iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** III **Month of publication:** March 2020

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue III Mar 2020- Available at www.ijraset.com

A Survey on an Efficient Data Group Sharing and Data Auditing with Multi-Owner in Cloud Computing

Prateeksha Nagargoje[1], Prof. V. L. Kolhe[2]
[1]*Post Graduate Student,* [2]*Assistant Professor, Department of Computer Engineering, DY Pail College of Engineering, Akurdi, Pune*

Abstract: ***Cloud computing is becoming a prominent computing paradigm that allows users to store their data into a cloud server to enjoy scalable and on-demand services. Group data sharing in cloud environments has become a hot topic in recent. With the popularity of cloud computing, how to achieve secure data sharing in cloud environments is an urgent problem to be solved. Although encryption techniques have been used to provide data confidentiality and data security in cloud computing, current technique cannot enforce privacy concerns over encrypted data associated with multiple data owners, which makes co-owners unable to appropriately control whether data distributor can actually distribute their data. An Efficient Data Group Sharing and Data Auditing with Multi-Owner in Cloud Computing, in which data owner can share private data with a group of users via the cloud in a secure way, and data distributor can distribute the data to a new group of users if the attributes satisfy the access policies in the encrypted data. Further present a multiparty access control mechanism over the distributed encrypted data, in which the data co-owners can append new access policies to the encrypted data due to their privacy preferences.***
Keywords: Data sharing, cloud computing, Data auditing, encryption, privacy conflict.

I. INTRODUCTION

Compared with the traditional information sharing and communication technology, cloud computing has attracted the interest of most researchers because a lot services are provided by the cloud service providers which helps to reduce costs needed for various resources [3][1]. Cloud storage is one of the most vital service in cloud computing. Scalability is another attracting factor which allows user to scale up and scale down the resources as required. Cloud computing also provides convenient and flexible ways for data sharing. There are two ways to share data in cloud storage. The first case refers to the scenario where one client authorizes access to his/her data for many clients known as one-to-many pattern and the second case refers to a situation in which many clients in the same group authorize access to their data for many clients at the same time known as many-to-many pattern[1]. As the data shared on the cloud is valuable, various security methods are provided by cloud. In current cloud applications various algorithms are used for data encryption and decryption. In encryption is based on ABE [Attribute Based Encryption [1]. Symmetric-key cryptography is used in to enable efficient encryption. Practical group key management algorithm based on a proxy re-encryption technology [7].

II. RELATED WORK

Q in long Huang et al. [1] proposed a secure exchange of data groups and conditional spreading scheme with multiple owners in cloud computing, where the data owner can share private data with a group of users in a secure way. Also, presented a multipart access control mechanism on the transmit encrypted text, where data owners can add new policies to access encrypted text due to their privacy preferences. In addition, three policy aggregation strategies are provided, including full authorization, owner priority and majority authorization to solve the problem of privacy
conflicts caused by different access policies [13]. Safety analysis and experimental results show the system is practical and efficient for the secure exchange of data with multiple owners in cloud computing.

Z. Yan et al. [2] proposed a system to check the data access to cloud computing based on data-driven trust owner and reputation generated by a series of reputation. It focuses flexibly by applying attributes Encryption and proxy encryption. Also, he integrates the concept of trust assessment and reputation aware of the context in a cryptographic system to support multiple controls scenarios and strategies. The safety and performance of the systems are evaluated and justified by an exhaustive analysis, Safety testing, comparison and implementation. The results shown the efficiency, flexibility and flexibility of the data system access control in cloud computing.

H. Cui al. [3] proposed a notion called a proxy-assisted encrypted text policy Attribute-based encryption (PA-CPABE), which outsources most decryption calculations to peripheral devices. For the existing ABE with outsourced decryption schemes (ABE-OD), PA-CPABE has the advantage that the distribution of keys. It does not require any secure channel. They presented a generic construction of PA-CPABE and therefore they demonstrate its security. Moreover, implement an instance of the proposed PA-CPABE framework to evaluate its performance.

K. Xue et al. [4] proposed a solution to secure encrypted cloud storages from EDoS attacks and provide resource consumption accountability. It uses CP-ABE systems in a black-box manner and complies with arbitrary access policy of CP-ABE. He also presented two protocols for different settings, followed by performance and security analysis.

N. Paladi et al. [5] depicted a structure for information and activity security in IaaS, comprising of conventions for a confided in dispatch of virtual machines and space-based stockpiling insurance. He will proceed with a broad
hypothetical examination with proofs about convention opposition against assaults in the characterized risk model. The conventions permit trust to be built up by remotely bearing witness to have stage setup before propelling visitor virtual machines and guarantee secrecy of information in
remote stockpiling, with encryption keys kept up outside of the IaaS space. Additionally, he introduced trial results exhibit the legitimacy and productivity of the proposed conventions. The structure model was actualized on a proving ground
working an open electronic wellbeing record framework, indicating that the proposed conventions can be incorporated
into existing cloud situations.

Q. Huang et al. [6] proposed a personality-based information bunch sharing and scattering plan out in the open cloud, where information proprietor could communicate scrambled information to a gathering of beneficiaries one after another by determining these recipients' characters in an advantageous and secure manner. So as to accomplish secure and adaptable information bunch dispersal, they embraced trait based and planned discharge contingent intermediary encryption to ensure that solitary information disseminators whose characteristics fulfil the entrance strategy of scrambled information can scatter it to different gatherings after the discharging time by designating a re-encryption key to cloud server. The re-encryption conditions are related with traits and discharging time, which permitted information proprietor to implement fine-grained and coordinated discharge get to command over dispersed figure writings. The hypothetical investigation and trial results show our proposed framework makes a trade-off between computational overhead and
expressive spread conditions.

L. Jiang et al. [7] based on restrictive intermediary
communicate re-encryption innovation, a scrambled information sharing plan for secure distributed storage is proposed. The plan not just accomplishes communicate information sharing by exploiting communicate encryption, yet in addition accomplishes dynamic sharing that empowers adding a client to and expelling a client from sharing gatherings progressively without the need to change encryption open keys. Besides, by utilizing intermediary re-encryption innovation, our plan empowers the intermediary (cloud server) to straightforwardly share scrambled information to the objective clients without the mediation of information proprietor while keeping information security, so that incredibly improves the sharing execution. Then, the accuracy and security is demonstrated, the exhibition is broke down and the test results are appeared to confirm the attainability and productivity of the proposed plan.

Based on multiparty privacy control model, K. Xu et al. [8] designed a mechanism to enable each individual in a photo be aware of the posting activity and participate in the decision making on the photo posting. Also, he studied the scenario when a user shares a photo containing individuals other than himself/herself (termed co-photo for short). For this purpose, need an efficient facial recognition (FR) system that can recognize everyone in the photo. However, more demanding privacy setting may limit the number of the photos publicly available to train the FR system. To deal with this dilemma, the mechanism attempts to utilize users' private photos to design a personalized FR system specifically trained to differentiate possible photo co-owners without leaking their privacy. Also, he developed a distributed consensus-based method to reduce
the computational complexity and protect the private training set.

L. Fang al. [9] proposed a bargain-based incentive method to resolve the policy conflict problem. He proposed a novel pricing system to achieve the balance between privacy loss and sharing benefit. Besides, they introduced a Clark-tax based punishment mechanism to make sure that no co-owners would act maliciously. Game analysis and user studies are performed to illustrate the effectiveness of our proposed system.

Q. Huang et al. Information security [10] issue is one of the primary deterrents to the wide use of portable human services interpersonal organizations (MHSN), since wellbeing data is viewed as exceptionally touchy. Additionally, presented a protected

information sharing and profile coordinating framework for MHSN in distributed computing. The patients can redistribute their encoded wellbeing records to distributed storage with personality based communicate encryption (IBBE) system and offer them with a gathering of specialists in a protected and effective manner. Then displayed a characteristic based contingent information re-encryption development, which allows the specialists who fulfil the pre-characterized conditions in the ciphertext to approved the cloud stage to change over a ciphertext into another ciphertext of a personality-based encryption conspire for master without releasing any delicate data.

III.OPEN ISSUES

Lot of work has been done in this field because of its extensive usage and applications. In this section, some of the approaches which have been implemented to achieve the same purpose are mentioned. These works are majorly differentiated by the algorithm for group sharing and auditing.

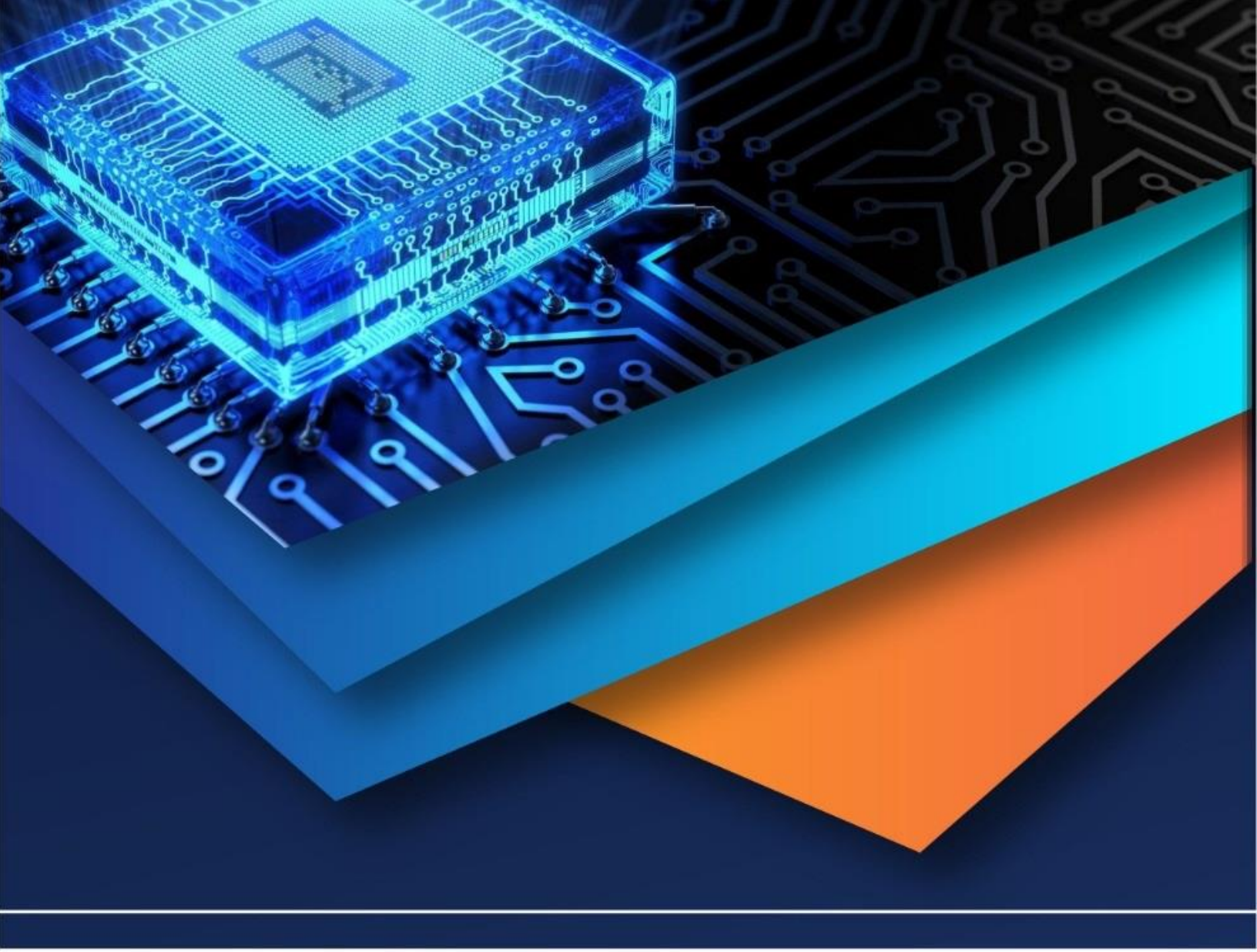
In current system when a user is revoked from a group, he is still able to access files from his previous group which leads to collision attack [1]. Another gap is that a user is not allowed to upload multiple files of same name and mostly used Attribute based encryption and Conditional proxy re-encryption techniques.

IV.CONCLUSION

Data security and privacy is a concern for users in cloud computing In particular, how to apply privacy concerns of multiple owners and protection of data privacy it becomes a challenge. In this survey, present a secure group for data exchange Multi-owner cloud computing scheme. In our schema, the data owner could encrypt his private data and share them with a group of data access devices simultaneously time conveniently based on the proposed technique. The data owner can specify specific access Attribute-based encrypted text therefore, the encrypted text can be encrypted only by data diffuser whose attributes satisfy the access policy in the encrypted tex.

REFERENCES

[1] Q in long Huang, Member, IEEE, Yixian Yang, Wei Yue and Yue He" Secure Data Group Sharing and Conditional Dissemination with Multi-Owner in Cloud Computing", IEEE TRANSACTIONS ON CLOUD COMPUTING , APRIL 2019
[2] Z. Yan, X. Li, M. Wang, and A. V. Vasilakos, "Flexible data access control based on trust and reputation in cloud -6computing," IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 485-498, 2017.
[3] H. Cui, X. Yi, and S. Nepal, "Achieving scalable access control over encrypted data for edge computing networks," IEEE Access, vol. 6, pp. 30049–30059, 2018.
[4] K. Xue, W. Chen, W. Li, J. Hong, and P. Hong, "Combining data owner-side and cloud-side access control for encrypted cloud storage," IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 2062–2074, 2018.
[5] N. Paladi, C. Gehrmann, and A. Michalas, "Providing user security guarantees in public infrastructure clouds," IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 405-419, 2017.
[6] Q. Huang, Y. Yang, and J. Fu, "Secure data group sharing and dissemination with attribute and time conditions in Public Clouds," IEEE Transactions on Services Computing, 2018.
[7] L. Jiang, and D. Guo "Dynamic encrypted data sharing scheme based on conditional proxy broadcast re-encryption for cloud storage," IEEE Access, vol. 5, pp. 13336 – 13345, 2017.
[8] K. Xu, Y. Guo, L. Guo, Y. Fang, and X. Li, "My privacy my decision: control of photo sharing on online social networks," IEEE Trans. On Dependable and Secure Computing, vol. 14, no. 2, pp. 199-210, 2017.
[9] L. Fang, L. Yin, Y. Guo, Z. Wang, and Fenzhua Li, "Resolving access conflicts: an auction-based incentive approach," Proc. IEEE Military Communications Conference (MILCOM), pp. 1-6, 2018.
[10] Q. Huang, W. Yue, Y. He, and Y. Yang, "Secure identity-based data sharing and profile matching for mobile healthcare social networks in cloud computing," IEEE Access, vol. 6, pp. 36584–36594, 2018.
[11] S. Wang, K. Liang, J. K. Liu, J. Chen, J. Yu, and W. Xie, "Attribute based data sharing scheme revisited in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 11, no. 8, pp. 1661–1673, 2016.
[12] K. Seol, Y. Kim, E. Lee, Y. Seo, and D. Baik, "Privacy-preserving attribute- based access control model for XML-based electronic health record system," IEEE Access, vol. 6, pp. 9114-9128, 2018.
[13] H. Hu, G. Ahn, and J. Jorgensen, "Multiparty access control for online social networks: Model and mechanisms," IEEE Trans. on Knowledge and Data Engine, vol. 25, no. 7, pp. 1614-1627, 2013.
[14] Q. Huang, Y. Yang, and M. Shen, "Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing," Future Generation Computer Systems, vol. 72, pp. 239-249, 2017.
[15] J. Hur, "Improving security and efficiency in attribute-based data sharing," IEEE Trans. on Knowledge and Data Eng., vol. 25, no. 10, pp. 2271-2282, 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY