECURITY ISSUES IN CLOU COMPUTING

Cloud computing has number of security issues that are discussed below.

Privacy and security:

When user data is hosted in cloud storage, cloud service providers can ensure that access to user data is restricted exclusively to user authorization. This is important because unauthorized access by cloud staff to sensitive user data can lead to security issues for user data. It may create several protection issues because the same fundamental hardware is used to store data from the data of various entities. There could be a risk of identity disclosure and privacy loss. Any hardware attacks can impact data from different organizations.

Availability and reliability:

If a cloud service provider is secure, it must be assured that no loss of data can occur. If data from cloud customers were leaked, the reliability of cloud service providers and the reliability of cloud applications may be diminished. A strong percentage of uptime and only one hour of

downtime in a year can be assured by cloud service providers. However, where an accident happens, businesses will also think about the lack of control over their records. Cloud services will therefore not offer guarantees about their remote internet connection's uptime, and may also lock off all connections to the cloud. The data availability assurance is limited to the hardware modules and the internet connectivity all the time.

Data integrity:
The integrity of data relates to the task of protecting and ensuring the authenticity and durability of data during its life cycle. The architecture, deployment and use of any device that stores, processes, or retrieves data are a vital feature. Cloud service providers can use frameworks to maintain data privacy after delivering data protection, and be able to say what has happened to a given dataset and at what extent. The service provider can allow the consumer informed of details such as the cloud, sources and integrity processes used to host specific data.

Place of Data and Relocation:
A high degree of data mobility is provided through cloud computing. The positioning of their data is not necessarily understood for cloud consumers. However, if any confidential information is stored in the cloud on a computing unit, they might like to know the position of it. They will also like a preferred place to be listed. Which includes a binding arrangement between the storage provider and the cloud customer that knowledge should live or exist on a known server at a specific site? Cloud vendors can also assume responsibility for maintaining data protection and offering robust authentication to secure the knowledge of cloud users [4].

The transfer of data from one place to another is another issue. On separate servers, several copies of user data can exist. Initially, data is processed at a convenient location selected by the cloud provider. It is also transferred from one position to another, though. Cloud vendors have arrangements with each other and use services from each other. This will contribute to data loss by relocation.

Lock-In for Data:
Due to some circumstances, the cloud service provider could shut down. This can contribute to data from cloud users being locked in. Ultimately, since the old service provider does not work any longer, the customer can search for another service provider. Under certain instances, people cannot get access to their data and have to permanently lose their data. This could be a significant factor stopping corporate entities from switching to cloud computing.

III. PRIVACY OF CLOUD DATA

Cloud service providers enable customers to store their personal information in the cloud, such as bank payments, health care records, advertisement details. Privacy-sensitive details can be stored in every region of the world. Data movement between different locations can generate problems, such as how user data privacy is supported and protection is guaranteed [5]. To solve security problems, several strategies have been developed.

Privacy is the protection of a cloud user's personal records. The cloud customer is able to store their data and remain clear of data protection issues.

Privacy is described by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Charted Accountants (CICA) as:

"Privacy is the right and duty of persons and organizations to collect, use, retain and disclose personal information."

A. Issues of privacy and protection

According to the form of cloud storage model, privacy and protection concerns differ. In cloud computing, the following questions are tackled:

- The styles of opponents and their potential to corrupt data from the cloud.
- The protection concerns involved with the position of cloud storage and, where applicable, unauthorized access factors.
- Cloud users do not have sufficient training, unauthorized access, difficulty, no proper user control, resolving data flow problems and limitations, legal issues, compulsory disclosure of details to the government, position of data, no assurance of data ownership, data protection, and breach disclosure are several other issues that concern cloud use.

IV. TECHNIQUES TO SOLVE PRIVACY PROBLEMS

Cloud computing is a global operating infrastructure that offers online computing resources. Three service types include cloud storage. They are Software as a Service (SaaS), Application as a Service (PaaS) and Technology as a Service (IaaS). One of the common terms in IT companies at present is cloud computing? Cloud computing enables vast volumes of information to be processed, and does not ensure the accuracy and quality of records. Cloud service providers can often misuse data from users. So, the consumer has to look after the credibility of their results. This is not always practicable. In order to preserve data

protection, users rely on third party auditors (TPA) [6]. But the TPA is insufficient to offer an assurance of consumer data protection.
The consumer needs to encrypt their data before saving it in the cloud to maintain data security. But conventional methods of encryption have not been successful. If the data owner wishes to store data in the cloud, it can be secured and processed after that. To access the data from cloud storage, the customer must use a hidden key. The consumer can need to download and then decrypt all encrypted data from cloud storage and then locate the necessary data after that. The consumer can find it very difficult when the encrypted data is very big. This can take more time and entail additional user tools. This will also make for heavy network utilization and can boost server loads.
Various methods used to protect cloud data privacy and confidentiality is compared below.

1) Provable Data Possession at Untrusted Stores

The purpose of this technique is to detect in data storage any server wrongdoing. It uses a Provable Data Ownership (PDP) model that enables a client that has stored data on an untrusted server to check that the original data is held by the server without restoring it. By sampling random sets of blocks from the server, the model produces probabilistic evidence of ownership, which dramatically decreases I/O costs. It helps the server to view a limited portion of the file for evidence creation. To check the facts, the client retains a constant amount of metadata. A tiny, constant volume of data is transmitted by the challenge/response protocol, which minimizes network connectivity. Therefore, in broadly dispersed storage networks, the PDP paradigm for remote data testing supports massive data sets.

It describes a Provable Data Possession (PDP) model that produces probabilistic evidence when a third party stores a file. The paradigm varies from other approaches since it requires the server to view specific parts of the file while generating evidence; the whole file must be accessed through all other strategies. The first proven-secure framework for remote data management is given by this model. The quantity of metadata stored by the customer to validate evidence of the server is order O (1). The bandwidth that the scheme requires is O (1). The client's challenge and the server's answer are both significantly more than 1 Kilobit. It also offers a more powerful variant of this scheme that, while it gives a poorer promise, shows data ownership using a single modular exponentiation on the server.

Two proven-secure PDP systems are present in this technique. Even contrasted with schemes that obtain poorer assurances, they are more successful than other alternatives. That is because, as compared to linear in the size of the results, the overhead at the server is low (or even constant). The experimental findings indicate that known data possession (PDP) efficiency is restricted and limited by the input and output of the disk and not by the cryptographic techniques used during file storage. This will only verify the confidentiality of personal records.

2) Privacy-Preserving Public Auditing for Secure Cloud Storage

If users no longer have physical custody of outsourced records, Cloud Computing's data integrity security is a daunting challenge, particularly for users with restricted computing capital. In addition, without caring about the need to check its legitimacy, consumers should be able to access the cloud storage as though it were local. Therefore, it is of vital importance to allow public audit capabilities for cloud storage such that consumers can use a third-party auditor (TPA) to verify the integrity of outsourced data and be worry-free. The auditing phase can incorporate no new risks to the privacy of user data and introduce no extra online pressure on consumers in order to safely introduce a successful TPA [7].

A stable cloud computing framework enabling public auditing that protects privacy is used.
The homomorphic linear authenticator is incorporated with the random masking technique to accomplish privacy-preserving public auditing. In the server's answer, the protocol has a linear combination of sampled blocks that are masked with server-generated randomness.

The TPA no longer has all the requisite knowledge for random masking to construct up a valid group of linear equations and can thus not extract the data material of the consumer, no matter how many linear combinations can be gathered from the same range of file blocks. In the other side, even with the inclusion of randomness, the consistency validation of the block-authenticator pairs can still be carried out in a new way that will be seen shortly. In order to equip the auditing protocol with public audit capabilities, this architecture allows use of a public key dependent HLA. The capability of public audit, storage correctness, privacy protection, and batch auditing and lightweight should be accomplished by its architecture.

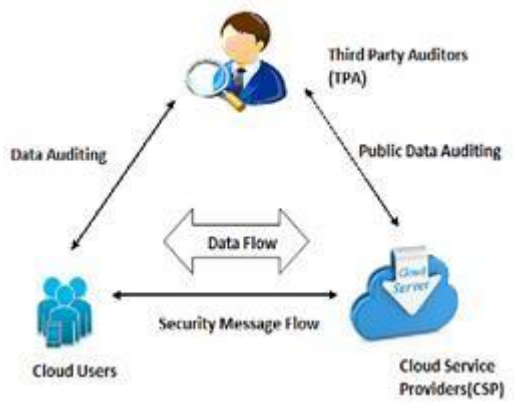


Fig1. Cloud Storage architecture With Cloud Service Providers, users, Third Party Auditor

3) Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds

This approach suggests an effective methodology focused on probabilistic query and periodic verification to enhance the efficiency of audit services based on techniques, fragment layout, random sampling and index-hash table, which can help proven improvements to outsourced data and timely irregular identification. This indicates that there is a smaller computational overhead for the current audit method.

Via the following audit functions, the TPA is guaranteed to be accurate and independent: TPA should be able to carry out routine checks on the accuracy and availability of assigned data at reasonable intervals; TPA should be able to arrange, manage and retain outsourced data instead of data owners; and TPA should be able to help dynamic data operations for approved applications; and TPA should be able to organize, manage and maintain outsourced data instead of data owners.

Our audit service consists of three processes to accomplish these functions: Tag Creation, Periodic Sampling Audit, and Complex Operations Audit.

This audit infrastructure's ultimate purpose is to improve the integrity of cloud storage providers, but not to increase the burden and overhead of the data owner. TPA can be built in clouds for this reason and managed by a cloud storage company (CSP). TPA must be adequately protected to withstand disruptive attacks in order to maintain faith and protection, and it should also be tightly regulated to avoid unauthorized access except by internal cloud members. A more realistic way is that a reliable third party could mandate TPA in clouds (TTP). This process not only increases the efficiency of audit services, but also guarantees full clarity of access for data owners. This implies that, besides keeping a hidden key and some secret information, data owners are allowed to use the audit service without extra costs.

4) Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing

This approach studies the topic of maintaining the security of Cloud Infrastructure data storage. In particular, consider the role of enabling, on behalf of the cloud customer, a third-party auditor (TPA) to check the accuracy of the dynamic data contained in the cloud. The implementation of TPA reduces the customer's presence by auditing if its data contained in the cloud is still intact, which may be critical for Cloud Storage to reach economies of scale. Supporting computer complexities through the most common modes of data operation, such as block adjustment, addition and deletion, is often a vital move for practicality, as Cloud Storage resources are not restricted to data archiving or backup alone. Although prior analysis to maintain the security of remote data frequently lacks the assistance of either public verifiability or complex data operations, all are accomplished in this document. The complexities and possible protection vulnerabilities of direct extensions with completely interactive data changes from previous works are established and then the technique of designing an elegant authentication mechanism for the smooth inclusion of these two excellent features in the architecture of the protocol is seen. In particular, by manipulating the classic Merkle Hash Tree (MHT) construction for block tag authentication, the Proof of Irretrievability model is enhanced to achieve powerful data dynamics. Extensive review of safety and efficiency reveals that the planned device is highly effective and known to be reliable.

5) Aggregate and Verifiably Encrypted Signatures from Bilinear Maps

A digital signature that supports aggregation is an aggregate signature scheme: Provided n signatures on n separate messages from n separate users, all of these signatures may be aggregated into a single short signature. This single signature (and the initial n messages) would persuade the verifier that the original n messages were genuinely signed by the n users (i.e., the person I signed MI for I = 1; n). It develops the idea of an aggregate signature, proposes authentication models for such signatures, and offers many aggregate signature implementations. Centered on bilinear maps attributable to Boneh, Lynn, and Shacham, it builds an appropriate aggregate signature from a recent short signature scheme.

In secure routing protocols like SBGP, aggregate signatures are useful for reducing the size of certificate chains (by aggregating all signatures in the chain) and for reducing the message size. It also illustrates that aggregate signatures offer birth to

signatures verifiably encrypted. Such signatures enable the verifier to verify that the encryption of a signature on a given message M is a given cipher text C. Encrypted signatures are verifiably used in contract-signing protocols. Finally, it is shown that the short signature scheme can be generalized to offer easy ring signatures utilizing similar concepts.

TABLE1

Comparison of various privacy preserving techniques

The comparison table lists the specific properties needed for the protection of cloud data and the correctness of the data when auditing. It addressed how different approaches protect the security of data collected in the cloud.

Properties Paper	Public auditing	Data privacy	Identity privacy
PDP	Yes [by user]	No	No
Privacy Preserving Public Auditing	Yes [by TPA]	Yes [ring signature]	No
Dynamic Audit Services	Yes [by TPA]	Yes [verification tag]	No
Enabling Public Verifiability	Yes [by TPA]	No	No
Aggregate & Verifiability Encrypted Signatures	Yes [by TPA]	No	No
Oruta: privacy preserving public auditing	Yes [by TPA]	Yes [ring signature]	Yes [homomorphic authenticable ring signature]

6) ORUTA: privacy preserving public auditing for shared data in cloud

This approach gives identity protection that is not offered by other approaches. The signer's name is kept secret from the Third-Party Investigator here (TPA). A person or a community of users who want to exchange data amongst them may be the cloud consumer. Each community participant has the ability to view and change the shared data as well. Each consumer has a user-generated private and public key of their own. Until sharing, each mutual data should be signed using private and public user keys. Data and its metadata for authentication, i.e., Cloud signatures are often processed. If evidence needs to be reviewed for accuracy, the documentation is checked by a third-party auditor (TPA). The credibility checking starts by submitting the TPA auditing challenge to the cloud server. The server then reacts to the task of auditing by presenting documentation of the ownership of mutual records. Through checking the correctness of the auditing evidence produced by the registry, the TPA tests the consistency of the details recorded on the server. TPA verifies if the signature is created by the user of the community on shared data. It is also hard to counterfeit the keys used for signing data so that people other than community users will not access the data. If the evidence is right, so the server will provide the correct facts.
Homomorphic Authenticable Ring Signature the ring signature used is (HARS). From conventional ring signatures, this ring signature is expanded. Ring signatures may often be shorter in duration than other signatures. It offers protection for identification, i.e., TPA recognizes that a signature is calculated using the private key of a community member, but doesn't know which key. As the signer's name is shielded from the TPA, this provides identity anonymity. HARS also has less verifiability for blocks. Without retrieving entire blocks of data, TPA will verify block correctness. It also helps complex operations on mutual data to be carried out.

V. CONCLUSION

Cloud storage is the technology with the highest development. Yet it also has its pitfalls, including the protection of cloud data privacy as a big concern. The approaches mentioned above offer different solutions to protect data privacy and also allow data auditing to verify data integrity. New approaches that address big challenges can be built in order to have maximum protection and privacy.

REFERENCES

1. *M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Comput- ing," Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.*
2. *G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-610, 2007.*
3. *Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.*
4. *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," Proc. ACM Symp. Applied Computing (SAC'11), pp. 1550-1557, 2011.*
5. *Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security (ESORICS'09), pp. 355-370, 2009.*
6. *Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory and*

Applications of Cryptographic Techniques:Advances in Cryptology (EUROCRYPT'03), pp. 416-432, 2003.

7. *Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc. IEEE Fifth Int'l Conf. Cloud Computing, pp. 43-56, 2014.*