International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

An Efficient Data Group Sharing and Data Auditing with Multi-Owner in Cloud Computing

Miss.Prateeksha Nagargoje and Mrs. V.L. Kolhe

Department of Computer Engineering D.Y. Patil college of Engineering,Akurdi, Pune Savitribai Phule Pune University Pune, India

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

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, exsisting 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 information proprietor can impart private information to a gathering of clients by means of the cloud in a safe manner, and information merchant can convey the information to another gathering of clients if the traits fulfill the entrance approaches in the scrambled information. Further present a multiparty get to control system over the appropriated scrambled information, in which the information co-proprietors can annex new access approaches to the encoded information because of their security inclinations.

Keywords: *Data sharing, cloud computing, Data auditing, encryption, privacy conflict.*

Introduction

Compared with the traditional information sharing and communication technology, cloud computing has attracted the interest of most researchers because a lot of 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 exsisting system, cloud based various algorithms are used for data encryption and decryption. The encryption is based on ABE i.e 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].

Literature Survey

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 integrate 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 re-encryption to ensure that solitary information disseminators whose characteristics fulfill 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 tradeoff 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-taxbased 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 fulfill 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.

Proposed Methodology

A. Group Member

In the proposed scheme, members are people with the same interests and want to share data in the cloud using encryption technique. The most worrying problem when users store data in the cloud server is the confidentiality of the outsourced data. In the system, users of the same group conduct a key agreement. Subsequently, a common conference key can be used to encrypt the data that will be uploaded to the cloud to ensure the confidentiality of the outsourced data. Attackers or the semi-trusted cloud server cannot learn any content of the outsourced data without the common conference key. This system uses a technique called group signatures, which allows users in the same group to anonymously share data in the cloud.

B. Group Manager

Group Manager is responsible for generating system parameters, managing group members (i.e., uploading member's encrypted data, authorizing group members). The group manager in our system is a fully trusted third party to both the cloud and group members. If an external user tries to access files from a different group more than three times then the manager will remove that particular user from the applications.

C. Cloud Service Provider(CSP)

Cloud server provider i.e CSP provides users with seemingly unlimited storage services. In addition to providing efficient and convenient storage services for users, the cloud can also provide data sharing services. However, the cloud has the characteristic of honest but curious. In other words, the cloud will not deliberately delete or modify the uploaded data of users, but it will be curious to understand the contents of the stored data and the user's identity.

D. Architecture

The trusted authority i.e the authority provider which shown in fig.(1) is a fully trusted part that initializes the system public key, and generates private keys for users. In system architecture, the user role divided into four categories which are data owner, data co-owner, data distributor and data accessor.

The data owner define an access policy to enforce dissemination conditions i.e read-write conditions. Then he encrypts data for a set of receivers, and outsources the ciphertext to CSP for sharing and and sprading the conditions. The data co-owners tagged by data owner can add some access policies to the encrypted data with CSP and generate the renewed ciphertext. The data distributor can access the data and also generate the re-encryption key to disseminate data owner's data to others if he satisfies enough access policies in the ciphertext. The data accessor can decrypt the initial, renewed and re-encrypted ciphertext with her or his private key.

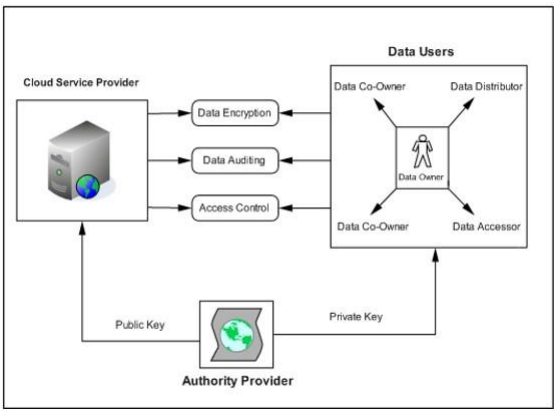

Fig. 1. Proposed System Architecture

E. Data Auditing

In this, Third Party Auditor i.e TPA is responsible for auditing. TPA is a Identified methods form a comprehensive sample for enabling continuous, secure, and privacy-preserving auditing of cloud storage data integrity. In the auditing thechnique we are going to use two algorithms for encryption. These algorithms are explained below:

F. Algorithm

1. Blowfish Algorithm

It is symmetric algorithm. It used to convert plain text into cipher text .The need for coming with this algo is weakness in DES/RSA. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider asweak.Blowfish was to be used 128-bit block with 128-bit keys.

Input:

128 bit /192 bit/256 bit input (0, 1) Secret key (128 bit) +plain text (128 bit).

Process:

10/12/14-rounds for-128 bit /192 bit/256 bit input
Xor state block (i/p)
Final round:10,12,14
Each round consists: sub byte, shift byte, mix columns, add round key.

Output:

cipher text(128 bit)

2. MD5 (Message-Digest Algorithm)

The MD message-digest algorithm is a generally utilized cryptographic hash work delivering a 128-piece (16-byte) hash value, commonly communicated in content arrangement as a 32 digit hexadecimal number. MD has been used in a wide assortment of cryptographic applications, and is likewise generally used to check information respectability. Steps:

- A message digest calculation is a hash work that takes a piece arrangement of any length and creates a piece succession of a fixed little length.
- The yield of a message digest is considered as an advanced mark of the info information.

- MD5 is a message digest calculation creating 128 bits of information.
- It utilizes constants determined to trigonometric Sine work.
- It circles through the first message in squares of 512 bits, with 4 rounds of activities for each square, and 16 tasks in each round.
- Most present day programming dialects gives MD5 algorithm as inherent capacities.

G. Mathematical Model

The mathematical model for Group Sharing and Auditing
System is as-
S ={*I,F,O,Success,Failure*}

Where,
I = Set of inputs i.e. Files
F = Set of functions
F ={*F*1,*F*2,*F*3,..*F*5}
Where,
F1: File Uploading
F2: File Encryption
F3: File Sharing
F4: File Auditing
F5: File Downloading
O = Group Sharing and Auditing
Space Complexity:

The space complexity depends on Presentation and visualization of discovered patterns.

More the storage of data more is the space complexity.
Time Complexity:

Check No. of patterns available in the datasets = n
If (n(1)) then retrieving of information can be time consuming, So the time complexity of this algorithm is O (nˆn).
Failures and Success conditions:

Failures:

1) Huge database can lead to more time consumption to get the information.
2) Hardware failure. 3) Software failure.

Success:

1) Search the required information from available in datasets.
2) User gets result very fast according to their needs.

Results and Discussion

To evaluate the performance, the schemes in [1] and Proposed system are simulated using the Stanford javax.cipher library. The experiments on these schemes are conducted on a laptop running Windows operation system with the following settings: CPU: Intel core i5 CPU at 2.5GHz; RAM memory:
4 GB

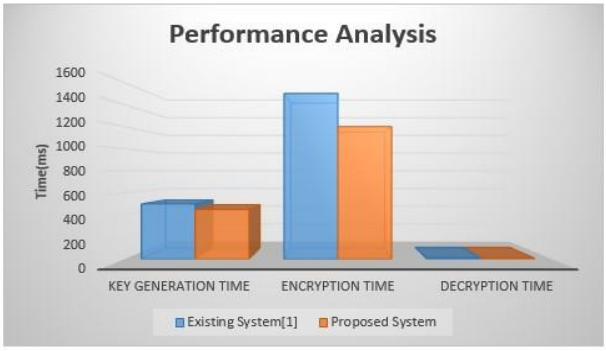

Fig. 2. Analysis Graph

	Existing System[1]	Proposed System
Key Generation Time	500ms	450ms
Encryption Time	1500ms	1200ms
Decryption Time	10ms	9ms

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 system present a secure group for data exchange Multi-owner cloud computing scheme. In the system 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 diff-user whose attributes satisfy the access policy in the encrypted text.

Future Scope

In the future, we will enhance our scheme by supporting Multi-keyword search over the ciphertext.

References

[1] Q in long Huang, Member, IEEE, Yixian Yang, Wei Yue and Yue He" Secure Data Group Sharing and Conditional Dissemination with Multi-
[2] Owner in Cloud Computing", IEEE transactions on cloud computing , april 2019
[3] Z. Yan, X. Li, M. Wang, and A. V. Vasilakos, "Flexible data access control based on trust and reputation in cloud computing," IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 485-498, 2017.
[4] 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.
[5] K. Xue, W. Chen, W. Li, J. Hong, and P. Hong, "Combining data ownerside and cloud-side access control for encrypted cloud storage," IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 2062–2074, 2018.
[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] S. Wang, K. Liang, J. K. Liu, J. Chen, J. Yu, and W. Xie, "Attributebased data sharing scheme revisited in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 11, no. 8, pp. 1661–1673, 2016.

[13] 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.

[14] 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.

[15] 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.

[16] J. Hur, "Improving security and efficiency in attribute-based data sharing," IEEE Trans. on Knowledge and Data Eng., vol. 25, no. 10, pp.

[17] 2271-2282, 2013.