*International Journal of advancement in electronics and computer engineering (IJAECE)*
*Volume 5, Issue 2, June. 2016, pp.906-909, ISSN 2278 -1412*


# A Review on Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud

Pinky Mehra[1], Vimal Shukla[2]
[1] *MTech Scholar, Department of Cyber Security, Kailash Narayan Patidar College of Science and Technology, Bhopal, mehrapinky10@gmail.com, India;*
[2,] *H.O.D, Department of Cyber Security, Kailash Narayan Patidar College of Science and Technology, Bhopal,vimalshukla.cse@gmail.com, India;*

***Abstract*** *– Benefit since cloud computing, users can get an effective and cheap approach for information allocation between group members within the cloud with the characters of low maintenance and little management value. Meanwhile, we should give security guarantees for the sharing information files since they are outsourced. Unfortunately, because of the frequent modification of the attachment, allocation information while provided that privacy-preserving is still a challenging issue, especially for an untrusted cloud owed to the collusion hit. Moreover, for existing schemes, the security of key distribution relies on the secure line, however, to have such channel is a strong assumption and is difficult for practice. In this paper, we propose a protected data distribution system for energetic members. Firstly, we propose a secure method for key distribution while not any protected communication channel and the user can strongly acquire their non-public keys from group manager. Secondly, our design can attain fine-grained access organize, any user within the group can use the source in the cloud and revoked users cannot access the cloud again after they're revoked. Thirdly, we can shield the scheme from collusion attack, which means that revoked users cannot get the initial file even though they conspire with the untrusted cloud. In our approach, by leveraging polynomial operate; we can achieve a secure user revocation scheme. Finally, our scheme will succeed fine potency, which means that previous users needn't to update their non-public keys for matters either a replacement user joins within the group or a user is revoked from the group.*
***Keywords****: Access power, Privacy-preserving, Key distribution, Cloud compute*

## I. Introduction

Cloud computing, with the uniqueness of intrinsic information allocation and stumpy maintenance, provides a enhanced utilization of resources. In cloud computing, cloud service providers offer an abstraction of infinite storage space for clients to host data. It can help clients reduce their financial transparency of data management by migrate the confined management system into cloud servers. However, security concerns become the main constraint as we now outsource the storage of data, which is possibly sensitive, to cloud providers. To preserve data privacy, a common approach is to encrypt data files before the clients upload the encrypted information into the cloud. Unfortunately, it is difficult to design a secure and efficient data sharing design, particularly for dynamic group in the cloud. Kallahalla presented a cryptographic storage system that enable protected data allocation on unreliable servers based on the techniques that isolating files into file group and encrypting every file group with a file-block key. However, the file-block keys need to be updated and distributed for a consumer revocation; consequently, the structure had a important key distribution overhead. Other schemes for data sharing on entrusted servers have been proposed in. Nevertheless, the complexity of user contribution and revocation in this scheme are linearly increasing with the number of data owners and the revoked users. Yu exploited and combined techniques of key policy attribute-based encoding, proxy re-encryption and lazy re-encryption to realize fine-grained information access manage exclusive of disclose information contents. However, the single-owner manner might hold back the implementation of applications, wherever any member within the cluster will use the cloud service to store and share information files with others. Lu projected a protected attribution scheme by leveraging group signatures and code text-policy attribute-based encoding techniques. Each user obtain two key after the listing while the characteristic key is used to decrypt the data which is encrypted by the attribute-based encode and the

group mark key is used for privacy-preserving and traceability. However, the revocation is not supported in this scheme. In this document, we suggest a protected information distribution scheme, which can accomplish protected key allocation and information allocation for dynamic group. The main contributions of our system contain.We offer a secure method for key allocation without any protected communication channels. The users can strongly get their confidential key from group manager without any record establishment due to the confirmation for the public means of the user.

Our design can recognize fine-grained access manages, with the assist of the group user list, any user within the cluster will use the supply within the cloud and revoked users cannot access the cloud once more after they're revoked.

We propose a secure information sharing scheme which way be protected againts collusion attack. The revoked users cannot be capable to get the unique information files once they are revoked still if they conspire with the entrusted cloud. Our scheme can achieve secure user revocation with the help of polynomial function.

Our scheme is capable to bear dynamic group resourcefully, when a new user join in the cluster or a user is revoked from the group, the private keys of the extra users do not need to be recomputed and updated.

We provide safety analysis to prove the security of our design. In addition, we also perform simulations to demonstrate the efficiency of our system.

## II. Literature Survey

Zhongma Zhu et. al. [1] "A protected Anti-Collusion Data allocation Scheme for Dynamic Groups in the Cloud" In the cloud among the characters of low preservation and little managing charge. Meanwhile, we must offer security guarantees intended for the allocation information files since they are outsourced. Unluckily, because of the frequent change of the attachment, distribution information while providing privacy-preserving is still a not easy issue, especially for an untrusted cloud due to the knowledge assault. Moreover, for accessible scheme, the security of key allocation is base on the make safe communication conduit, however, to have such conduit is a strong supposition and is difficult for observe. In this proposed work, author intends a protected anti-collusion information distribution method for dynamic groups in the cloud. In our system, the users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels.

M. Armbrust et.al. [2] "over the Clouds: A Berkeley vision of Cloud Computing" In this projected process of cloud computation , cloud service providers offer an abstraction of infinite storage space for clients to host data It can help clients reduce their financial overhead of data managements by migrating the confined managements system into cloud server. However, protection concerns become the main constraint as we now outsource the storage of data, which is possibly sensitive, to cloud providers To preserve data privacy, a common approach is to encrypt data files before the clients upload the encrypted data into the cloud.

Kallahalla et al [3] "Plutus: Scalable protected folder allocation on Untrusted Storage," As storage space system and being storage space devices themselves become network, they must protect alongside the usual attack on communication traverse an untrusted, potentially unrestricted, network as well as attack on the store information itself. This is a challenge because the major purpose of networked storage space is to allow simple sharing of information, which is frequently at odds with data security. To protect store information it is not enough to use conventional network security techniques that are used for secure communication between pairs of user or connecting clients and servers. Thinking of a store information item as simply a message with very long network latency is a misleading correspondence. Since the same piece of information could be read by numerous users, when one user places data into a shared storage space system, the eventual addressee of this ``message" (stored data item) is often not known in advance. In addition, because many users could inform the same piece of information, a third client may from time-to-time update ``the message" before it reaches its eventual recipient. Stored data must be sheltered over longer period of time than distinctive message round-trip times. The method described in this article are used as configuration blocks to design Plutus, a complete, protected, and well-organized file organization. We built a prototype implementation of this plan by incorporate it keen on OpenAFS, and measured its presentation on micro-benchmarks. We showed that the presentation impact, due typically to the cost of cryptography, is equivalent to the cost of two popular scheme that encrypt on the wire. Yet, almost all of Plutus' cryptography is performed on clients, not servers, so Plutus has advanced scalability along by means of stronger security.

Shucheng Yu et.al. [4] "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud compute" Cloud computing is a shows potential to computing model which freshly has drained general awareness from both academia and industry. By combine a position of existing and new technique from research areas such as Service-Oriented Architectures (SOA) and virtualization, it is regard as such a compute model in which capital in the compute transportation are provide as services over the Internet. Along through this new model, various business models are developed, which can be describe by terms of "X as a service (XaaS)" . This paper aims at very well grained data admittance organize in cloud computing. One confront in this context is to achieve very well- grainedness, data discretion, and scalability at the same time, which is not provide by

present work. In this paper we propose a system to attain this goal by exploiting KP-ABE and exclusively combine it with technique of alternative re-encryption and lazy re-encryption. Furthermore, our projected scheme can enable the data owner to delegate most of calculation visual projection to controlling cloud servers

R. Lu et.al. [5] "protected attribution: The vital of Bread and Butter of Data Forensics in Cloud Computing," In this proposed method of cloud computing of data of forensics is given a easy technique Secure provenance that records possession and procedure history of information matter is very important to the accomplishment of data forensics in cloud computing, yet it is still a difficult matter today. In this article, to undertake this unknown area in cloud computing, we planned a new protected attribution system based on the bilinear combination technique. As the necessary bucks and grease of information forensics and post examination in cloud computing, the projected method is characterize by given that the information privacy on aware credentials store in cloud, unsigned verification on user admittance, and attribution tracking on doubtful credentials protected attribution is of dominant importance to the increase of cloud computing, yet it is still tough today. In this paper, we properly distinct the protected attribution and the equivalent safety model in cloud computing. Then, we projected a actual secure attribution SP scheme based on the bilinear pairings, and used the demonstrable safety method to prove its safety in the standard model. Due to its inclusive security features, the proposed SP system provides trusted evidences for information forensics in cloud computing and thus push the cloud computing for broad acceptance to the public.

## III. Method

Threat model, System model and Design goals

**3.1 Threat Model**: In this paper, we intend our plan delightful keen on account the Dolev-Yao representation, in which the invader can grasp, capture and grouping any significance at the correspondence channels. By means of the Dolev-Yao demonstration, the most excellent method to defend the information from attack.

**3.2 System Model**: Here the proposed model is illustrated in figure 1; the system model consists of three different entities: the cloud, a grouping administrator and a huge amount of group members. The cloud, supporting by the cloud examine provider, provide storage-space for hosting in sequence files in a expend as you go method on the further dispense, the cloud is untrusted because the cloud check provider are with no trouble to develop into untrusted. Therefore, the cloud will try to learn the substance of the stored data. Group manager will find charge of system parameter production, user registration, also, client repudiation. Group persons (clients) are an arrangement of sign up clients that will accumulate their own particular information into the cloud and inform them to others. In the plan, the meeting enrollment is strongly changed, because of the new client call-up and client denial.

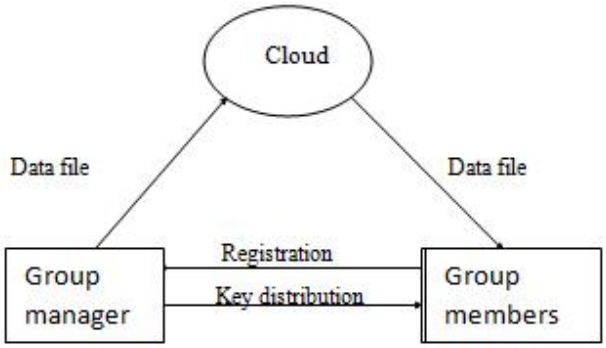


Figure1: System Model

**3.3 Design Goals:**

We represent the standard plan objectives of the projected plan including key circulation, information secrecy, access control and effectiveness as takes after:

3.3.1 Key distribution:

The prerequisite of key transportation is that clients can safely get their confidential keys from the assembly executive with no credential establishment. in other obtainable plans, this reason is skilful by expect with the intention of the communication channel is protected, on the other hand, in our plan; we can achieve it without this solid thought.

3.3.2 Access control:

First, collect individuals can make use of the cloud asset for information stockpile and information allocation. Next, unapproved clients can't get to the cloud asset whenever, and disavowed clients will be empty for utilizing the cloud quality again once they are renounced.

Information classification: data confidentiality requires that unapproved clients with the cloud are unfitted for taking in the matter of the put missing information. To keep up the ease of access of information confidentiality for element gathering is still a necessary and testing issue. in particular, renounce clients can't decode the put away information document after the denial.

3.3.3 Efficiency:

Any gathering part can store and communicate information records to others in the gathering by the cloud. Client repudiation can be accomplished without plus the others, which implies that the residual clients don't have to overhaul their private keys. In this segment, we verify the security of our design in terms of key distribution, access control and data confidentiality. in our scheme, the communication entities can securely negotiate the public key pk and distribute the private

key

key = {xi , ai , bi } to users without any certificate authorities and secure communication channels.

## IV. CONCLUSION

In this paper, we outline a protected against agreement information sharing plan for element bunches in the cloud. In our plan, the clients can safely acquire their private keys from gathering director Certificate Authorities and secure correspondence channels. Likewise, our plan can bolster dynamic gatherings proficiently, when another client joins in the gathering or a client is denied from the gathering, the concealed key of alternate clients don't should be recomputed and redesigned. In addition, our plan can accomplish secure client repudiation, the disavowed clients can not have the capacity to get the first information records once they are denied regardless of the possibility that they plot with the untrusted cloud.

## References

[1] Zhongma Zhu, Rui Jiang, "A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud" 10.1109/TPDS.2015.2388446, IEEE Transactions on Parallel and Distributed Systems

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr.2010.

[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[4] Shucheng Yu, Cong Wang, Kui Ren, and Weijing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[5] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[6] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yang, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, June 2013.

[7] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[8] Lan Zhou, Vijay Varadharajan, and Michael Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage," IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 1947-1960, December 2013.

[9] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content

[10] sharing in public clouds," *IEEE Trans. on Know. and Data Eng.*, vol. 25, no. 11, pp. 2602-2614, 2013.

[11] Dolev, D., Yao A. C., "On the security of public key protocols", *IEEE trans. On Information Theory*, vol. IT-29, no. 2, pp. 198–208, 1983

[12] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[13] D. Boneh, X. Boyen, H. shacham, "Short group signature," *Proc. Int'*Cryptology Conf. Advances in Cryptology, pp.41-55, 2004.

[14] B. den Boer, Diffie–Hellman is as strong as discrete log for certain primes in Advances in Cryptology – CRYPTO 88, Lecture Notes in Computer Science 403, Springer, p. 530, 1988.

[15] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," *Proc. Int'l Conf.* Financial Cryptography and Data Security (FC), pp.136- 149, Jan. 2010.

[16] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.