International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 6, June 2020||

Data Sharing with Fine-grained Access Control using Block chain Technology

Shamsundar Sadashiv Bhimade, Prof. Antosh Madappa Dyade

Student, Department of Computer Science, SVERI'S College of Engineering, Pandharpur, University of Solapur, India

Professor, Department of Computer Science, SVERI'S College of Engineering, Pandharpur, University of Solapur, India

ABSTRACT: Group data sharing in block chain technologyand cloud computing 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.Data Sharing 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: Block chain,Data sharing, cloud computing, Data auditing, encryption, Privacy conflict.

I. INTRODUCTION

Cloud computing provides on demand service and processing resources to the Users or devices. It is dynamic computing style in which dynamically scalable and usually virtualization resources are provided as a service over the internet. Fundamental service offered by cloud providers is data storage. Cloud servers managed by cloud providers which are not fully trusted. Users may store data files on cloud which may be sensitive and confidential, like business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. One of the most significant difficulties is identity privacy for the wide deployment of cloud computing. Several security schemes for data sharing untrusted servers have been proposed. In these approaches, data owners store the encrypted data files in entrusted storage and distribute the corresponding decryption. Users may not be willing to join in cloud computing systems without the guarantee of identity privacy, because their real identities could be easily disclosed to cloud providers and attackers. Identity privacy may incur the sabotage of privacy. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable. Therefore, traceability, which enables the group manager to track over the real identity of a user, is also highly desirable. Highly recommended for any member in a group should be able to fully access stored data and sharing services provided by the cloud, which could be defined as the multiple-owner manner. More broadly, each user in the group is able to not only read data, but also modify their part of data in the entire data file. Finally, groups are normally dynamic in practice. Changes in membership makes secure data sharing extremely difficult. On the other side, the various system challenges granted from new users to learn the content of data files stored before their participation, because it is impossible for new approved users to contact with anonymous data owners, and obtain the corresponding decryption keys. An appropriate membership revocation mechanism without updating the secret keys of the remaining users is also desired to minimize the complexity of key management.

II. RELATED WORK

On the security of public key protocol Proposes public key encryption protocol, describes the various techniques to encrypt the public key[1].First complete group key management scheme which can supports all these functions yet preserves efficiency. The proposed scheme is based on the new concept of access control polynomial (ACP) that efficiently and effectively support full dynamics, flexible access control with fine-tuned granularity, and concealment .New scheme is protected from various attacks from both external and internal malicious parties[2].Achieving secure role based control on

encrypted data in cloud achieved through RBAC. RBE scheme allows RBAC policies to be apply for the encrypted data stored in public clouds. RBE-based hybrid cloud storage architecture provides facility of an organization to store data securely in a public cloud, while maintaining the sensitive information related to the organization's structure in a private cloud[3].One approach to encrypt documents satisfying different policies with different keys using a public key cryptosystem such as attribute-based encryption, and proxy re-encryption is called
broadcast group key management (BGKM), and then give a secure construction of a BGKM scheme called ACVBGKM. Major advantage of the BGKM scheme is that adding users/revoking users can be performed efficiently by updating only some public information. BGKM used for an efficient approach for fine-grained encryption-based access control for documents stored in an untrusted cloud file storage [4].MONA proposed a new secure multi-owner data sharing scheme, for multiple groups in the cloud. They applied the group signature. and dynamic broadcast encryption techniques, any cloud user can secretly share data with others. The storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. Also they analyze the security of scheme with difficult proofs, and demonstratethe efficiency of scheme in experiments[5].Data distribution in cloud infrastructure provides an effective approach called Secure-Split-Merge (SSM) is introduced for the security of data. The proposed SSM scheme was it uses unique mechanism for performing splitting of data using AES 128 bit encryption key. The chunks of encrypted splits are being maintained on various group servers of different types of cloud zones. The comparative analysis shows that the proposedsystem gives effective outcomes as compared to various existing and traditional security standards[7].Security achieves against chosen-plaintext attacks using the k-multi linear Decisional Diffie-Hellman assumption[8]. Fine-grained two-factor authentication (2FA) access control system for cloud services. Proposed 2FA access control system, it was an attribute based access control mechanism implemented with the necessity of both a user secret key and a lightweight security device[9].Efficient and secure re-encryption scheme has been proposed for data sharing in unreliable cloud environment. This scheme is built on top of Cipher text-Policy Attribute- Based Encryption (CPABE), fine-grained access control to share data. That scheme can achieve user revocation without whole cipher texts re-encryption and key re-distributions also, re-encryption is not performed until a user requests for that data, which reduces overheads. Further, it does not need any clock synchronization [10]. W. Sun et al. [11] present a privacy-preserving multi-keyword text search (MTS) scheme with similarity-based ranking to address this problem. To support multi-keyword search and search result ranking, we propose to build the search index based on term frequency and the vector space model with cosine similarity measure to achieve higher search result accuracy. G. W. Peters et al. [12] presents a work which give a diagram of the idea of block-chain innovation and its capacity to disturb the universe of managing an account through encouraging worldwide cash settlement, shrewd contracts, mechanized keeping money records and advanced resources. In such manner, they first give a concise outline of the center parts of this innovation, and in addition the second-age contract-based improvements. L. Luu et al [13] presents a work which gives another circulated understanding convention for authorization less block-chains called ELASTICO. ELASTICO is productive in its system messages and permit complex foes of up to one-fourth of the aggregate computational power.

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 in Block chain technology.

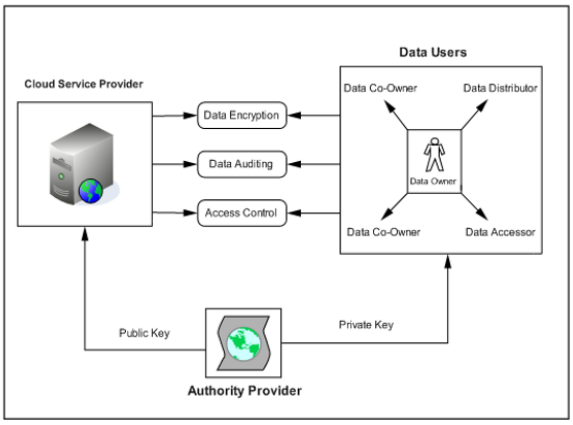
In current system when a user is revoked from a group, he is still able to access files from his previous group which leads to collision attack [1]. Another gap is that a user is not allowed to upload multiple files of same name and mostly used Attribute based encryption and Conditional proxy re-encryption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

IV.PROPOSED SYSTEM

The data owner define an access policy to enforcedissemination conditions i.e read-write conditions. Then he encrypts data fora set of receivers, and outsources the ciphertext to CSP for sharing and andsprading 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.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 6, June 2020||



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.

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.

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.

Algorithms:

1. AES Algorithm for Encryption.

AES (advanced encryption standard).It is symmetric algorithm. It used to convert plain text into cipher text .The need for coming with this algo is weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider asweak.AES was to be used128-bit block with128-bit keys.
Rijendeal was founder. In this drop we are using it to encrypt the data owner file.
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)

V.RESULT AND DISCUSSION

To evaluate the performance, the schemes in [1] and Proposed system are simulated using the Stanford javax.cipher library. The experimentson 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

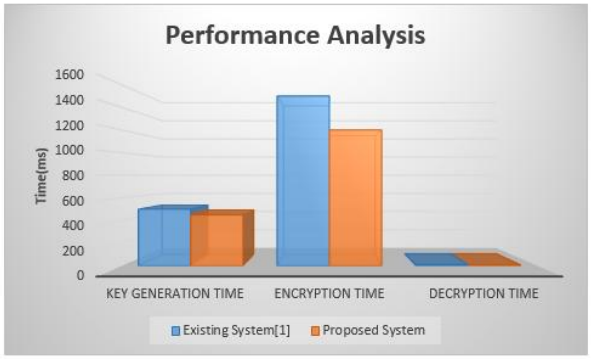


Fig. Performance analysis

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

VI.CONCLUSION

This system is design for secure data sharing scheme, for dynamic groups in an untruth cloud. A new type authentication system, which is highly secure, has been proposed in this system. User is able to share data with others in the group without disclose identity privacy to the cloud. It also supports efficient user revocation and new user joining. User revocation can be done through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. System also provides the new double encryption technique for data security. New re-encryption provides tight authentication.

REFERENCES

[1] D. Dole and A. C. Yao, On the security of public key protocols,IEEE Trans. Inf. Theory, vol. IT-29, no. 2, pp. 198208, Mar. 1983.

[2] X. Zoo, Y.-S. Dai, and E. Bettino, A practical and flexible key management mechanism for trusted collaborative computing, in Proc. IEEE Conf. Compute. Common. 2008, pp. 12111219.

[3] L. Zhou, V. Varadharajan, and M. Hitchens, Achieving secure role-based
access control on encrypted data in cloud storage, IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 19471960, Dec. 2013.

[4] M. Nabeel, N. Shang, and E. Bertino, Privacy preserving policy based content sharing in public clouds, IEEE Trans. Know. Data Eng., vol. 25, no. 11, pp. 26022614, Nov. 2013.

[5] X. Liu, Y. Zhang, B. Wang, and J. Yang, Mona: Secure multi owner data sharing for dynamic groups in the cloud, IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 11821191, Jun. 2013.

[6] Z. Zhu, Z. Jiang, and R. Jiang, The attack on Mona: Secure multi owner data sharing for dynamic groups in the cloud, in Proc. Int. Conf. Inf. Sci. Cloud Compute., Dec. 7, 2013, pp. 185189

[7] BurhanUl Islam Khan, Rashidah F. Olanrewaju SSM: Secure-Split-Merge Data Distribution in Cloud Infrastructure, in 2015 IEEE Conference on Open Systems (ICOS), August 24-26, 2015, Melaka, Malaysia

[8] JieXu, Qiaoyan Wen, Wenmin Li, and Zhengping Jin, Circuit Ciphertext- Policy Attribute-Based Hybrid Encryption with Verifiable Delegation in Cloud Computing IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 11821191, Jun. 2013.

[9] Joseph K. Liu, Member, IEEE, Man Ho Au, Member, IEEE, Xinyi Huang,Rongxing Lu, Senior Member, IEEE, and Jin Li, Fine-Grained Two- Factor Access Control for Web-Based Cloud Computing Services, IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 11821191, March 2013.

[10] NazatulHaque Sultan Ferdous Ahmed Barbhuiya, A Secure Re- Encryption Scheme for Data Sharing in Unreliable Cloud Environment, 978-1-5090-2616-6/16 2016 IEEE DOI 10.1109/SERVICES.2016.16.

[11] S. Pasupuleti, S. Ramalingam, R. Buyya, "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing," J NETW COMPUT APPL., vol. 64, pp. 12 – 22, 2016.

[12] W. Sun, B. Wang, N. Cao, H. Li, W. Lou, Y. Hou, H. Li, "Privacy preserving multi-keyword text search in the cloud supporting similarity based ranking," IEEE T Parall Distr., vol. 25, no. 11, pp. 3025 – 3035, 2014.

[13] 9/G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in Banking Beyond Banks and Money. New York, NY, USA: Springer-Verlag, 2016, pp. 239–278.