International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Survey on Securely Shared Data on Cloud

Priti Padole[1], Priti Saktel[2]

[1]M. Tech student, Department of CSE, G.H Raisoni Institute of Engineering & Technology, Nagpur, Maharashtra, India

[2]Assistant Professor, Department of CSE, G.H Raisoni Institute of Engineering & Technology, Nagpur, Maharashtra, India

Abstract: ***Cloud is common place to store data and shared with multiple users. But some system problem or human error it generate more problem about integrity of cloud data. In the proposed scheme a new privacy preserving authenticated scheme for accessing secure data. It helps to verify the authenticity of the user without knowing the user's identity before storing information. It also allowed only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. Moreover, authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.***

Keywords: cloud computing, IDEA, Data Dynamics

1. Introduction

Now in a day's Cloud computing is most important factor in IT sector. By using this technology we can increase reliability, scalability as well as flexibility by decreasing cost as well time in faster world.

There are some major clouds computing service provider like Amazon, Google, Microsoft, Yahoo etc. There are many techniques to store data in cloud storage. Cloud service provider provides data storage service that ensure about users confidentiality, availability and integrity of data.

- **Confidentiality**: It is a set of rules that limits access to information.
- **Integrity**: It is the assurance that the information is trustworthy and accurate.
- **Availability:** It is a guarantee of ready access to the information by authorized people.
- Cloud improves due to centralization of data, increased security but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored data. Security is better than personal systems, because providers are able to devote resources to solving security issues that many customers cannot afford.

Why enhance the security in cloud?

Because there is number of user shared data with other users but when users data for other users then that time owner of data does not know about who access data.

The main reason is that the size of cloud data is large. In general downloading the entire cloud data to verify data integrity will increase cost or even waste user's amounts of execution and communication resources, especially when data have been corrupted in the cloud. Beside this, many uses of cloud data (e.g., data mining and machine Learning) do not necessarily need users to download the entire cloud data to local devices. It is because cloud Providers, such as amazons, can offer users computation Services directly on large-scale data that already existed in the cloud.

To enhancement of security level of shared data in cloud we use dynamic hashing technique and ammonization technique in encryption algorithm to protect our shared data from attackers.

Recently many works focus on providing three advanced features for remote data integrity checking protocols: data dynamic, verifying data publicly and providing privacy against various verifiers. The system also supports data dynamics at the block level which includes block insertion, modification and deletion. It also supports end of data operation. In addition, it can be easily adapted to support data dynamics. Can be adapted to support data dynamics by using the techniques. On the other hand, It support verifiability, by which anyone (not just the client) can perform the integrity checking operation.

2. Related Work

1) Boyang Wang, Baochun Li, and Hui Li, **[1]** Using Homomorphic Authenticable Ring Signature (HARS) and its properties established privacy-preserving public auditing mechanism for shared data in the cloud. It also support dynamic operations on shared data because when a user modifies a single block in shared data by performing an insert or delete operation, the indices of blocks that after the modified block[1].
2) C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,**[2]** By using data possession (PDP) model, the client pre-processes the data and then sends it to an untrusted server for storage, while keeping a small amount of data. The user asks after uploading data on server to prove that the stored data has not been modified (without downloading the actual data). However, the original PDP scheme applies only to static files [2].
3) C. Wang, Q. Wang, K. Ren, and W. Lou to securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce additional on-line burden to the cloud user [3].
4) E.-C. Chang and J. Xu, [4] shows how to modify Merkle's scheduling algorithm to achieve various tradeoffs between storage and computation. The improvement is achieved by

Licensed Under Creative Commons Attribution CC BY

means of a careful choice of what nodes to compute, retain, and discard at each stage.

5) Sushmita Ruj, Milos Stojmenovic, Amiya Nayak [5] By using attribute based encryption w privacy preserving authenticated access control scheme for securing data in clouds. At the time of user upload their data on cloud that time cloud verifies the authenticity of the user without knowing the user's identity before storing information by allowing only valid user to data decrypt.

3. Algorithm for enhance security of data on cloud

A. Homomorphic Authenticable Ring Signature (HARS)
Homomorphic Authenticable Ring Signature (HARS) is extended form of ring signature which not only able to verify privacy but also support to blockless verification [1].

B. Attribute Based Signature (ABS)
In Attribute Based Signature, users have a complaint to server with a message. This complaint helps to know the user have authenticated access, without knowing user identity. Other users or the cloud can verify the user and the validity of the message stored. By combining ABS (Attribute Based Signature) ABE(Attribute Based Encryption) to get authenticated access control without knowing the identity the user to the cloud. It create symmetric key to provide privacy preserving authenticated access control in cloud [5].

C. Markle's Signature Algorithm
The Merkle Signature algorithm gives an alternative of signature scheme. It only based on a secure hash function and a secure one-time signature. This algorithm is used for modification of data when user wants. This algorithm specially used for done dynamic operation on data like when any user want to modified other user data at that time firstly verify that user and send massage to authenticate user if user is valid then data will be modified by user otherwise not. In this algorithm allow only append mode [4].

D. Provable Data Possession (PDP)
Provable Data Possession (PDP) allows to user that has stored data at an entrusted server to verify that the server actual data without downloading. This model proofs of possession of server by sampling set of random blocks from the server, which reduces device costs. The user maintains a specific amount of large data to verify the proof. Thus, the PDP model for remote data checking supports large data sets in widely-distributed storage systems [2].

E. Third party Authentication (TPA)
Third party authentication (TPA) model play role of inspector that allows private as well as public audit ability. By using this model increase the security of data that store on cloud. To secure that data third party used encryption algorithm like RC5 to store data and create one secret key which send to user to decrypt data. But some time there is untested things are generated that's why there is many possibility to loss of data [3] .

F. International Decryption Encryption Algorithm (Idea)
IDEA algorithm is used to store data in encrypted format on cloud directly without any central authority interference. It is more secure than other one and to enhance security on cloud IDEA combine with Bit Serial architecture algorithm which is used to create data pattern when encrypt the data.

4. Conclusion

This paper presents the survey of various techniques and algorithm for enhance the security level for sharing data on cloud. As in the previous techniques and algorithm there were many drawbacks. The existing solutions is used to direct communicate without any centralise interference and store the data in encrypted format on cloud using IDEA algorithm which is implement easily and by combining bit serial architecture that create data pattern it make more secure.

References

[1] Boyang Wang, Student Member, IEEE, Baochun Li, Senior Member, IEEE, and Hui Li, Member, IEEE" Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud" IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 2, NO. 1, JANUARY-MARCH 2014.
[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.
[3] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses," Computer, vol. 45, no. 1, pp. 39-45, 2012
[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm.Security (CCS '07), pp. 598-610, 2007.
[5] 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), pp. 1-9, 2009.
[6] B. Wang, B. Li, and H. Li, "Certificateless Public Auditing for Data Integrity in the Cloud," Proc. IEEE Conf. Comm. and Network Security (CNS'13), pp. 276-284, 2013
[7] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computer and Comm. Security (CCS'09), pp. 213-222, 2009.
[8] C. 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.
[9] 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), 2008.
[10] A. Shamir, "How to Share a Secret," Comm. ACM, vol. 22, no. 11, pp. 612-613, 1979.

Licensed Under Creative Commons Attribution CC BY