© 2018 IJSRSET | Volume 4 | Issue 8 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Robust Public Storage with Heterogeneous Framework

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

[1]Associate Professor, BLDEA'S College of Engineering and Technology, Vijayapur, Karnataka, India

[2]Student, BLDEA'S College of Engineering and Technology, Vijayapur, Karnataka, India

ABSTRACT

Cloud storage with flexibility and security can be obtained by the CP-ABE algorithm for data access and control. In CP-ABE valid users are verified by one authority which leads to time consuming process. Other algorithms with more than one authority are introduced but could not overcome the issue. A heterogeneous framework was introduced to overcome issues of CP-ABE. Auditing is used for the malicious user and attacker. Central authority CA verifies the valid user for security using multiple authorities. The proposed framework is efficient and secured along with performance improvement.

Keywords: CP-ABE, Cloud Storage, CA, AA

I. INTRODUCTION

Cloud storage is an positive and important service in cloud computing[1–4]. There are many advantages of cloud storage but it even has some new issues to deal with such as security and access control. The service provider of cloud cannot be trusted and to deal with data access control many schemes were proposed among which CP-ABE is better. This scheme gives data access control which is safe and secured. Cryptography encrypts the data using user provided attributes to generate secret key. Ciphertext uses these attributes for decryption and generates the decrypted data for the user. Two types of schemes are used i.e. single and multiple authorities. The CP-ABE has some issues related to key generation i.e. efficiency and robust. Even using multiple authorities cannot solve this issue and hence the RAAC scheme is introduced.

II. LITERATURE SURVEY

P. Mell and T. Grance [1]., introduced the description of cloud computing from NIST which provides the features and support of cloud computing along with the advantages of cloud computing.

Z. Fu *et al.*[2] introduced study and solution to the issues in search of multiple keyword and providing protection in cloud computing. To provide user interest WordNet, semantic ontology are used

X. Sun *et al.*[3] proposed an innovative semantic algorithm for semantic relationship and encryption of dataset. The proposed algorithm build trapdoor and generates tree structure for efficiency and vector documents.

K. Xue and P. Hong [4] proposed a framework to public group share with efficient cloud server and data is private hence not available for the providers and attackers. A rule is formed using signature ads proxy encryption. This proxy signature provides priorities efficiently by the group member and manages it. The cloud server enhances the technique, not necessary to be online always and data is private.

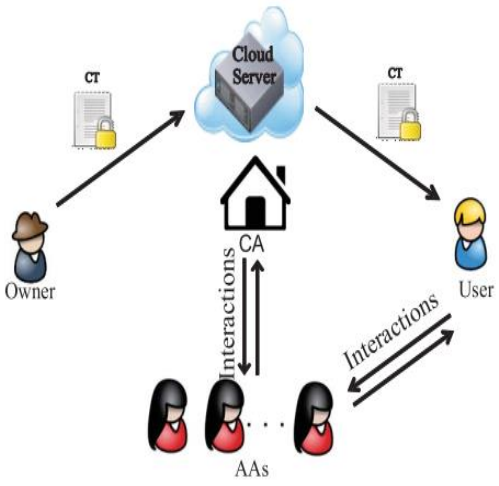
Y. Wu *et al.* [5] proposed MCP-ABE algorithm and data access control is done by scalable media. Encryption using many attributes makes the algorithm efficient and flexible, the decryption can be done when the attributes are matched.

III.OBJECTIVE

The salient features of the proposed system are:

1. The issues of existing algorithms related to key generation are handled in the proposed framework which uses Central Authority and multiple Attribute Authorities for robust and efficiency. The multiple AAs verify the valid user separately and deal with the huge workload and the CA deals with the attribute set. The proposed system deals with the issues in existing system and overcome the issues.
2. The proposed algorithm also contains the feature of existing system such as CP-ABE. Hence makes the proposed system robust and flexible.

IV. SYSTEM ARCHITECTURE



The above figure shows the architecture of the system, the modules included are data providers and consumers, CA, AAs and public cloud. The admin of the system is CA. 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.

V. CONCLUSION

The issues in the existing system are handled in the proposed algorithm. The proposed algorithm uses one central authority and multiple AA which makes the system more reliable. Every user requests AA to get the secret key and AA request CA. The AAs and CA verifies the valid user. This issue is solved using a technique called auditing which traces the misbehavior of AA and invalid user. The analysis shows the proposed system is better and efficient than other existing systems.

VI.REFERENCES

[1] M. Young, *The Techincal Writers Handbook.* Mill Valley, CA: University Science, 1989.

[2] J. U. Duncombe, “Infrared navigation—Part I: An assessment of feasibility (Periodical style),” *IJREAM Trans. Electron Devices*, vol. ED-11, pp. 34–39, Jan. 1959.

[3] S. Chen, B. Mulgrew, and P. M. Grant, “A clustering technique for digital communications channel equalization using radial basis function networks,” *IJREAM Trans. Neural Networks*, vol. 4, pp. 570–578, Jul. 1993.

[4] R. W. Lucky, “Automatic equalization for digital communication,” *Bell Syst. Tech. J.*, vol. 44, no. 4, pp. 547–588, Apr. 1965.

[5] S. P. Bingulac, “On the compatibility of adaptive controllers (Published Conference Proceedings style),” in *Proc. 4th Annu. Allerton Conf.*

Circuits and Systems Theory, New York, 1994, pp. 8–16.

[6] G. R. Faulhaber, "Design of service systems with priority reservation," in *Conf. Rec. 1995 IJREAM Int. Conf. Communications,* pp. 3–8.

[7] W. D. Doyle, "Magnetization reversal in films with biaxial anisotropy," in *1987 Proc. INTERMAG Conf.*, pp. 2.2-1–2.2-6.

[8] G. W. Juette and L. E. Zeffanella, "Radio noise currents n short sections on bundle conductors (Presented Conference Paper style)," presented at the IJREAM Summer power Meeting, Dallas, TX, Jun. 22–27, 1990, Paper 90 SM 690-0 PWRS.

[9] J. G. Kreifeldt, "An analysis of surface-detected EMG as an amplitude-modulated noise," presented at the 1989 Int. Conf. Medicine and Biological Engineering, Chicago, IL.

[10] J. Williams, "Narrow-band analyzer (Thesis or Dissertation style)," Ph.D. dissertation, Dept. Elect. Eng., Harvard Univ., Cambridge, MA, 1993.