IJRRECS/April 2016/Volume-4/Issue-4/5445-5449 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN EFFECTIVE APPROACH FOR MANAGING PRIVILEGES OF ACCESSING CLOUD DATA

Padmala Saidesh Kumar[1]

[1]Dept of CSE, University of Hyderabad, Hyderabad, T.S, India

ABSTRACT:

The expertise of cloud computing has attracted much attention from academia as well as industry because of profitability; on the other hand it has several challenges. In our work we recommend an efficient method for permitting cloud servers to mange user access privileges devoid of knowing their identity data. The proposed system is a semi-anonymous privilege control proposal for managing of not only data privacy, but moreover user identity privacy within traditional methods of access control. This technique decentralizes central authority to limit the leakage of identity and hence attains semi-anonymity. In addition, it moreover generalizes file access control for privilege control, by which privileges of the entire operations above the system of cloud data re managed within fine-grained manner.

Keywords: Cloud computing, Fine grained, Semi-anonymous, Data privacy, central authority, Privileges.

1. INTRODUCTION:

Many techniques were proposed to keep data contents privacy by the use of access control. Identity-based encryption was initially introduced where the message sender specifies an identity so that only receiver by means of matching identity decrypts it. Later the fuzzy Identity-based encryption was proposed, known as Attribute-Based Encryption. And later many tree-based methods of Attribute-Based Encryption, Key-Policy based encryption

and cipher text-policy based encryption were introduced to state more general form than effortless overlap. In the Key-Policy based encryption a cipher-text is linked by means of a set of attributes, and private key is connected by a monotonic access structure similar to a tree, which explains user identity. In the cipher text-policy based encryption, cipher-texts are formed by means of an access structure, which identify encryption policy, and generate private keys in relation to users' attributes. Different from data privacy, less effort is paid for protecting privacy of user identity during interactive procedures [1]. User identity, which is described by means of their attributes, is disclosed towards key issuers, and issuers will issue private keys in relation to their attributes. However it seems normal that users are eager to maintain their identity secret while they still obtain their private keys. Hence in our work we recommend AnonyControl for permitting cloud servers to mange user access privileges devoid of knowing their identity data. The proposed system is a semi-anonymous privilege control proposal for managing of not only data privacy, but moreover user identity privacy within traditional methods of access control. Proposed scheme is semi-anonymous as partial identity information is revealed to each of the authority, but we can attain full-anonymity and moreover permit collusion of authorities. The proposed method decentralizes central authority to limit the leakage of identity and hence attains semi-anonymity. Besides, it moreover generalizes file access control for privilege control, by which privileges of the entire operations above the system of cloud data re managed within fine-grained manner.

2. METHODOLOGY:

Cloud computing technology gives flexible, economical use of computing resources. But the data is outsourced towards some of the cloud servers, and a variety of privacy concerns come out from it. The technology of cloud computing has attracted much attention from academia as well as industry because of profitability; however it moreover has three challenges that should be managed. Firstly, data confidentiality must be assured. The data privacy is not only concerning data contents. As the most attractive part of cloud computing is computation outsourcing, it is far enough to just carry out an access control. Secondly, personal data is at risk as one's identity is genuine based on his data for intention of

access control. While people are more concerned regarding their identity privacy, the identity privacy moreover needs to be managed previous to cloud entering our life. Finally cloud computing system has to be resilient in the situation of security breach where some part of system is compromised by means of attackers. We recommend semi-anonymous privilege control proposal for permitting cloud servers to mange user access privileges devoid of knowing their identity data. The proposed system is for managing of not only data privacy, but moreover user identity privacy within traditional methods of access control [2]. This method decentralizes central authority to limit the leakage of identity and hence attains semi-anonymity and moreover generalizes file access control for privilege control, by which privileges of the entire operations above the system of cloud data re managed within fine-grained manner. In our scheme, a number of trees are necessary in each data file to confirm user identity and to grant him advantage. The proposed schemes protect user privacy against each of the single authority. Partial information is disclosed within the proposed system and the scheme is tolerant against authority compromise.

3. AN OVERVIEW OF PROPOSED SYSTEM:

In our proposed system, there are four entities such as attribute authorities, cloud server, data owners as well as data consumers. A user might be a data owner as well as a data consumer at the same time. Authorities are assumed to contain influential computation abilities, and they are managed by means of government offices as some attributes partly contain user identifiable data. The complete attribute set is separated as N disjoint sets and managed by each of the authority, thus each authority is conscious of only component of attributes [3]. Data owner is entity who outsources encrypted data file towards cloud servers. Cloud Server is supposed to contain enough storage capacity. Newly joined consumers of data ask for private keys from entire authorities, and they do not make out which attributes are managed by which authorities. When consumers of data make a request of their private keys from authorities, authorities mutually make equivalent private key and forward it to them. The entire data consumers download encrypted data files, but only that private keys which assure privilege tree can carry out operation which is linked with the privilege. The server is

allotted to carry out a function when and only if user's credentials are verified by means of privilege tree [5]. Cloud has several challenges that should be managed such as firstly, data confidentiality must be assured; secondly, personal data is at risk as one's identity is genuine based on his data for intention of access control and finally cloud computing system has to be resilient in the situation of security breach where some part of system is compromised by means of attackers. The proposed system permits cloud servers to mange user access privileges devoid of knowing their identity data. It manages not only data privacy, but moreover user identity privacy within traditional methods of access control and decentralizes central authority to limit the leakage of identity and hence attains semi-anonymity. In our work encryption policy is explained by means of a tree known as access tree. Each of the non-leaf nodes of tree is a threshold gate, and each of the leaf nodes is explained by means of an attribute [4]. One access tree is necessary in each data file for defining of encryption policy. The proposed system generalizes file access control for privilege control, by which privileges of the entire operations above the system of cloud data re managed within fine-grained manner. The privilege in our system is described as similar to privileges that are managed in normal operating systems. In our system, a number of trees are necessary in each data file to confirm user identity and to grant him benefit accordingly. In our work we believed semi-honest authorities in the proposed system and understood that they will not collude with each other. This is an essential statement in proposed system since each of the authority is responsible of a subset of complete attributes set, and for attributes that it is responsible of and it knows precise information of key requester. When the data from the entire authorities is gathered in total, total attribute set of key requester is improved and therefore his identity is revealed to authorities [6]. Hence the proposed system is semi-anonymous as partial identity information is revealed to each of the authority, but we can attain full-anonymity and moreover permit collusion of authorities.

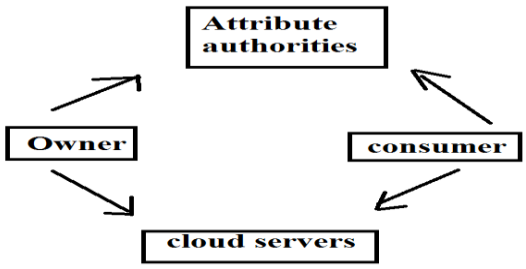

Fig1: proposed system.

4. CONCLUSION:

Most of the schemes on the basis of attribute-based encryption were proposed for securing of cloud storage. On the other hand, most of the work focuses on privacy of data contents and access control, while less consideration is paid towards privilege control as well as identity privacy. We suggest a technique for permitting cloud servers to mange user access privileges devoid of knowing their identity data. The proposed technique is a semi-anonymous privilege control proposal for managing of not only data privacy, but moreover user identity privacy within traditional methods of access control. The technique decentralizes central authority to limit the leakage of identity and hence attains semi-anonymity. It generalizes file access control for privilege control, by which privileges of the entire operations above the system of cloud data re managed within fine-grained manner. The proposed system protects user privacy against each of the single authority. Partial information is revealed within the proposed system and the scheme is tolerant against authority compromise.

REFERENCES

[1] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proc. 16th CCS, 2009, pp. 121–130.

[2] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," Inf. Sci., vol. 180, no. 13, pp. 2618–2632, 2010.

[3] V. Božovi´c, D. Socek, R. Steinwandt, and V. I. Villányi, "Multi-authority attribute-based encryption with honest-but-curious central authority," Int. J. Comput. Math., vol. 89, no. 3, pp. 268–283, 2012.

[4] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in Public-Key Cryptography. Berlin, Germany: Springer-Verlag, 2013, pp. 162–179.

[5] J. Hur, "Attribute-based secure data sharing with hidden policies in smart grid," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 11, pp. 2171–2180, Nov. 2013.

[6] Y. Zhang, X. Chen, J. Li, D. S. Wong, and H. Li, "Anonymous attributebased encryption supporting efficient decryption test," in Proc. 8th ASIACCS, 2013, pp. 511–516.