IJRRECS/March 2016/Volume-4/Issue-3/5244-5248 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

PROTECTION OF USER PRIVACY IN ACCESS CONTROL METHODS

P.Mallika[1], Dr.P.Venkateswarlu[2], A.Arun Kumar[3]

[1]M.Tech Student, Dept of CSE, Nagole Institute of Technology & Science, Hyderabad, T.S, India

[2]Professor & HOD, Dept of CSE, Nagole Institute of Technology & Science, Hyderabad, T.S, India

[3]Associate Professor, Dept of CSE, Nagole Institute of Technology & Science, Hyderabad, T.S, India

ABSTRACT:

While people are more worried regarding their identity privacy, it moreover needs to be protected prior to cloud entering our life. Any of the authority or else server alone should not make out any client's personal data. Different methods were proposed to defend data contents confidentiality by means of access control. We need to attain a multi-authority cipher text based encryption which achieves security; assurance privacy of data consumer identity information; as well as tolerating compromise attacks on authorities hence we propose a framework to permit cloud servers to manage user access privileges without finding of their identity data. The proposed framework not only data privacy, but also user identity privacy within existing access control methods. It decentralizes central authority to confine identity leakage and as a result gets semi-anonymity and generalizes file access control to privilege control, by which privileges of the entire operations on cloud data are managed within an efficient way.

Keywords: Identity privacy, Privilege control, Access control, Cipher text based encryption, Cloud servers, Semi-anonymity, Multi-authority.

1. INTRODUCTION:

The most attractive feature of cloud computing is computation outsourcing, which is far beyond enough to carry out an access control. But however, in the cloud system, data confidentiality has to be assured. The data confidentiality is not just concerning data contents. When sensitive information is outsourced towards the cloud servers, which is beyond user control in the majority of cases, privacy risks will increase severely since the servers may unlawfully examine user data and access their information, or else other users infer sensitive information from outsourced computation [1]. In cloud system moreover personal information is at risk since one's identity is verified based on data for access control purpose. The cloud system has to be resilient in security breach in which some part of system is compromised by means of attackers. Different from data confidentiality, less attempt is paid to defend user identities during the interactive protocols. User identities, described by their attributes, are commonly disclosed towards key issuers, and issuers provide private keys based on their attributes. However it seems normal that users are eager to maintain their identities undisclosed while they get their private keys. Various methods were proposed for securing of cloud storage but most of them focus on data contents privacy and access control, while less consideration is paid towards privilege control as well as identity privacy [2][3]. Hence we propose AnonyControl framework to permit cloud servers to manage user access privileges without finding of their identity data. The system decentralizes central authority to confine identity leakage and as a result gets semi-anonymity. It moreover generalizes file access control to privilege control, by which privileges of the entire operations on cloud data are managed within a fine-grained manner.

2. METHODOLOGY:

Cloud computing has greatly attracted attention from several areas because of profitability. Various methods were proposed to defend data contents confidentiality by means of access control among them Identity-based encryption was introduced by Shamir where sender of a message specifies an identity so that only receiver by similar identity can decrypt it. Later Fuzzy Identity-Based Encryption was projected, which is also identified as Attribute-Basis Encryption. Tree-based

methods such as key-policy based encryption and Cipher text Encryption are provided to convey more common condition. They are complements to each other in sense that decision of encryption policy is made by various parties. Our goal is to attain a multi-authority cipher text based encryption which achieves security; assurance privacy of data consumer identity information; as well as tolerates compromise attacks on authorities or else collusion attacks by authorities. In our work we introduce a system for allowing cloud servers to supervise user access privileges without revealing of identity data. The proposed scheme protects user's privacy against each of the single authority and partial information is disclosed in this system; and this scheme is tolerant against authority compromise. Our semi-anonymous attribute-basis privilege control method was introduced to handle the problem of user privacy within cloud storage server. By means of multiple authorities within cloud system, our proposed system will gain not only fine-grained privilege control but moreover identity anonymity while performing privilege control on the basis of user identity information. Semi-honest authorities were imagined within the proposed system and assume that they do not collude with each other which are most essential [5]. The introduced scheme was projected to address not only data privacy, but also user identity privacy within existing access control methods and this method decentralizes central authority to confine identity leakage and as a result gets semi-anonymity.

3. AN OVERVIEW OF PROPOSED SYSTEM:

Cloud computing is a revolutionary perception, which facilitate flexible and uses low-cost computing resources, but data is outsourced towards some cloud servers, and thus a variety of privacy concerns emerge from it. Moreover personal data is at risk since one's identity is verified based on data for access control purpose. While sensitive information is outsourced in the direction of the cloud servers, which is away from user control in the majority of cases, privacy risks will increase rigorously. Various schemes on attribute-based encryption were proposed for securing of cloud storage. However, most of the works focus on data contents privacy and access control, while less consideration is paid towards privilege control as well as identity privacy. Less

works were done to defend user identities which are commonly disclosed towards key issuers and issuers provide private keys based on their attributes during the interactive protocols. We propose a framework to permit cloud servers to manage user access privileges without finding of their identity data. We assume semi-honest authorities within the proposed system and assume that they do not collude with each other. This is an important supposition within the proposed system because each of the authority is responsible for a subset of complete attributes set, and for attributes that it is responsible for, it knows precise information of key requester. When the data from the entire authorities is gathered complete attribute set of key requester is improved and as a result his identity is revealed to authorities. The system moreover generalizes file access control to privilege control, by which privileges of the entire operations on cloud data and partial information is disclosed in this system. In this system, user privacy is protected against each of the single authority and this scheme is tolerant against authority compromise [6]. In this sense, the proposed system is semi-anonymous as partial identity data is disclosed to each of the authority, but we can attain full-anonymity and moreover permit the collusion of authorities. The proposed framework addresses not only data privacy, but also user identity privacy within existing access control methods. The important point of identity data leak we had in our existing attribute basis encryption methods is that key generator authorities provides attribute key on the basis of reported attribute, and generator has to recognize user attribute to perform so. We initiate a novel method to allow key generators issue exact attribute key devoid of knowing what attributes users contain. A naive result 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 make out which attribute keys was picked by the key requester, but we need to completely trust key requester regarding picking of any attribute key not authorized to him.

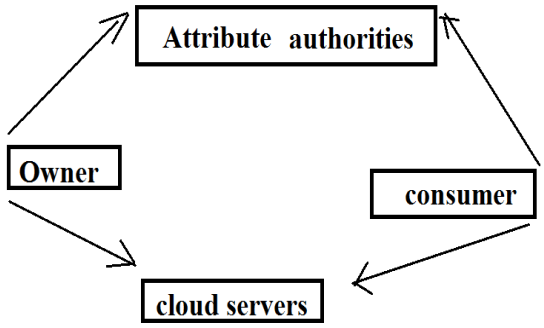

Fig1: proposed system.

4. CONCLUSION:

In cloud computing, computing resources are provided using Internet and data storage and computation are outsourced towards some party within cloud. Most of the works spotlight on data contents privacy as well as access control, while less consideration is paid towards privilege control as well as identity privacy Our objective is to achieve a multi-authority cipher text based encryption which achieves security; assurance privacy of data consumer identity information hence an AnonyControl framework was proposed to permit cloud servers to manage user access privileges without finding of their identity data. Semi-honest authorities were imagined within the proposed system and assume that they do not collude with each other which are most essential. The proposed system address data privacy and user identity privacy within existing access control methods and protects user's privacy against each of the single authority and partial information is disclosed in this system. The structure decentralizes central authority to confine identity leakage and as a result gets semi-anonymity and generalizes file access control to privilege control, by which privileges of the entire operations on cloud data are managed within a fine-grained manner. By multiple authorities within cloud system, our proposed system will gain not only fine-grained privilege control but moreover identity anonymity while performing privilege control on the basis of user identity information.

REFERENCES

[1] 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.

[2] 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.

[3] F. Li, Y. Rahulamathavan, M. Rajarajan, and R. C.-W. Phan, "Low complexity multi-authority attribute based encryption scheme for mobile cloud computing," in Proc. IEEE 7th SOSE, Mar. 2013, pp. 573–577.

[4] 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.

[5] 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.

[6] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2001, pp. 213–229.