IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 6, June 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006231|

An Integrate Privacy Preserving Attribute-Based Access Control Framework Supporting Secure Deduplication

Mandalam Dedeepya[1] , Parvathareddy Divya[2] Mr.J.Sathiya Jebasundar[3]

UG Student, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India [1,2]

Assistant Professor, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India [3]

ABSTRACT: Recent advances in information technologies have facilitated applications to generate, collect or process large amounts of sensitive personal data. Emerging cloud storage services provide a better paradigm to support the needs of such applications. Such cloud based solutions introduce additional security and privacy challenges when dealing with outsourced data including that of supporting fine-grained access control over such data stored in the cloud. In this paper, we propose an integrated, privacy-preserving user-centric attribute based access control framework to ensure the security and privacy of users' data outsourced and stored by a cloud service provider. The core component of the proposed framework is a novel privacy-preserving, revocable cipher text policy attribute-based encryption scheme. To support advanced access control features like write access on encrypted data and privacy-preserving access policy updates, we propose extended Path-ORAM access protocol that can also prevent privacy disclosure of access patterns. We also propose an integrated secure deduplication approach to improve the storage efficiency of CSPs while protecting data privacy. Finally, we evaluate the proposed framework and compare it with other existing solutions with regards to the security and performance issues.

I. INTRODUCTION

RECENT advances in information technologies have enabled applications to generate, collect, or process large amounts of privacy-sensitive data. Even though personalized applications have been proposed recently, their deployment and maintenance costs are significantly higher because of the increasingly challenging security, privacy, and management issues. To cope with increased storage capacity requirements and complex data management issues, cloud based storage services have become a very promising alternative for individual users as well as organizations. A cloud storage service helps to aggregate users' or organizations' distributed data from different applications .They, however, introduce additional security and privacy
challenges such as those related to data privacy, access control and secure storage. Although encrypting the privacy-sensitive data that is outsourced to the cloud storage can ensure data confidentiality, providing fine-grained access control on such data is still a significant challenge . The mechanisms used for outsourcing data to the cloud storage may further introduce privacy issues. For instance, an adversary may be able to analyze access patterns the cloud to infer privacy sensitive information about the user. Several cryptography-based access control schemes have been proposed recently to tackle the challenges related to ensuring data confidentiality by using encryption and providing fine-grained access control over encrypted outsourced data. These solutions aim to ensure that users can access their encrypted outsourced data at various levels of granularity. Cipher text Policy Attribute based Encryption (CP-ABE) [8] provides one promising approach for fine-grained access control on such data stored in the cloud storage. However, several challenges need to be tackled before CP-ABE schemes can be used in these applications. For example, original CP-ABE schemes do not support features like, privilege revocation and write access on encrypted data and policy updates.

II. LITERATURE SURVEY

[1]Ei Mon Cho, Takeshi Koshiba,"Secure deduplication in a Multiple Group signature setting", 2015.
Multiple group setting schemes have recently become important for enabling deduplication for cloud servers. We consider a new primitive, cross-group deduplication, allowing the multiple groups by the group signature features. We propose a new framework DDUP-MUG (deduplication for the multiple-group signature scheme) that allows one or more groups individual management and several clients from different groups who attempt to store an identical

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006231|

message on the server. In this paper, the group managers mainly manage the new entities and produce revocation lists for clients and the server respectively. We use Message Lock Encryption (MLE) as an ingredient for deduplication and we provide new three protocols, namely UPL-Dup (for uploading a new message), EDT-Dup (for editing the existing message) and DEL-Dup (for eliminating the existing message) in the DDUP-MUG framework.

[2]Ei Mon Cho,Takeshi Koshiba, "Big Data Cloud Deduplication based on verifiable hash converge group signcryption" 2017.
As Big Data cloud storage servers are becoming popular the shortage of disk space in the cloud becomes a problem. Data deduplication is a method to control the explosion growth of data on the cloud and most of the storage providers are finding more secure and efficient methods for their sensitive data. Recently, an interesting technique called signcryption has been proposed, in which both the properties of signature (ownership) and encryption are simultaneously implemented, with better performance than the traditional signature-then-encryption approach. According to the deduplication, we introduce a new method for a group of users that can eliminate redundant encrypted data owned by different users. Furthermore, we generate the tag which will be the key component of big data management. We propose a new primitive group signcryption for deduplication called verifiable hash convergent group signcryption (VHCGS) by adding the properties of group signcryption and the verification facilities for the storage server (third party).

[3]Zheng Yan, Wenxiu Ding, Xixun Yu, Haiqi Zhu" Deduplication On Encrypted Big Data in Cloud" 2016.
Cloud computing offers a new way of service provision by re-arranging various resources over the Internet. The most important and popular cloud service is data storage. In order to preserve the privacy of data holders, data are often stored in cloud in an encrypted form. However, encrypted data introduce new challenges for cloud data deduplication, which becomes crucial for big data storage and processing in cloud. Traditional deduplication schemes cannot work on encrypted data. Existing solutions of encrypted data deduplication suffer from security weakness. They cannot flexibly support data access control and revocation. Therefore, few of them can be readily deployed in practice. In this paper, we propose a scheme to deduplicate encrypted data stored in cloud based on ownership challenge and proxy re-encryption. It integrates cloud data deduplication with access control. We evaluate its performance based on extensive analysis and computer simulations. The results show the superior efficiency and effectiveness of the scheme for potential practical deployment, especially for big data deduplication in cloud storage.

[4]Chun-I Fan,Shi-Yuan Huang,Wen-Che-Hsu"Encrypted Data Deduplication in Cloud Storage 2015".
Cloud storage is a remote storage service, where users can upload and download their data anytime and anywhere. However, it raises issues regarding privacy and data confidentiality because all the data are stored in the cloud storage. This is a subject of concern for users, and it affects their willingness to use cloud storage services. On the other hand, a cloud storage server typically performs a specialized data compression technique (data deduplication) to eliminate duplicate data because the storage space is not infinite. Data deduplication, which makes it possible for data owners to share a copy of the same data, can be performed to reduce the consumption of storage space. Due to the above issues, there is a research on encrypted data deduplication. In this manuscript, we propose an encrypted data deduplication mechanism which makes the cloud storage server be able to eliminate duplicate ciphertexts and improves the privacy protection.

[5]Wenlong Tian ,Ruixuan Li ,Weijun Xiao ,Zhiyong Xu"PTS-Dep:A High-Performance Two-Party Secure Deduplication For Cloud Storage"2018.
In cloud storage, the message-locked encryption method is widely used in security deduplication. However, Brute force attack becomes a serious issue. Current research addresses the brute force attack problem in secure deduplication using a third-party model. Even though there is a trusted third party in real life, it is hard to be applied to traditional two-party based deduplication system which only includes the client and the storage provider. It is obvious that industries prefer to take the simpler and more practical secure architecture under the same level of security. However, the existing two-party secure deduplication approaches either have inferior performance or security holes. To make the two-party secure deduplication comparable in performance with unprotected baseline and keep the same level security with the existing two-party secure deduplication, we propose a high-performance two-party secure deduplication, PTS-Dep. By leveraging secure duplicate data detection scheme and secure duplicate data's key sharing scheme, PTS-Dep can perform data deduplication with the security guarantee. Our approach improves average deduplication performance up to 92\% for Fslhome workloads compared to previous secure deduplication schemes when the average chunk size is 12KB.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006231|

III. PROPOSED SYSTEM

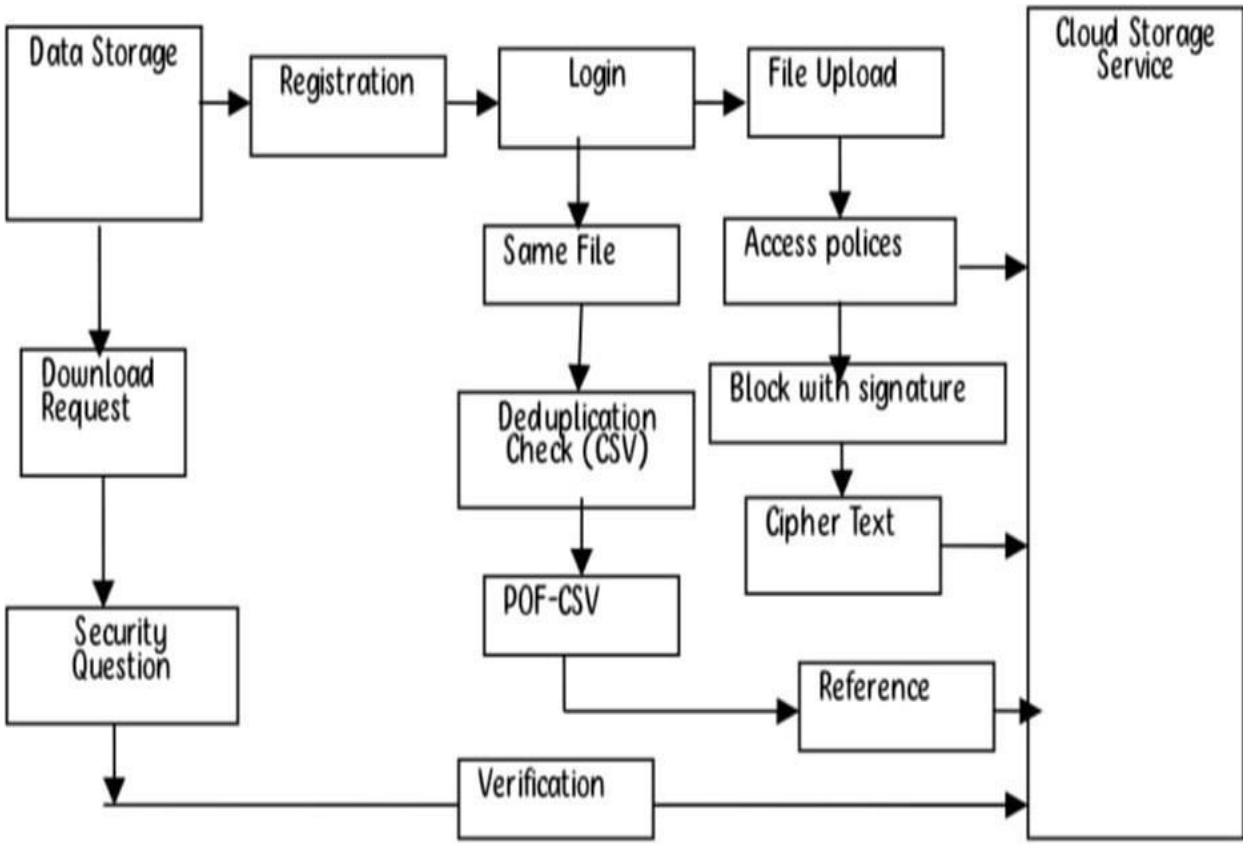
In this work, we proposed to storage across multiple CSP's and preserve data security by managing deduplication. we also introduced a scheme called Provable Ownership of the File(POF).They enhance user privacy and improve the performance of practical deployment. The random hash code challenge is applied to verify data ownership, which can guarantee that the data holder really have the original data rather than its hash code.

AIM:
The main aim of this project is to control file duplication in cloud computing.

OBJECTIVE:
The base part is our outsourced data, which defines the structure of outsourced data. Confidentiality of data is protected by symmetric encryption. We use PR-CP-ABE scheme to provide read access service to data is protected read access service to data by protecting private key of an existing symmetric encryption accesses data stored in an . In a CP-ABE scheme, an access policy that is attached to the cipher text may include several pieces of privacy sensitive based mechanism. Moreover the extended path ORAM protocol focuses on privacy issues related to disclosure in access pattern. The integration of ePath ORAM and PR-CP-ABE support advanced access control, such as write operation on data, access policy update, which are neglected in existing CP-ABE schemes.

WORKING DETAILS:
Registered users send access request and receive encrypted file if authorized. User calculates checksum mismatch occurs. Avoid De-duplication maintains the checksum data and block of the data compare at the time of file upload to avoid De-duplication. Auditor receives metadata after upload. Performs period on-demand integrity checks by sending challenges to cloud service provider auditor confirms response and reports status to Data Owner.

ARCHITECTURE DIAGRAM:



International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006231|

MODULE DESCRIPTION:

1.Cloud User Authentication

Owner has an initial level Registration Process in Cloud Service Provider(CSP). The users provide their own personal information for this process. The server in turn stores the information in its database. Then they have the Login process for the further access in cloud service Provider.

2. File Upload and Comparison

In this module, the data Owner create their account under the Public cloud and upload the file in cloud storage. Here the Provable Ownership of the file(POF) scheme is proposed. While uploading the file by data owner, the hash key is generated based on MD5 algorithm. The hash key is unique for all the upload files. But if the same file is upload by the other data Owner it will not allow the file to upload rather then it will replace the reference id through Mapping of index. It also check the file for physical present or not by both the data Owner.

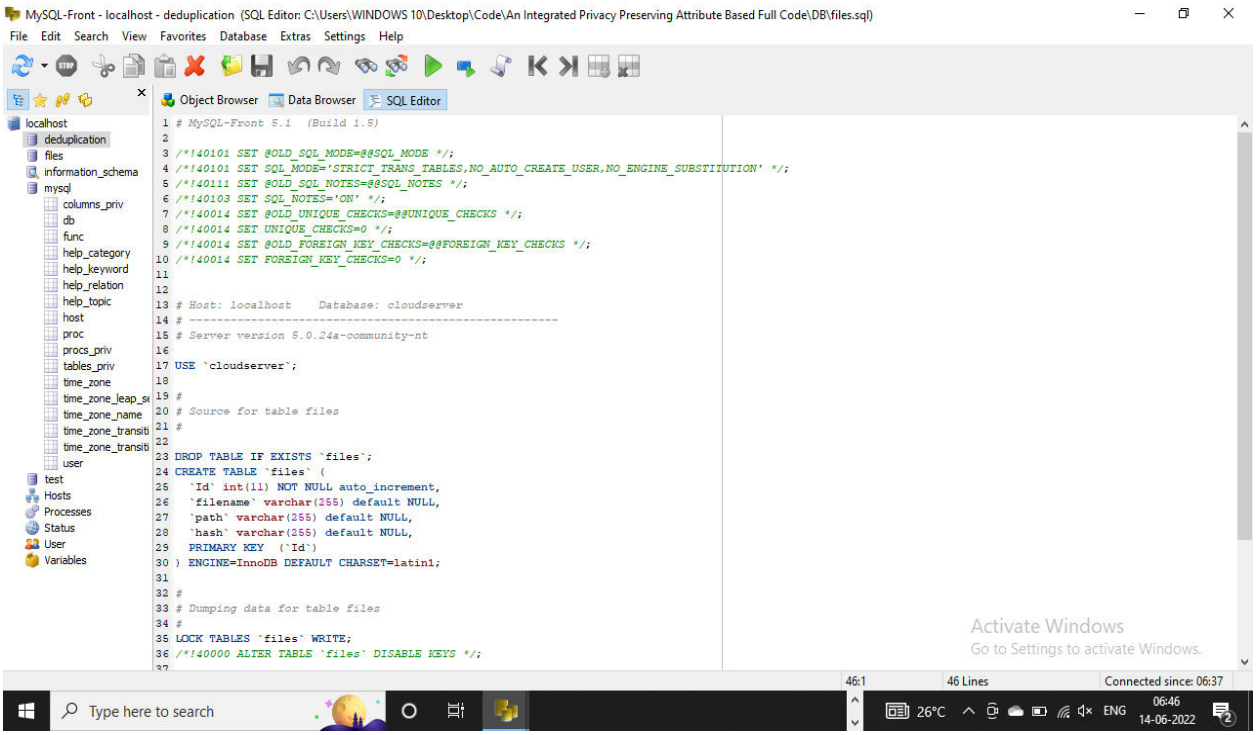
3. Set Access Policy for File

In this module User will chooses the file and uploads to Storage where the HDFS storage system .In the system will generate a signature in particular file and then split into multiple block. Each block will be generate signature with key . In the signature by using MD5 message-digest algorithm is cryptographic hash function producing a 128-bit hash value typically expressed in text format as 32 digit hex value so that files of same are de-duplicated. After that generate convergent keys for each blocks splitting to store CSV file .like filename, file path, blocks, username, password and block keys.

4. File Download Request and Handling

In this module, the data owner will download the file from cloud service provider. If they do not find the file then they will request to download the file from different Cloud service provider and also check whether the file is present or not then it gives the response to data owner.

IV.RESULT



| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006231|

V.CONCLUSION AND FUTURE ENHANCE

Thus we achieve data de-duplication and access control with different security requirements. Security analysis with secure, efficient and advanced has performed. In addition, we will conduct game theoretical analysis to further prove the rationality and security of the proposed scheme.

REFERENCES

[1]R.xu and J. B. Joshi, "An integrated privacy preserving attribute based access control framework," in Proc. IEEE 9th Int. Conf. Cloud Comput., 2016, pp. 68–76.

[2] Y. Zhang, M. Qiu, C.-W. Tsai, M. M. Hassan, and A. Alamri, "Health-cps: Healthcare cyber-physical system assisted by cloud and big data," IEEE Syst. J., vol. 11, no. 1, pp. 88–95, Mar. 2017.

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, et al., "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, 2010.

[4] D. J. Abadi, "Data management in the cloud: limitations and opportunities," IEEE Data Eng. Bull., vol. 32, no. 1, pp. 3–12, Jan. 2009.

[5] H. Takabi, J. B. Joshi, and G.-J. Ahn, "Security and privacy challenges in cloud computing environments," IEEE Security Privacy, vol. 8, no. 6, pp. 24–31, Nov./Dec. 2010.

[6] M. S. Islam, M. Kuzu, and M. Kantarcioglu, "Access pattern disclosure on searchable encryption: Ramification, attack and mitigation," in Proc. Netw. Distrib. Syst. Security Symp., 2012, vol. 20, Art. No. 12.

[7] M. Maffei, G. Malavolta, M. Reinert, and D. Schroder, "Privacy € and access control for outsourced personal records," in Proc. IEEE Symp. Security Privacy, 2015, pp. 341–358.

[8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.

[9] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. 14th Int. Conf.Pract.Theory Public Key Cryptography Conf.Public Key Cryptography,2011,pp.53–70.

[10] L. Zu, Z. Liu, and J. Li, "New ciphertext-policy attribute-based encryption with efficient revocation," in Proc. IEEE Int. Conf. Com put. Inf. Technol., 2014, pp. 281–287.

[11] M. T. Goodrich, M. Mitzenmacher, O. Ohrimenko, and R. Tamassia, "Practical oblivious storage," in Proc. 2nd ACM Conf. Data Appl. Security Privacy, 2012, pp. 13–24.

[12] E. Stefanov, M. Van Dijk, E. Shi, C. Fletcher, L. Ren, X. Yu, and S. Devadas, "Path ORAM: An extremely simple oblivious ram protocol," in Proc. ACM SIGSAC conf. Comput. Community Security, 2013, pp. 299–310.

[13] D. Apon, J. Katz, E. Shi, and A. Thiruvengadam, "Verifiable oblivious storage," in Proc. Int. Workshop Public Key Cryptography, 2014, pp. 131–148.

[14] E. Stefanov and E. Shi, "Multi-cloud oblivious storage," in Proc. ACM SIGSAC Conf. Comput. Commun. Security, 2013, pp. 247–258.

[15] D. T. Meyer and W. J. Bolosky, "A study of practical deduplication," ACM Trans. Storage, vol. 7, no. 4, 2012, Art. no. 14.

[16] N. Mandagere, P. Zhou, M. A. Smith, and S. Uttamchandani,"Demystifyingdata deduplication,"inProc.ACM/IFIP/USENIX Middleware Conf. Companion, 2008,pp. 12-17

[17] J. R. Douceur, A. Adya, W. J. Bolosky, P. Simon, and M. Theimer, "Reclaiming space from duplicate files in a serverless distributed file system, in Proc. 22ndInt.Conf.Distrib. Comput. Syst., 2002, pp. 617–624.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details