ISSN 2395-1621

A Combined Cloud Architecture for Prevention of Duplication and Anonymous User Authentication

[#1]Aarti V Suvase, [#2]Prachi V Raut, [#3]Neha K Malvadkar, [#4]Monali V Patil

[#1234]Computer Engineering, Savitribai Phule Pune University, Dr D.Y Patil College of Engineering,Pune

ABSTRACT

Now a day's Cloud Computing is a arising technique so long as exciting countryside for the services over the framework of internet and clients are big business with cloud for delicate information. Cloud has a very challenging task of server management in terms of safety and the access control mechanisms. Thus, When clients call for data the cloud server grieves with the giving out overhead for the Key Distribution and data administration when a progress of acceptable grained access control and the scaling factor must be well enough. The concern like is to maintain scalability, fine graininess of access control mechanisms as well as information confidentiality at the same stage on the risk of ambiguity. System provides the access strategies and then offers the permission to data owner and modifier to untrusted cloud sever by maintaining the security and encryption of data. This can be overcome by taking combination of key policy and attribute Based Encryption (KP-ABE). The proposed system also removes the duplicate copies of data and this technique is stated as Data Deduplication. This data compression technique widely used in cloud storage to improve the space and bandwidth of cloud.

ARTICLE INFO

Article History

Received :15th April 2016

Received in revised form :

17th April 2016

Accepted : 19th April 2016

Published online :

23rd April 2016

Keywords— Cloud Storage, Access control, Key Distribution Centre, Attribute Based Encryption, Data Deduplication.

I. INTRODUCTION

Wireless communication has announced its arrival on big stage and the world is going mobile. We want to control everything and without moving an inch. This remote control of appliances is possible through Embedded In today's world of internet Cloud computing is growing standard in service area over the Internet. Cloud computing offers hiding policies and the virtualized policies for the data over the internet.[1]. Clients can use the cloud computing for the storage of data to server using the internet and store data on the server is highly sensitive and quick to respond. for e.g. Different application for social networks and students records .For this the high level security and the privacy is needed for the data over cloud computing.

Firstly, the client should verify the cloud that it should not be interfaced with the farm out data before starting his communications over the internet. Hence, there is need of privacy to avoid the proof of identity of the clients from cloud or other client [5].The data which is subcontracted is the check of the cloud over the internet, and the cloud is only answerable for the facility it provides to the client. The validity of the client who stores the data is also confirmed. By using the phenomenon of the Access control the permission is given to those clients having the authorization to access. A large information of different tenders can be keep back over the cloud .In the application of public networking where the client stores the personal data, the Access control plays the very vital role to give the own access to specific client.

The deduplication comparison technique is used to take away the significant duplicated data, over the stored data in cloud [6],due to this the storage space and the bandwidth of cloud can be compact. The defence of the secrecy of receptive data and prevention of duplication is through convergent encryption. Differential privileges of

clients are deliberated in replica check besides the data itself. The enhanced data transfer and the data storage consumption will reduce the number of bytes that must be transfer are achieved by via the defined method.

II. EXISTING S YSTEM

In general alive work centred control in cloud on access is centralized. All systems used ABE and there is no requirement of authentication because the key which used is symmetric in nature. A single key distribution centre (KDC) where secret keys and attributes are circulated to all clients is used by authors for centralized approach. Data deduplication of solidity also advantageous in the cloud storage to minimize the storage space and save bandwidth. For firmly accomplishment of duplicate confirming with inconsistency privileges the classified cloud is been involved to permit data clients at proxy in deduplication of data structure.

A. Disadvantages of Existing System:

- Existing system makes use of asymmetric key approach which does not beneficial for authentication.
- As the large number of clients are keep nearby by the cloud environment it difficult to maintain.
- While providing the confidentiality to the data is incompatible with data deduplication is said to be traditional encryption.
- The analogous data replicas of not the same clients will lead to different encrypted texts, making deduplication difficult

III. PROPOSED SYSTEM

This system sorts the first effort to report the difficulty of deduplication of data [1], will contribute better data safety. It recommended to the system that checks the rationality of the sequences without understanding the client's identification before storing the data. In this strategy, it also contain characteristic of access control in which only answerable clients are able to decode the kept information.

It also ignored the replay attacks and maintains the formation reworked copy, and assessment of data stored in the cloud .This System offered a fully distributed ABE where clients could have one or more than one attributes from each precise. In this to avoid this issue, the decoding job to an exchanging the server, so that the client can calculate with smallest resources.

In KP-ABE, [2] information is linked with attributes for each of which a public key part is described. The encryption authority associates the set of attributes to the message by scrambling it with the evaluating public key parts.

Client is assured for an access structure which is usually symbolized as an access tree i.e. within centres of the access tree are control doors and leaf hubs are attached with attributes. Client secret key is caused to reoccurrence the access structure so the client has the ability to decrypt a cryptograph-text if the information attributes accomplish his access structure.

The convergent encryption technique has been proposed to encrypt the data before positioning. The problem of authorized data deduplication is introduced in the proposed system to have better security. Different privileges of clients are considered in replica check. This structure represents new deduplication satisfying recognized duplicate check in mutual cloud. The structure is secure in crucial of the definitions specified in the proposed security model.[5] It put on a model of this proposed authorized replica check .

IV. MATHEMATICAL MODEL

Identities are mapped by Map e: G X G=GT This map satisfies following properties

1. $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G$ and $a, b \in \mathbb{Z}_q$, $\mathbb{Z}_q = \{0, 1, 2, \ldots, q-1\}$.
2. Nondegenerate: $e(g, g) \neq 1$.

To generate secret keys for user j SHA-1 hash function is used and represented as:

$$SK[j] = \{\alpha_i, y_i, i \in L_j\}.$$

The public key of KDC is published as

$$PK[j] = \{e(g, g)^{\alpha_i}, g^{y_i}, i \in L_j\}.$$

set of attributes from KDC are used to generate secret keys as

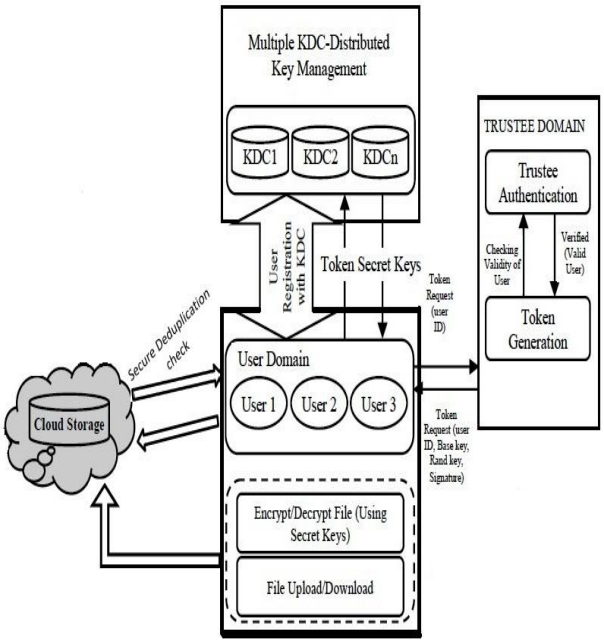
$$sk_{i,u} = g^{\alpha_i} H(u)^{y_i},$$

Decryption process as

a. For each $x \in X'$, $dec(x) = \frac{C_{1,x} e(H(u), C_{3,x})}{e(sk_{\pi(x),u}, C_{2,x})}$.

b. U_u computes $MSG = C_0 / \Pi_{x \in X'} dec(x)$.

V. SYSTEM ARCHITECTURE



VI. RESULT ANALYSIS

The results represented here are partial. The following results are for the access control mechanism.

A. Analysis Based on Access Control

The client can able to take decision that which client can access clients data, and which client can only read the data rather can modify it and write back. There are 2 types of access policies, the only read policy permits client to only read the file and can only downloads the file. Client cant make any changes through it

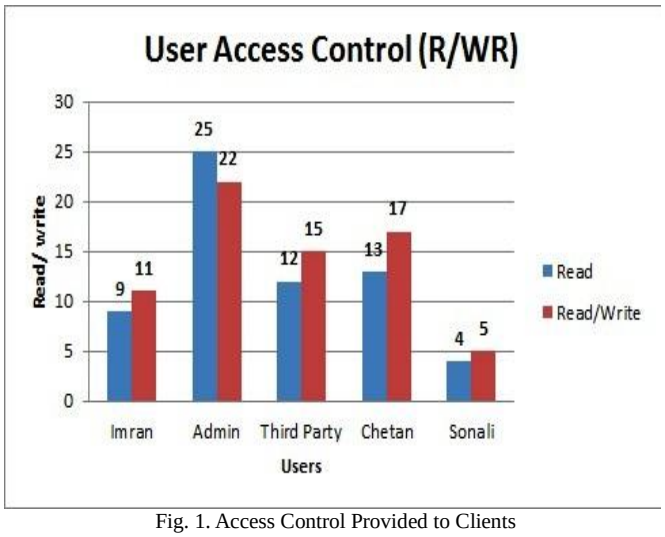


Fig. 1. Access Control Provided to Clients

B. Analysis based on file size

As per the cloud storage the number of client are able to upload or download a file, there may be variations in time required to upload and download. Partially the system is decentralized in nature.

C. Analysis based on the Key encryption and decryption

The system performs the encryption and decryption stored on cloud, so that the cloud must not pretend the contents.The key distribution centre provides the necessary keys with time effective manner

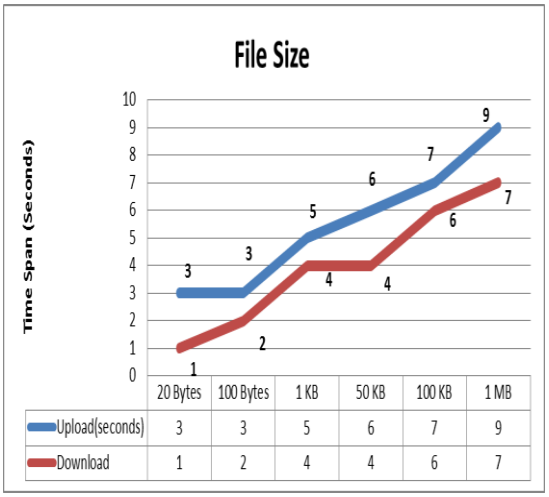


Fig.2 Upload/Download time based on file size

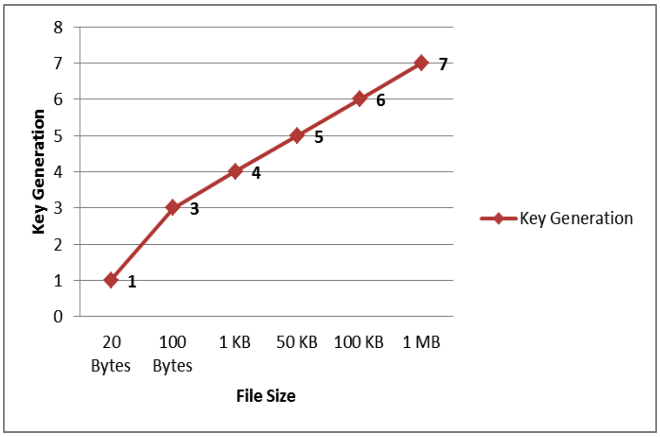


Fig.3 Encryption/Decryption time based on file size

VII. CONCLUSION

The proposed system gives a Hybrid access control technique with unknown authentication, which provides client revocation and prevents replay attacks. The cloud does not know the individuality of the client who stores information, but only verifies the clients important data. Key distribution is done in a hybrid way. In future, it hides the attributes and access policy of a client. Here further more it given many new deduplication constructions supporting approved duplicate sign up hybrid cloud design, during which the duplicate check tokens of files as generated by the personal cloud server with personal keys. Refuge analysis demonstrates that our scheme is vulnerable in terms of business executive and outsider attacks lay out in the planned security model.

.

ACKNOWLEDGEMENT

The authors are thankful to researches, publishers. For making the availability of their resources and publications. Teacher's guidance is equally responsible for this paper. This Work was supported by "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds" by the Sushmita Ruj, Amiya Nayak.And also by the Research of "A Hybrid Cloud Approch for Secure Authorized Deduplication" under the Jin LiWenjing Lou

REFRENCES

[1] Sushmita Ruj, Milos Stojmenovic, and Amiya Nayak, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014

[2] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance," IACR Cryptology ePrint Archive, 2008.

[3] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the Decryption of ABECiphertexts," Proc. USENIX Security Symp., 2011.

[4] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," in *CloudCom*, ser. Lecture Notes in Computer Science, vol.5931. Springer, pp. 157–166, 2009.

[5] S. Ruj, M. Stojmenovic and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", *IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, pp. 556–563, 2012.

[6] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *IEEE INFOCOM*. , pp.441–445, 2010.

[7]S.Yu,C.Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *ACM ASIACCS*, *pp. 261–270, 2010.*

[8] W. K. Ng, Y. Wen, and H. Zhu. Private data deduplication protocols in cloud storage. In S. Ossowski and P. Lecca, editors, *Proceedings of the 27th Annual ACM Symposium on Applied Computing*, Pages 441–446. ACM, 2012.

[9] Jin Li, Yan Kit Li, Xiaofeng Chen, PatricP. C. Lee, Wenjing Lou,"A Hybrid Cloud Approach for Secure Authorized Deduplication",IEEE Transactions on Parallel and Distributed Systems, 2014.

[10] M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf.Computer and Comm. Security,

[11]C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, "Toward Secure and Dependable Storage pp. 121-130, 2009.Services in Cloud Computing", *IEEE T. Services Computing*, vol.5, no. 2, pp. 220–232, 2012.

