IJRRECS/January 2016/Volume-4/Issue-1/5165-5169 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

TOWARDS AN EFFECTIVE PRIVILEGE CONTROL SYSTEM FOR HANDLING PRIVACY ISSUES OF DATA

S.Komali[1], N.Vijaya Sunder Sagar[2], M.Dileep Kumar[3], Thadaka Mounika[4]

[1,3]Assistant Professor, Dept of CSE, Ashoka Institute of Engineering and Technology, Malkapur, Hyderabad, T.S, India

[2]Assistant & HOD, Dept of CSE, Ashoka Institute of Engineering and Technology, Malkapur, Hyderabad, T.S, India

[4]M.Tech Student, Dept of CSE, Ashoka Institute of Engineering and Technology, Malkapur, Hyderabad, T.S, India

ABSTRACT:

Various techniques were proposed to defend privacy of data contents by means of access control. As the interesting part of cloud computing is computation outsourcing, it is far beyond enough to carry out simply an access control. Users want to manage privileges of data management above other users. Our objective is to achieve multi-authority cipher-text basis encryption that attains security and assures privacy of consumers' identity data. We provide a semi-anonymous privilege control system to deal with the data privacy and moreover privacy of user identity in traditional methods of access control. The system will decentralize central authority to limit identity leak and consequently attain semi-anonymity and moreover the system will generalize file access control to privilege control, by which the entire operations privileges on cloud data are controlled in a fine-grained manner. It will permit cloud servers to manage privileges of user access devoid of knowing identity information and is capable to defend user's privacy against each of the single authority and only partial information is disclosed in this system. The structure is broad-minded against authority compromise, and does not bring the complete system down.

Keywords: Cloud computing, Access control, Multi-authority, Cipher-text basis encryption, Anonymous privilege, Central authority, Cloud data, Data privacy.

1. INTRODUCTION:

In the recent times, people are concerned regarding their identity privacy that moreover needs to be secluded. The cloud system has to be flexible in security breach where system is compromised by means of attackers. Identity-basis encryption was introduced in which message sender will identify an identity so that simply a receiver by means of matching identity will decrypt it. Later Attribute-basis encryption was introduced in which an identity is sighted as set of descriptive attributes, and decryption is feasible when decrypter identity have several overlaps with the specified one in cipher-text. Several methods based on attribute-based encryption were proposed to safe cloud storage. But most works spotlight on privacy of data contents privacy as well as access control, less attention was paid towards privilege control as well as identity privacy [1]. In our work, we provide a semi-anonymous privilege control system known as AnonyControl to deal with the data privacy and moreover privacy of user identity in traditional methods of access control. The proposed system will permit cloud servers to manage privileges of user access devoid of knowing identity information. The scheme will decentralize central authority to limit identity leak and consequently attain semi-anonymity and moreover the system will generalize file access control to privilege control, by which the entire operations privileges on cloud data are controlled in a fine-grained manner.

2. AN OVERVIEW OF SYSTEM REPRESENTATION:

Quite a lot of methods based on attribute-based encryption were proposed to safe cloud storage. In attribute-basis encryption, an identity is sighted as set of descriptive attributes, and decryption is feasible when decrypter identity have several overlaps with the specified one in cipher-text. In key based encryption, cipher-text is connected by means of a set of attributes, and private key is linked by means of monotonic access structure. In cipher-text basis encryption, cipher-texts are created by means of access construction that identifies encryption policy, and private keys are produced in relation to user attributes. Our objective is to attain multi-authority cipher-text basis encryption that attains security and assures privacy of consumers' identity data. Different from privacy of data, less attempt will protect user identity privacy during the protocols of interactive. User identities that

are described by means of their attributes are disclosed towards key issuers, and issue private keys in relation to their attributes however it seems normal that users maintain their identities secret while they obtain their private keys. In our work, we provide a semi-anonymous privilege control system to deal with the data privacy and moreover privacy of user identity in traditional methods of access control. The scheme will decentralize central authority to limit identity leak and consequently attain semi-anonymity and moreover the system will generalize file access control to privilege control, by which the entire operations privileges on cloud data are controlled in a fine-grained manner. The proposed system will permit cloud servers to manage privileges of user access devoid of knowing identity information [2][3]. The proposed system is capable to defend user's privacy against each of the single authority and only partial information is disclosed in this system. The system is broad-minded against authority compromise, and does not bring the complete system down. In our model, there are four entities such as Attribute authorities, data owners, cloud server as well as data consumers. A user may be owner and consumer at the same time. Authorities contain dominant computation abilities, and are managed by means of management offices since some attributes hold user identifiable information. Data owner wishes to allot encrypted data file towards cloud servers that contain enough storage capability. Newly fixed consumers request confidential keys from all of authorities, and they do not identify the type of attributes that are guarded by authorities. When consumers ask for private keys from authorities, they generate equivalent private key and forward it to them [4]. All consumers download encrypted data files, however those whose private keys assure privilege tree carry out actions connected with privilege. The server performs an operation and only when user credentials are confirmed through privilege tree.

3. AN OVERVIEW OF PROPOSED SYSTEM:

The security of numerous attribute basis encryptions schemes and ours depend on supposition that no algorithms of probabilistic polynomial time can solve decisional Diffie–Hellman assumption by non-negligible benefit. This supposition is realistic as discrete logarithm problems are extensively considered as intractable, and

groups we select are groups of cyclic multiplicative of prime order. Our goal is to attain multi-authority cipher-text basis encryption that attains security and assures privacy of consumers' identity data. In our work, policy of encryption is described by means of a tree known as access tree. The privilege in our system is described as comparable to privileges that are managed in normal operating systems. In our work, we provide a semi-anonymous privilege control system known as AnonyControl to deal with the data privacy and moreover privacy of user identity in traditional methods of access control. The scheme will decentralize central authority to limit identity leak and consequently attain semi-anonymity and moreover the system will generalize file access control to privilege control, by which the entire operations privileges on cloud data are controlled in a fine-grained manner. We have believed the semi-honest authorities in the proposed system and we imagined that they will not scheme with each and it is an essential supposition in proposed system since each of the authority is a subset of entire attributes set and it knows accurate information of key requester. The system will permit cloud servers to manage privileges of user access devoid of knowing identity information [5]. It is capable to defend user's privacy against each of the single authority and only partial information is disclosed in this system; it is broad-minded against authority compromise, and does not bring the complete system down. When information from the entire authorities is collected, total attribute set of key requester is improved and hence identity is disclosed towards authorities. The system is semi-anonymous as partial identity data is revealed towards each authority; however we can attain full-anonymity and moreover permit collusion of authorities. The important point of identity information leak is that key generator provides attribute key on basis of reported attribute, and generator should identify user attributes. A naive key is to provide the entire attribute keys of the entire attributes to key requester and allow him choose whatever he needs. In this means, key generator does not recognize the attribute keys that are picked up by key requester, but we have to completely believe key requester that he will not choose any of the attribute key not approved to him [6].

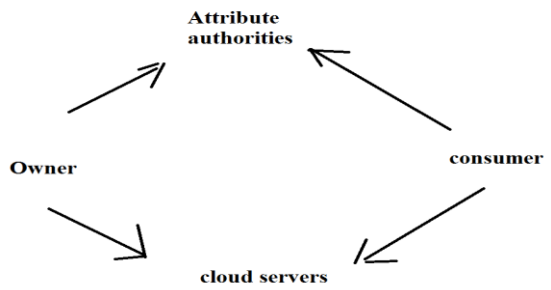

Fig1: system representation.

4. CONCLUSION:

In the technique of cloud computing, computing resources are offered dynamically by means of Internet and data storage is outsourced to some party within cloud. It attracts interests because of profitability, however also has as a minimum of three challenges to be handled. In our work, we make available a semi-anonymous privilege control system to deal with the data privacy and moreover privacy of user identity in traditional methods of access control. Our purpose is to attain multi-authority cipher-text basis encryption that attains security and assures privacy of consumers' identity data. The structure is broad-minded against authority compromise, and does not bring the complete system down. The proposal will decentralize central authority to limit identity leak and consequently attain semi-anonymity and moreover the system will generalize file access control to privilege control, by which the entire operations privileges on cloud data are controlled in a fine-grained manner. The projected arrangement will permit cloud servers to manage privileges of user access devoid of knowing identity information. The projected structure is capable to defend user's privacy against each of the single authority and only partial information is disclosed in this system.

REFERENCES

[1] V. Bo˘zovi´c, D. Socek, R. Steinwandt, and V. I. Vill´anyi, "Multiauthority attribute-based encryption with honest-but-curious central authority," IJCM, vol. 89, no. 3, pp. 268–283, 2012.

[2] F. Li, Y. Rahulamathavan, M. Rajarajan, and R.-W. Phan, "Low complexity multi-authority attribute based encryption scheme for mobile cloud computing," in SOSE. IEEE, 2013, pp. 573–577.

[3] K. Yang, X. Jia, K. Ren, and B. Zhang, "Dac-macs: Effective data access control for multi-authority cloud storage systems," in INFOCOM. IEEE, 2013, pp. 2895–2903.

[4] Z. Wan, M. Gu et al., "Hierarchical attribute-set based encryption for scalable, flexible and fine-grained access control in cloud computing," in ISPEC. Springer, 2011, pp. 98–107.

[5] A. Kapadia, P. Tsang, and S. Smith, "Attribute-based publishing with hidden credentials and hidden policies," NDSS, 2007.

[6] S. Yu, K. Ren, and W. Lou, "Attribute-based content distribution with hidden policy," in Workshop on Secure Network Protocols. IEEE, 2008.