Robust Public Storage with Heterogeneous Framework

Prakash H. Unki[1], Sana M. Sangtrash[2]

[1]Associate Professor, Department of Computer Science and Engineering, BLDEA's V.P.Dr.P.G.Halakatti College of Engineering & Technology,Vijayapur, Karnataka, India
[2]M.Tech Student, Department of Computer Science and Engineering, BLDEA's V.P.Dr.P.G.Halakatti College of Engineering & Technology, Vijayapur, Karnataka, India

ABSTRACT

To get secured and flexible cloud storage with data access control the CP-ABE scheme is used. But in CP-ABE one authority is used to verify legal users and distribution of keys which becomes an issue when used for large storage in cloud and which results in time consuming for the users as they have to wait for the secret key. But techniques with multiple authority were also proposed but in vain as they could not deal with the issues and were less efficient. Therefore a miscellaneous framework was introduced to deal with issues of single authorities and least efficiency. The introduced framework is more efficient and provides easy access control which also has a method known as auditing to deal with the illegal users and attackers. This framework uses multi authorities for verification of legal users but to deal with illegal users cross verification is done by the central authority i.e. CA. Every user and AA has unique identity which helps in verification and ensures security. Security and performance analysis proves that the introduced framework is efficient and better than the other existing techniques and also improves the performance of key generation.

Keyword: Multiple authorities, CP-ABE, Cloud storage.

1. INTRODUCTION

Cloud storage is an optimistic and significant resource in cloud computing[1–4]. Higher intelligibility, greater security and accuracy, fast implementation and great safety are the few advantages of cloud storage. Although the advantages listed above there are new challenging issues such as data access control and data security.

Cloud service providers operate cloud storage and they are not considered under trustworthy data provider, in the cloud storage old methods are not suited in the client or server. In the cloud storage, control to access data is a challenge. To overcome this control of access of data challenge in storage of cloud, few techniques were introduced where the best algorithm is ciphertext policy attribute based encryption (CP-ABE). One of the best advantage of this CP-ABE technique is it provides straight control based on policy to access for the data owners, to grant easy and safe control of access for storage system of cloud. In CP-ABE technique, cryptography method is used for control of access, in cryptography the files data of the data provider is encrypted using attributes to get access structure, and this attributes by the user are assigned for secret key. The user can decrypt the ciphertext into plaintext only when the set of attributes of users secret key matches the access. The two categories single authority [5]–[9], and multiple authority [10] of CP-ABE based control of access techniques for cloud storage. Despite the already available CP-ABE techniques control of access have many good characteristics, which are not either robust or efficient in generation of key. In charge authority of all attributes is only one which will make all available secret key request unavailable at the required time. Same issue arises when multi-authority techniques are used, because a disjoint attribute set is managed by each of multiple authorities.

2. LITERATURE SURVEY

P. Mell and T. Grance [1]., proposed the explanation from NIST that describes essential characteristics of cloud computing and is destined to give cloud services with vast comparison and implementation methods, and to provide basics for the discussion of cloud computing and its best usage.

Z. Fu *et al.*[2] proposed for the first time, studies and solution for the issues of a search for customized multiple keyword over encrypted data while protecting seclusion in cloud computing. To achieve user interested model for each user, semantic ontology WordNet is used to adapt the mechanism to smartly express user's interests.

X. Sun *et al.*[3] introduced an creative search for semantic technique based on the hierarchical and semantic relation concepts and also between the concepts of the datasets encrypted. This technique particularly indexes

 DOI : 10.18231/2454-9150.2018.0224 © 2018, IJREAM All Rights Reserved.

document and also based on hierarchical concepts trapdoors are build. A structure of tree based on index is utilized to assemble all of the index vector documents for improvement in search efficiency.

K. Xue and P. Hong [4] proposed secured framework for public cloud for group sharing, which efficiently take benefits with the help of server of cloud and no private data is accessible for the data provider and attackers of cloud. Framework is used to form a protocol which consists of signature and re-encryption of proxy and enhancement of *TGDH*. The leader of group efficiently provides priorities to multiple selected group members of group management by applying the proxy signature schemes. Cloud servers are used to help the enhanced *TGDH* technique negotiation enables the group and pair of group key are updated, it's not required for all available group members to be online all the time. The sensitive information is not exposed to cloud servers and encryption is adopted and the operations of computation are assigned.

Y. Wu *et al.* [5] introduced a novel MCP- ABE scheme and rather than explicit consumer names list data consumers are used to employ the MCP-ABE for sharing scalable media to design an control of access technique. The ciphertext can decrypt only when the access policy matches the attributes of users makes a content provider specifies an access policy and have one ciphertext encrypted with multiple messages which is allowed by MCP-ABE which makes the scheme efficient and flexible.

3. OBJECTIVE

The important features of the system proposed are as followed.

1) To overcome the problem of single point performance in the existing technique which is a bottleneck of key distribution a heterogeneous framework is introduced for public cloud storage with one CA (Central Authority) and many AAs (Attribute Authorities) which is efficient and robust. Multiple AAs are used to handle the heavy load to verify the user legitimacy and each of each multiple AAs verify the user legitimacy independently and universal attribute set are managed and computational tasks is handled by CA. For cloud storage, the bottleneck is single point performance and less efficient which is addressed by this proposed technique framework.

2) The existing technique CP-ABE is constructed again to be compatible with the introduced technique framework which is robust and highly efficient and also contains the features of CP-ABE i.e. fine granularity, flexible and secured.

The proposed technique contains a mechanism of auditing which support the system to track AA's behavior based on legal users verification.

4. SYSTEM ARCHITECTURE

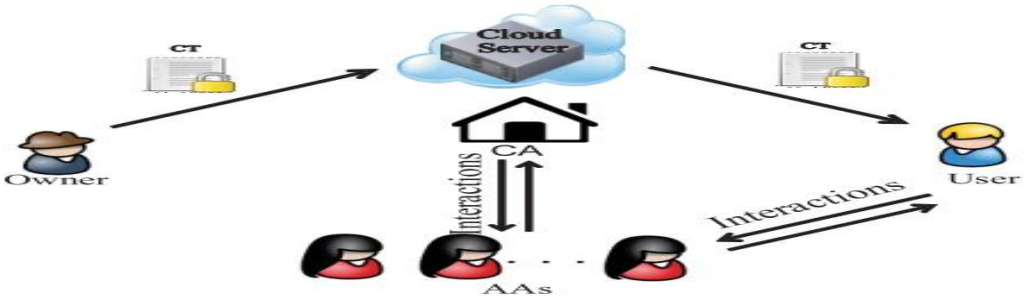

Fig:1 System architecture

Fig:1 shows the architecture of the system which contains 5 modules i.e. data providers, data consumers, CA, AAs and public cloud. The central authority (CA) of the system is the admin of the system. The responsibilities of attribute authorities i.e. AAs are to verify the user legitimacy performance and for verified legitimacy users generate intermediate keys. The responsibility of the data owner is to provide access policy to each file which defines who all can access that file, and based on policies defined the file is encrypted. CA assigns identity to the data consumer i.e. User globally. Every user has a attribute set which associates with secret key. A platform which is publically available to store the data is known as cloud server. For owners, data access control is not done by cloud server.

CONCLUSION

To overcome the issues of existing CP-ABE technique a framework is introduced known as RAAC. The RAAC is more efficient and robust and uses multiple AAs with single CA. Whenever user request for decryption, the AA

 DOI : 10.18231/2454-9150.2018.0224 © 2018, IJREAM All Rights Reserved.

verifies the legal user and then serves the users but AA cannot be trustworthy, to deal with this issue a procedure known as auditing and tracing is introduced. This procedure is used to know the misbehavior of AA. To verify the system efficiency and security analysis of performance and security is made which proved that the system is efficient to illegal user and attackers and also the cloud server. Due to the tracing method AA cannot reject the key distribution of misbehavior. Finally, the analysis of performance proved that the introduced system is better than the existing systems.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 800-145, 2011.

[2] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 9, pp. 2546–2559, Sep. 2016.

[3] Z. Fu, X. Sun, S. Ji, and G. Xie, "Towards efficient content-aware search over encrypted outsourced data in cloud," in Proc. IEEE Conf. Comput. Commun. (INFOCOM), Apr. 2016, pp. 1–9.

[4] K. Xue and P. Hong, "A dynamic secure group sharing framework in public cloud computing," IEEE Trans. Cloud Comput., vol. 2, no. 4, pp. 459–470, Oct. 2014.

[5] Y. Wu, Z. Wei, and R. H. Deng, "Attribute-based access to scalable media in cloud-assisted content sharing networks," IEEE Trans. Multimedia, vol. 15, no. 4, pp. 778–788, Jun. 2013.

[6] J. Hur, "Improving security and efficiency in attribute-based data sharing," IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271–2282, Oct. 2013.

[7] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214–1221, Jul. 2011.

[8] J. Hong, K. Xue, W. Li, and Y. Xue, "TAFC: Time and attribute factors combined access control on time-sensitive data in public cloud," in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2015, pp. 1–6.

[9] Y. Xue, J. Hong, W. Li, K. Xue, and P. Hong, "LABAC: A locationaware attribute-based access control scheme for cloud storage," in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2016, pp. 1–6.

[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Advances in Cryptology—EUROCRYPT. Berlin, Germany: Springer, 2011, pp. 568–588.

[11] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Secur. Privacy (S&P), May 2007, pp. 321–334.

 DOI : 10.18231/2454-9150.2018.0224 © 2018, IJREAM All Rights Reserved.