Scientific Journal Impact Factor (SJIF) : 3.518
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

Using Public Key Cryptosystem Securely Share Data to Others in Cloud Storage

Anap Rahul B[1] ,Tambe Puja M[2] , Warungase Kiran R[3], Sable Pravin S[4] , Prof. S. A. Aher.[5]
[1,2,3,4] *B.E. Students, I.T. Dept. , S.V.I.T. Nashik, India*
[5]*Asst. Prof., I.T. Dept., S.V.I.T. Nashik, India*

Abstract— Data sharing is assuming fundamental part in the distributed storage. Using distributed storage utilizer can store and allocate their information safely and productively. So information access security turns into the basic area to be engaged. Cryptography profits the information proprietor to stake the information to in harmless approach. Hence utilizer encodes information and transfers on server. Furthermore divergent encryption and decoding keys are incited for divergent information. The encryption and decoding keys might be unique for disparate arrangement of information. Simply those set of decoding keys are ordinary that the selected information can be unscrambled. As of right now a open key cryptosystems which cause a cipher text which is of steady size. In this manner to handover the decoding rules for number of cipher text. The change is one can collect a set of mystery keys and check them as minor size as a single key with holding the same ability of the considerable number of keys that are molded in a bunch.

Keywords— Cloud stockpiling, Attribute base encryption, Identity base encryption, Cloud capacity, information sharing, key total encryption**.**

I. Introduction

In current time Data sharing is a considerable usefulness in distributed storage. Case in point, bloggers can let their partner's assessment a subset of their isolated pictures; an endeavor might finance her representative's admission to a quantity of delicate information. The phrenic origination prompting difficulty is in what way we can proficiently share encoded information. Obviously clients can download the encoded information from the capacity, unscramble them, then direct them to others for sharing, yet it drops the estimation of cloud capacity. Hence the clients ought to be competent to give the entrance privileges of the sharing information to others with the goal that they can get to these information from the server unswervingly.

Distributed computing is generally increasing innovation; information can be safeguarded on cloud remotely and can have access to cosmically monstrous applications with quality housing which are shared among clients. As expansion in outsourcing of information the distributed computing obliges does the administration of information [1]. Its adaptable and cost upgrading trademark incentivizes the end utilizer and also undertakings to store the information on cloud. The insider assailment is one of security concern which's should be engaged.

Cloud Accommodation supplier need to find out whether reviews are held for clients who have physical access to the server. As cloud settlement supplier stores the information of diverse clients on same server it is conceivable that client's private information is spilled to others. The open examining arrangement of information stockpiling security in distributed computing gives a protection safeguarding examining convention [2]. It is compulsory to find out that the information uprightness without bargaining the namelessness of the information utilizer. To discover the honesty the utilizer can confirm metadata on their information, transfer and check metadata [3].

II. Literature survey

In [3] V. Goyal, O. Pandey, A. Sahai, and B. Waters develop a pristinely incipient cryptosystem for fine-grained sharing of encoded information that we incline to decision Key-Policy Attribute-Predicated secret inditing (KP-ABE). In our cryptosystem, cipher texts area unit marked with sets of attributes and personal keys area unit cognate to access structures that management that cipher texts a utilizer is yare to decode. In AN Attribute-Predicated secret inditing (ABE) system, a utilizer s keys and cipher texts area unit marked with sets of descriptive attributes and a culled key will decode a culled cipher text providing there s a match between the attributes of the cipher text and consequently the utilizer s key. The cryptosystem sanction for cryptography once a minimum of k attributes overlapped between a cipher text and a non-public key. Whereas this primitive was shown to be subsidiary for error-acceptable encryption with biometrics.

In this system every cipher text is marked by the encryptor with a group of descriptive attributes. Every private secret is cognate to AN access structure that species which marginally cipher texts the key will decode. We incline to decision such a theme a Key-Policy Attribute-Predicated secret inditing , since the access structure is per the non-public key, whereas the cipher texts area unit merely marked with a group of descriptive attributes.

In [4] M. J. Atallah, M. Blanton addresses the matter of access management and, an abundance of categorically, the key management drawback in AN access hierarchy. Informally, the overall model is that there s a group of access categories authoritatively mandated smallness partial order. a utilizer Coalesced Nation agency obtains access (i.e., a key) to an explicit category additionally can acquire access to any or all progeny categories of her category through key derivation. Our answer to the higher than drawback has the subsequent properties:

Wholly hash functions area unit utilized for a node to derive a descendant's key from its own key.

1. The house complication of the general public info is that equipollent to that of storing the hierarchy.
2. The private data at a class consists of a single key associated with that class.
3. Revocations are handled locally in the hierarchy
4. The scheme is probably safe against collusion

In [5] endeavor to alleviate the issue of constructing a secure and forfended system of cloud storage which fortifies active and even capricious users and data province. The above mentioned utilizable and sought-after attributes & properties is not offered by the antecedent system as it is predicated on certain constructions. Consequentiality is of the fact that, active utilizer is unsupported. The utilization of public cloud infrastructure introduces paramount security and privacy jeopardies. Techniques for data encrypting can be used when there is a case of confidential data. It is unnecessary for the cloud client endeavoring to implement data control to let the cloud server ken the identity or data of the users. In some measure, the manner and extent to which there is such interactive shares on the web is due to the marginally pseudo perception of a sense of anonymity.

The drawback can be that ideal and faultless privileges of secrecy and anonymity might be invective by users with the wrong intentions. This illustrates the equal necessity to hold up data attribution, particularly, to keep restrictive and accurate records of the personnel performing any operation on the data stored in a cloud. The given four aspects inspect the limited problems involved in the relations and dealings of these two cryptographic primitives as well as add to the research of safe cloud storage systems:

1. Survey of Cryptographic Toolkits and a General System Diagram.
2. Invalidation in Group Signatures.
3. Dynamic Broadcast Encoding.
4. Linkage between Group Signatures and Broadcast Encoding.

In [6] D. Boneh constructs an efficient aggregate sign from a recent short sign scheme. Aggregate signs are subsidiary for lowering the size of corticated chains and for lowering message size in safe routing protocols such as SBGP. We additionally view those aggregate signatures give elevate to variably encrypted signatures. Such signatures empowers the viewer to test that a given cipher text C is the encryption of a signature on a given message M.iii Proposed method

III. PROPOSED SYSTEM

We are investigating data sharing problem in Cloud Storage. Our focus is on fulfilling Data Sharing requirements of applications in storage. For solving this problem we are going to propose a special type of public key encryption, which we call key aggregate cryptosystem (KAC). In KAC the decryption key size and cipher text size are constant. There is limitation of file size for storage in cloud. The performance of retrieval is slow. Decryption key is not Constant-size, less secure to Attack. To solve the problem of key management and key sharing Increase the storage Capacity. Our main goal is to solve data sharing problem in cloud storage and performance of retrieval should be fast. It should be more secure to attack and increase the storage Capacity of data. To show how securely, efficiently, and flexibly share data with others in cloud storage. Solve the problem of key management and key sharing.

A. Proposed System Architecture:

Figure 1: Proposed System Architecture.

B. Framework

The substratum of the key-aggregate encryption scheme consists of five polynomial-time algorithms, which are shown below: Setup ascertains that the owner of the data can construct the public system stricture or parameter. KeyGen, as the denomination suggests engenders a public/master secret key pair. By utilizing this public and master-secret key cipher text class index he can convert plain text into cipher text with the avail of Encrypt. Utilizing Extraction, the master-secret can be utilized to engender an aggregate decryption key for a set of cipher text classes. These engendered keys can be securely conveyed to the appointees by

utilization of secure mechanisms with opportune security measures adhered to. If and only if the cipher text's class index is enclosed in the single key, then every utilizer with an aggregate key can decode the given cipher text provided by the utilization of Decrypt

C. Proposed System Algorithm

1. Setup: Setup ascertains that the owner of the data can build the public system stricture or parameter he engender account on cloud. After entering the input, the total of cipher text classes n and a security level parameter 1, the public system parameter is given as output, which customarily discarded from the input of other algorithms for the purport of conciseness.

2. KeyGen: it is for engenderment of public or master key secret pair.

3. Encrypt: run any person who want to convert plaintext into cipher text with the avail of public and master-secret key

4. Extract: Give input as master secret key and S indices of distinct cipher text class it engender output aggregate key. This is done by executing extract by the information owner himself. The output is shown as the aggregate key represented by Ks, when the input is entered in the form the set S of indices relating to the sundry classes and master secret key mask

5. Decrypt: When an appointee receives aggregate key Ks as exhibited by the anterior step, it can execute Decrypt. The decrypted pristine message m is shown on entering Ks, S, i, and C, if and only if I belongs to the set S.

IV. RESULT ANALYSIS

Results of conventional methods and proposed method are discussed here. A comparison of the number of generated keys according to respective delegation ratios between three methods is depicted in Figure 1.

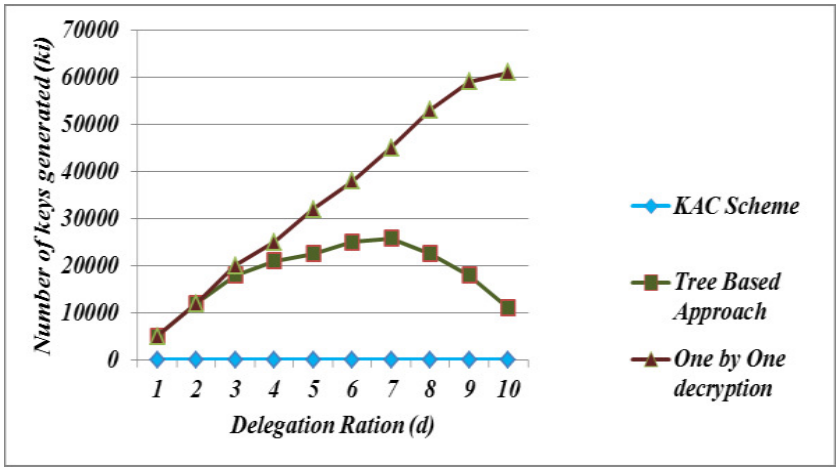

Figure 2 : Comparison of KAC with the Existing Methods

One-to-One decryption Method is represented by brown colored line and Tree Based Method is represented by the green curve line. Proposed system is shown by blue horizontal line. Graph symbolize that

if we generate the key one by one, the number of generated keys would be exactly equal to the number of the represented cipher text classes. According to the delegation ratio as shown in the graph Tree-based structure prevents a number of generated keys. In contradiction with this, our proposed framework, aggregate keys number remains constant. With the help of fixed size aggregate key, the delegation of decryption can be efficiently implemented.. In this experiment, the delegation is randomly chosen. It covers the condition that the needs for delegating to various users may be unpredictable as time goes by, even after a careful initial planning. In all above cases Hierarchical key assignment doesn't saved much. However the proposed system saves great extent overhead of key management.

V. Conclusion

Sharing of data in cloud is always hard in the cloud. For this reason the Key Aggregate Cryptosystem (KAC) is implemented which makes available the constant size aggregate secret key regardless of number of cipher text classes. This not only enhances user privacy and confidentiality of knowledge in cloud storage, but it does this by supporting the distribution or appointing of secret keys for varied cipher text classes and generating keys by various derivation of cipher text category properties of the data and its related keys. This summarizes up the scope of our paper. As there number of cipher text classes in advance coupled with exponential growth in the number of cipher texts in cloud storage, there is a need for reservation of cipher text classes for future use. As for potential changes and improvement to our current cause, in future, the parameter size is often altered particularly such that it is independent of maximum number of cipher text classes.

VI. Acknowledgement

A dissertation of this magnitude has been a journey with various ups and downs. Whenever We are standing on most difficult step of the dream of our life, We often remember the great almighty god for his blessings kind help and he always helps us in tracking off the problems by some means on our lifetime. We feel great pleasure to represent this project entailed data sharing in cloud storage by using key public key cryptosystem. We would like to convey sincere gratitude to our project guide and head of information technology engineering department Prof. S.A Aher for her valuable guidance and support and who guided us and provided with her useful and valuable suggestions and without her kind co-operation it would have been extremely difficult for us to complete this dissertion. We would like to convey sincere gratitude to B.E. Co-cordinator Prof. R.S. Bhalerao for his valuable guidance and support. We would like to express our appreciation and thanks to Prof .Dr. G. B. Shinde, Principal, S.V.I.T. Nashik.
Finally we are very grateful to inspiring parents who loving and caring support contributes a major share in completion of our task.

References

[1] key –Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, *Senior Member, IEEE*

[2] C Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy- Preserving Public Auditing for Secure Cloud Storage," *IEEE Trans.Computers*, vol. 62, no. 2, pp. 362–375, 2013

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute Based Encryption for Fine-Grained Access Control of Encrypted data,"in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*. ACM, 2006, pp. 89–98.

[4] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," *ACMTransactions on Information and System Security (TISSEC)*, vol. 12,no. 3, 2009.

[5] S. S. M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R. H. Deng,"Dynamic Secure Cloud Storage with Provenance," in *Cryptography and Security: From Theory to Applications – Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday*, ser. LNCS, vol. 6805. Springer, 2012, pp. 442–464.

[6] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," in *Proceedings of Advances in Cryptology - EUROCRYPT '03*, ser. LNCS,vol. 2656. Springer, 2003, pp. 416–432.

[7] S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, "SPICE - Simple Privacy-Preserving Identity-Management for Cloud Environment," in *Applied Cryptography and Network Security – ACNS 2012*, ser. LNCS, vol. 7341. Springer, 2012, pp. 526–543.

[8] L. Hardesty, "Secure computers aren't so secure," MIT press, 2009,http://www.physorg.com/news176107396.html

[9] B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," in *International Conference on Distributed Computing Systems - ICDCS 2013*. IEEE, 2013.

[10] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," in *Proceedings of ACM Workshop on Cloud Computing Security (CCSW '09)*. ACM, 2009, pp. 103–114.