IJRRECS/January 2016/Volume-4/Issue-1/5124-5129 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN EFFECTIVE SCHEME FOR MANAGING DATA PRIVACY IN ACCESS CONTROL SYSTEM

M.Anil Kumar Yadav[1], B.V.Seshu Kumari[2]

[1]M.Tech Student, Dept of CSE, St. Peter's Engineering College, Hyderabad, T.S, India

[2]Assistant Professor, Dept of CSE, St. Peter's Engineering College, Hyderabad, T.S, India

ABSTRACT:

As most part of cloud computing is outsourcing of computation, it is extreme beyond enough to carry out access control. A variety of schemes on the basis of attribute-based encryption were projected to protect cloud storage. Our purpose is to attain multi-authority cipher text-policy attribute-based encryption that attains security and assures privacy of consumer identity data; and endures compromise attacks on authorities or else collusion attacks by means of authorities. In our work we introduce semi-anonymous system of privilege control known as AnonyControl to deal with data confidentiality and user identity confidentiality in the traditional methods of access control. This technique decentralizes central authority to confine leakage of identity and as a consequence attains semi-anonymity. Besides, it furthermore generalizes access control of file towards privilege control, by means of which privileges of the entire operations on cloud data is managed in fine-grained mode. The proposed system permit cloud servers to manage the privileges of user access devoid of recognizing their identity data and this scheme defend user privacy against each of the particular authority. Proposed scheme is tolerant in opposition to authority compromise.

Keywords: Attribute-based encryption, Cipher text-policy attribute-based encryption, Semi-anonymous, Anony Control, Central authority, Access control, Data confidentiality.

1. INTRODUCTION:

Cloud computing attracts interest from academia along with industry because of effectiveness; however it moreover has as a minimum of three challenges that should be handled. Firstly, data privacy should be assured and not only access but moreover operation has to be guarded [1]. Secondly, personal data is at threat since one's identity is legitimated on the basis of data for the intention of access control. As people are concerned regarding their identity privacy, identity privacy has to be protected. Lastly, cloud system has to be flexible in case of security violation where system is compromised by means of attackers. Different from data privacy, less attempt is paid to guard user identity confidentiality during interactive protocols. Users' identities that are explained by means of their attributes are revealed towards key issuers, and issuers provide private keys in relation to their attributes. However it seems normal that users are eager to carry on their identities secret while they acquire their private keys. Our objective is to attain multi-authority cipher text-policy attribute-based encryption that attains security and assures privacy of consumer identity data; and endures compromise attacks on authorities or else collusion attacks by means of authorities. We suggest efficient methods to permit cloud servers to manage the privileges of user access devoid of recognizing their identity data [2][3]. In our work we provide a semi-anonymous system of privilege control known as AnonyControl to deal with data confidentiality and user identity confidentiality in the traditional methods of access control. Proposed system decentralizes central authority to confine leakage of identity and as a consequence attains semi-anonymity. Besides, it moreover generalizes access control of file towards privilege control, by means of which privileges of the entire operations on cloud data is managed in fine-grained mode.

2. PROPOSED SYSTEM REPRESENTATION:

Cloud paradigm is revolutionary concept that permits flexible, on-demand as well as low-cost practice of computing resources, however data is outsourced towards several cloud servers, and a variety of privacy issues come into view from it. In the cloud paradigm computing resources are offered with dynamism by means of Internet and data storage in addition to computation is

outsourced towards someone in a cloud. We suggest efficient methods to permit cloud servers to manage the privileges of user access devoid of recognizing their identity data. The proposed schemes defend user privacy against each of the particular authority. Proposed schemes are tolerant in opposition to authority compromise. AnonyControl deal with data confidentiality and user identity confidentiality in traditional methods of access control and decentralizes central authority to confine leakage of identity and as a consequence attains semi-anonymity. It generalizes access control of file towards privilege control, by means of which privileges of the entire operations on cloud data is managed in fine-grained mode. Our intention is to attain multi-authority cipher text-policy attribute-based encryption that attains security and assures privacy of consumer identity data; and endures compromise attacks on authorities or else collusion attacks by means of authorities. In the proposed system model, there are four entities such as Attribute Authorities, Cloud Server, Owners as well as Consumers. A user may be the owner and a consumer at the same time. Authorities are supposed to include commanding computation ability, and they are managed by means of government offices since a number of attributes partly enclose user identifiable data [4]. The complete attribute set is divided as disjoint sets and guarded by each of the authority; hence each of the authority is conscious of part of attributes. Owner wishes to outsource encrypted information file towards cloud servers, who is supposed to contain sufficient storage ability, and store them. Recently connected consumers make a request of private keys from the entire of authorities, and they do not identify the attributes to be controlled. When Data consumers make a request towards their private keys from authorities, authorities mutually produce equivalent private key and send it towards them. Each and every consumer downloads encrypted files; however those private keys convince privilege tree carry out process connected by privilege. The server executes an action and only if user credential are confirmed all the way through privilege tree.

3. AN OVEVIEW OF ACHIEVING COMPLETE ANONYMITY:

In our work, encryption policy is explained by means of a tree known as access tree and each of the non-leaf nodes of tree is

threshold gate and each of the leaf nodes is explained by means of an attribute. Single access tree is necessary in each of the data file to describe encryption policy. The privilege in our system is described as comparable to privileges that is managed in normal functioning systems. Data file contain quite a lot of operations that are executable and each of them is authorized towards approved users by means of various level of qualifications. In our system, quite a lot of trees are necessary in each data file to confirm user identity and grant rights accordingly. In our work we present a semi-anonymous system of privilege control known as AnonyControl to deal with data confidentiality and user identity confidentiality in the traditional methods of access control. It decentralizes central authority to confine leakage of identity and as a consequence attains semi-anonymity and it moreover generalizes access control of file towards privilege control, by means of which privileges of the entire operations on cloud data is managed in fine-grained mode. Our work attains multi-authority cipher text-policy attribute-based encryption that attains security and assures privacy of consumer identity data; and endures compromise attacks on authorities or else collusion attacks by means of authorities. The proposed scheme protects user privacy against each of the particular authority. Partial data is disclosed within the proposed system [5]. Proposed scheme is tolerant in opposition to authority compromise. We have believed semi-honest authorities within AnonyControl and assumed that they will not collude by each other and this is an essential statement in AnonyControl since each of authority is in charge of subset of complete attributes set, and meant for attributes. When data from the entire authorities is collected in general, total attribute set of key requester is improved and as a result his distinctiveness is revealed to authorities. The proposed system is semi-anonymous as data of partial identity is revealed towards each authority; however we attain full-anonymity and moreover permit approval of authorities. The important point of identity data leak is that key generator will provide attribute key on the basis of reported attribute, and generator has to recognize user attribute to perform so. We require introducing a novel technique to allow key generators to provide accurate attribute key devoid of attributes the users contain. A naive way out is to provide the entire attribute keys of the entire attributes

towards key requester and allow him choose whatever he wants. In this means, key generator does not recognize the type of attribute keys, has been picked by key requester, but we need to completely believe key requester that he will not choose any of the attribute key not authorized to him [6].

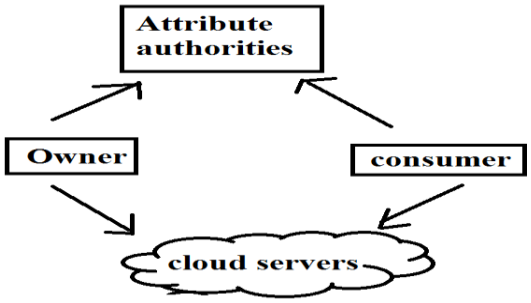

Fig1: an overview of proposed system.

4. CONCLUSION:

Most of the work spotlight on privacy of data contents as well as access control, whereas less consideration is paid towards privilege control as well as identity privacy. In our work we present approaches to permit cloud servers to manage the privileges of user access devoid of recognizing their identity data. Our work attains multi-authority cipher text-policy attribute-based encryption that attains security and assures privacy of consumer identity data; and endures compromise attacks on authorities or else collusion attacks by means of authorities. We make available a semi-anonymous system of privilege control known as AnonyControl to deal with data confidentiality and user identity confidentiality in the traditional methods of access control. This technique decentralizes central authority to confine leakage of identity and as a consequence attains semi-anonymity. Besides, it additionally generalizes access control of file towards privilege control, by means of which privileges of the entire operations on cloud data is managed in fine-grained mode. The projected schemes defend user privacy against each of the particular authority and these schemes are tolerant in opposition to authority compromise. The projected The proposed system is semi-anonymous as data of partial identity is revealed towards each authority; however we attain full-anonymity and moreover permit approval of authorities.

REFERENCES

[1] M. Chase, "Multi-authority attribute based encryption," in TCC.Springer, 2007, pp. 515–534.

[2] M. Chase and S. S. Chow, "Improving privacy and security in multiauthorityattribute-based encryption," in CCS. ACM, 2009, pp. 121–130.

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

[4] J. Hur, "Attribute-based secure data sharing with hidden policies insmart grid," TPDS, vol. 24, no. 11, pp. 2171–2180, 2013.

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

[6] D. Boneh and M. Franklin, "Identity-based encryption from the weilpairing," in CRYPTO. Springer, 2001, pp. 213–229.