Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Security for Shared Data Over Public Cloud for Maintaining Privacy

Subhash G. Rathod [#1], Dr. R N khobragade[#2], Dr. Vilas Thakare [#3,] Sushama L. Pawar[#4].

[#1]Research scholar, (PG Computer Science & Engg. Department), SGB Amravati University, Amravati, Maharashtra, India, (AP, MMIT, PUNE)
[#2,3]Professor, PG Dept. of Computer Science, SGB Amravati University, Amravati, M.S. India
[#4] Research scholar, Computer Engineering, VIIT, Pune, M.S. India
subhashrathod@gmail.com

Article Info
Page Number: 7167-7173
Publication Issue:
Vol. 71 No. 4 (2022)

Article History
Article Received: 25 March 2022
Revised: 30 April 2022
Accepted: 15 June 2022
Publication: 19 August 2022

Abstract
Currently, outsourcing of data to remote cloud is increasing day by day, People are outsourcing their data at Cloud Service Provider (CSP) who are offering vast amount of storage space with low cost which is minimizing the maintenance and burden of local data storage but once data goes into cloud user lose control over their data which brings new security risk. Data storage cost, access restriction and maintaining the integrity of data is a major concern in cloud security. Many organizations do not trust cloud providers to store their confidential data in public cloud storage because of security threats. The solution to the problem is given by different researchers in their work. However, the work in this regard has not achieved all security aspects correctly. The solution to the problem is given by different researchers in their work. However, the work in this regard has not achieved all security aspects correctly. To improve the correctness and performance of data security on the cloud while transferring the file is discussed in detail. While processing users request different attributes are checked for the processing of data. Each state is strictly defined with the attributes over the access.

Keywords: - Data Storage Cost, Cloud Security, Cloud Service Provider (CSP)

Introduction

In today's world cloud is the major trend for data storage in a distributed way to overcome the usage cost. The typical system uses heavy charges to use the data and store data in their physical locations. The cloud computing an approach which stores the data virtually in the storage system. This helps the user to avoid the storage space and they can use at anytime from anywhere. The cloud also helps to work efficiently for certain data access from multiple stations. The complexity of data storage is decreasing as researchers work on it. The services provided by the different organizations for data storing is easy with the cloud [8].

Cloud computing is the system where loosely coupled data is used but the organization should know the correctness of the use, the data correctness is the highest priority for any organization. In a system different authorized users have been allowed to access cloud storage but everyone has some restrictions. The system should work efficiently but the access control is managed by the system administrator. The personal data security is a major concern while transfer or store

the file. every activity should be passed through a secure manner as its open storage and open to access for any users from the cloud. A restriction has been providing with the responsibility and usage of data for a particular use, to restrict the user's number of methods or approaches that can be used for a purpose [5].

Data storing capacity of the cloud provides great significance to users. The user will not care about data storage locations physically and the capacity or expenditure required about that. In the system, the user has no concern with the data storing hardware requirements to execute the operation. The well-known examples of cloud systems are amazon simple storage services and amazon elastic compute cloud. The users are free from the responsibility of local users to store the data. The procedure of maintaining data security is not a concern with the user once the system is driven by the cloud. In user's aspect, even he uses the cloud security model for data but security concern remains in higher priority for the data on the cloud [8]. In a cloud the security concerns because of the external attacks on the cloud data which leads to adulterate the content of data and violates the integrity of cloud storage. As the correctness of user data not maintained on the cloud, the users would be worried about his data in the system [7]. In response to the problem of security, some mechanism should be there to tackle the problems of security and provide meaningful architecture. In a mechanism, the data should be free from the risk of interactions with any cloud users. In response, the method has included the cryptography mechanism with significant modifications and also auditor is introduced to keep watch on the system. This proves that data confidentiality and integrity over the data of the cloud.

The auditing task is performed with the use of third-party auditor (TPA) on cloud storage. Data auditing in cloud computing done with the Third Party Auditor (TPA). The data integrity and cloud secure storage checked by the TPA over the cloud. Auditing can be done individually or can audit entire user's data in single instance which is called batch auditing [6, 7, 9].

Cloud Platform Security Issues

The following formatting rules must be followed strictly

Education Cloud Platform

Now a day's education institutes are coming online, now learning and teaching is not confined to textbooks and classrooms, most of the education organizations now uses computers and mobile devices. Now students can pursue any course without physically going to the teaching institute. In remote education sharing educational documents and resource integration is a huge concern. With the frequent use of cloud for learning, security challenges are coming along the way, such as information theft, security assault in educational network.

Enterprise Cloud Platform

An enterprise cloud provides a unified operating environment through a single point of control for managing infrastructure and applications in any cloud. E-commerce companies or banks with huge data require large number of operating and maintenance staff but the malicious insider with authority can quickly access confidential information from cloud. Most of the cities have

free Wi-Fi network, people uses Wi-Fi without any security cover data can be exchanged without encryption.

Healthcare Cloud Platform

Healthcare cloud platform provides capabilities to manage health data at large scale and make it easier for healthcare organizations. Healthcare technologies perform important role while gathering of health records of patient through various gadgets, like smart watch, mobile phone, smart bands, and these gathered data is useful for healthcare research. Gathered data is shared across many insurance providers and healthcare networks. It is important to ensure that data to flow securely through every point of care to improve patient experiences and health outcomes.

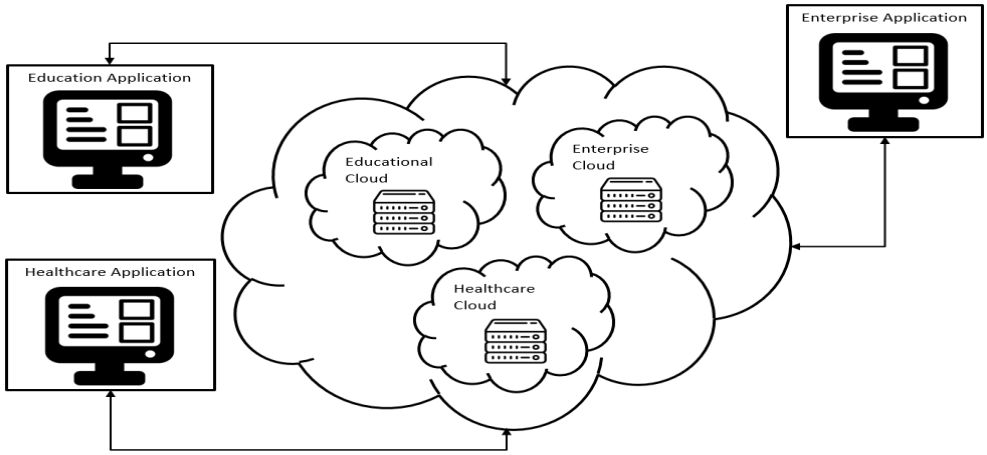

Figure 1 Cloud Storage Model

Literature Review of Existing Frameworks

Identity Based PDP Protocol

Author HAO YAN AND WENMING GUI presented a public identity-based PDP protocol for secure data storage. This protocol is mainly build to provide identity privacy protection of multiple users. With the help of this protocol a TPA can check the integrity of group shared data but cannot know who the owner of the data is.

There are four participants in proposed scheme: key generation Centre, CSP, users and TPA.

1. Key generation Centre is responsible for generating private keys for all users subscribed to the cloud. Here author assumed that the keys are transmitted by secure channel.
2. Cloud Service Provider (CSP) generates proofs for data integrity and maintains user's data.
3. Users those are subscribed to the cloud generate tags for their data and outsource the data to Cloud Service Provider. Here users share data in a group.
4. TPA checks the integrity of data. To audit the data TPA sends integrity challenge to CSP and gets a proof from CSP. Then TPA validates the proof and generate reports of data validation.

Proposed scheme ensures relationship between data and uploader in proof generation phase and not in integrity audition phase so that auditor does not know the data owner. In this paper author took efforts to protect privacy of data uploader [1].

Key Aggregation Encryption and ABE Technology

Author, Huang Nana, Yang Yuan proposed HealthCare cloud architecture which integrates multiple application based on privacy protection. Proposed framework uses attribute based encryption to encrypt Personal Health Record (PHR) files. Instead of traditional domain division which has public domain (PUD) and personal domain (PSD), the public domain (PUD) is further divided into PUD1 and PUD2 based on different access control over PHR files. Users in PUD1 have read or write access to the PHR files, while the users in PUD2 only have read permissions [2].

In the PSD, author used key aggregation encryption (KAE) to gain read access permission. For PHR users of PUD1 and PUD2, the outsourceable ABE technology is adopted to greatly reduce the computing burden of users [2].

ORUTA Framework (Ring Signatures and Homomorphic Authenticators)

Author, Boyang Wang, Baochun Li and Hui Li proposed Oruta framework which audit the shared data in the cloud and preserve the privacy of data owner during auditing phase. Here framework utilizes ring signatures to construct homomorphic authenticators, these authenticators helps public verifier to audit shared data and verify integrity without retrieving the entire data, With ring signatures, a verifier is convinced that a signature is computed using private key of one of group member but the verifier will not be able determine which group member.

Homomorphic authenticators are also called as homomorphic verifiable tags, which is a basic tool to construct auditing mechanism. Homomorphic authentication scheme is unforgeable that is only user with private key can generate valid signature [3].

CP-ABE Scheme

In this paper author Kaiping Xue, Weikeng Chen, Wei Li, Jianan Hong, Peilin Hong proposed an encrypted cloud storage with combined cloud-side and data owner-side access control, This framework is built to resistance DDoS/EDoS attacks and provides resource consumption accounting. Proposed framework uses CP-ABE Scheme for base construction.

Proposed system supports arbitrary CP-ABE constructions which is secure against malicious data users. Here author designed three controls among three entities in the system.

Control I: Data owners only allow authorized data users to decrypt the files.

Control II: Data owners verify the resource consumption records of the cloud provider.

Control III: The cloud provider verifies the data users before the download [4].

Table 1. Comparative analysis between different frameworks

Parameters	**EIBPIASDC [1]**	**IPMCP [2]**	**Oruta [3]**	**CDOCAECS [4]**
Security	Yes	Yes	Yes	Yes
Confidentiality	Yes	Yes	Yes	Yes
Integrity	Yes	No	Yes	No
Flexibility of authorization	No	Yes	No	No
Separation of duties	Yes	Yes	Yes	Yes
Data storage reduction	No	No	No	No
Fine-grained control	No	Yes	No	Yes

Conclusions

An organization need lot of hardware resources need to store data physically and takes more time and expenses to maintain it. As the data grows the necessity for storage space also grows, and it is necessary for businesses to store their massive data at low cost. Storing data in public cloud is more beneficial that storing it traditionally on local drive, most of the service provider gives certain degree of data security, but more security requires as the new vulnerabilities in cloud comes into picture.

Acknowledgment

The I am very much thankful to my PhD guide Dr. R. N. Khobragade for guiding. I am thankful to research centre head Dr. V. M. Thakare for supporting and helping in all way's needs. I am thankful to whole Sant Gadge Baba Amravati family for supporting, guiding and helping me.

References

[1] HAO YAN, WENMING GUI "Efficient Identity-Based Public Integrity Auditing of Shared Data in Cloud Storage with User Privacy Preserving" IEEE Access 10.1109/ACCESS.2021.3066497

[2] Huang Nana, Yang Yuanyuan, "An Integrative and Privacy Preserving-Based Medical Cloud Platform, IEEE Xplore 2021

[3] Boyang Wang, Baochun Li and Hui Li "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud" IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 2, NO. 1, JANUARY-MARCH 2014.

[4] Kaiping Xue, Weikeng Chen, Wei Li, Jianan Hong, Peilin Hong "Combining Data Owner-side and Cloud-side Access Control for Encrypted Cloud Storage" 1556-6013 (c) 2018 IEEE.

[5] Cong Wang, Bingsheng Zhang, Kui Ren and Janet M. Roveda3 "Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud" IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING 2013.

[6] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou "Privacy-Preserving Public Auditing for Secure Cloud Storage" IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2, FEBRUARY 2013.

[7] Kan Yang and Xiaohua Jia "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", IEEE Transactions on Parallel and Distributed Systems, Volume: 24, 2013 (4).

[8] Dr. Nashaat el-Khameesy, Hossam Abdel Rahman "A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems" Journal of Emerging Trends in Computing and Information Sciences, VOL. 3, NO. 6, June 2012 ISSN 2079-8407 (3).

[9] Chang Liu, Rajiv Ranjan, Chi Yang, Xuyun Zhang, Lizhe Wang, and Jinjun Chen "MuR-DPA: Top-Down Levelled Multi-Replica Merkle Hash Tree Based Secure Public Auditing for Dynamic Big Data Storage on Cloud" IEEE TRANSACTIONS ON COMPUTERS, VOL. 64, NO. 9, SEPTEMBER 2015

[10] Salah H. Abbdal, Hai Jin, Ali A. Yassin, Zaid Ameen Abduljabbar, Mohammed Abdulridha Hussain1, Zaid Alaa Hussien, Deqing Zou "An Efficient Public Verifiability and Data Integrity Using Multiple TPAs in Cloud Data Storage" 978-1-5090-2403-2/16 $31.00 © 2016 IEEE

[11] Farah Jihan Aufa, Endroyono, Achmad Affandi Department of Electrical Engineering Institute Teknologi Sepuluh Nopember Surabaya, Indonesia "Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm" 978-1-5386-5813-0/18©2018 IEEE.

[12] 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.

[13] V. Sathish, T. A. Sangeetha "Cloud-Based Image Processing with Data Priority Distribution Mechanism" Journal of Computer Applications (JCA) ISSN: 0974-1925, Volume VI, Issue 1, 2013

[14] Andrew B. Watson, NASA Ames Research Center "Image Compression Using the Discrete Cosine Transform"

[15] Solomon GuadieWorku, Chunxiang Xu, Jining Zhao, and Xiaohu. "Secure and Efficient Privacy-Preserving Public Auditing Scheme for Cloud Storage". Computers & Electrical Engineering, Volume 40, Issue 5, pp. 1703-1713, July 2014.

[16] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy- Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE lNFOCOM, pp. 525-533, 2010.

[17] B. Wang, B. Li, and H. Li, "Panda: Public Auditing for SharedData with Efficient User Revocation in the Cloud." IEEE Trans. Services Computing, 20 Dec .2013. DOT: 10. l109/TSC.20 13 .2295611.

[18] 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'll), pp. 1550-1557,2011.

[19] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps" Proc. 22ndInt'l Conf. Theory and Applications of

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

[20] Rathod, S., Khobragade, R. N., Thakare, V. M., Walse, K. H., & Pawar, S. (2022, September). Lightweight Auditable Secure Cloud Storage with Privacy Enabled Data Storage Optimization. In 2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS) (pp. 1-6). IEEE.

[21] Rathod, S., Khobragade, R. N., Thakare, V. M., Walse, K. H., & Pawar, S. (2022, September). Model for Efficient Data Storage on Public Cloud. In 2022 IEEE International Conference on Block chain and Distributed Systems Security (ICBDS) (pp. 1-5). IEEE.

[22] Rathod, S. G. SECURITY FOR SHARED DATA OVER PUBLIC CLOUD FOR MAINTAINING PRIVACY.

[23] Subhash Gulabrao Rathod, Dr. K. H. Walse, Dr. R N khobragade, Dr. Vilas Thakare , & Sushama L. Pawar. (2022). PRESERVING PRIVACY & MAINTAINING SECURITY FOR SHARED DATA OVER PUBLIC CLOUD: A SURVEY. International Journal Of Advance Research And Innovative Ideas In Education, 8(3), 4971-4976.

[24] Rathod, S., & Gupta, A. K. (2014). An Authentication and Recovery method for color Images.