IJRRECS/November 2015/Volume-3/Issue-11/4852-4857 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

A DYNAMIC APPROACH TOWARDS SUPPORTING OF CLOUD APPLICATIONS

Vusa.Sobha Rani[1], K.T.Chowdary[2]

[1]PG Scholar , Dept of CSE , Krishnaveni Engineering College for Women, Narasaraopet, AP, India

Email:sobhavusa@gmail.com

[2]Assistant Professor , Dept of CSE , Krishnaveni Engineering College for Women, Narasaraopet, AP, India

Email: ktchowdary43@gmail.com

ABSTRACT:

Managing of access control in the cloud system is important since only official users contain permission towards valid service. Much quantity of data is stored in cloud system, and most of it is sensitive information. We intend to introduce decentralized approach of access control that is used for securing of data storage within cloud system that maintains the process of anonymous authentication. In the proposed process, cloud will make verification of series accuracy without user identity information previous to data storage process. The projected decentralized scheme of access control used for securing of data storage by means of anonymous authentication will provide user revocation as well as prevents from replay attacks. Single key distribution centre is single failure point and it is tricky for maintenance due to more users who are maintained in cloud setting for this reason we focus that clouds have to consider a decentralized method during distribution of secret keys as well as attributes for users. Our proposed structure is decentralized and dynamic whereas most of the existing works that are made within cloud system are centralized natured.

Keywords: Access control, Single key distribution, Decentralized approach, Data storage, Cloud system, Attributes, Anonymous authentication.

1. INTRODUCTION:

Data that is stored in cloud system is extremely sensitive hence security along with privacy is, extremely important in cloud computing. Privacy of user is also important with the intention that cloud users do not recognize user identity. Search process on encrypted information is a vital issue in clouds and it has to be effective [1]. Cloud system must not recognize query but must return records that assure query. For offering of secured data storage, data requires an encryption process on the other hand, data is frequently modified and this property should be considered during scheming of effective method of storage techniques. Wang et al. have explained the security of storage by means of Reed-Solomon erasure-correcting codes. User authentication by means of methods of public key cryptography was studied. Cloud system responsibility is typical task and involves various issues of technical problems as well as law enforcement. In our work we propose a decentralized approach of access control that is used for securing of data storage within cloud system that maintains the process of anonymous authentication. In the proposed method, cloud will make verification of series accuracy without user identity information previous to data storage process [3]. Single key distribution centre is single failure point and it is tricky for maintenance due to more users who are maintained in cloud setting. Hence we focus that clouds have to consider a decentralized method during distribution of secret keys as well as attributes for users. It is more common for cloud system to contain lots of key distribution centres in various locations. Our system is decentralized and dynamic whereas most of the existing works that are made within cloud system are centralized natured. The proposed decentralized approach of access control used for securing of data storage by means of anonymous authentication will provide user revocation as well as prevents from replay attacks.

2. METHODOLOGY:

Additional attention should be provided for ensuring of access control of the sensitive information that is related to health and important documents. Access control generally is of user-based, role-based as well as attribute-based access control. User-based access control list includes users who are approved to have permission to data. Attribute-based access control is more

promising approach, in which users are offered attributes, and data contain attached access policy. Users holding valid attributes, will satisfy access policy, have permission to the data. An area in which access control is broadly used is health care. For offering secured data storage, data requires an encryption process on the other hand, data is frequently modified and this property should be considered during scheming of effective method of storage techniques. Clouds store sensitive information concerning patients to allow permission towards researchers along with policy makers [2]. It is significant to manage accessing of data with the intention that only official users can have permission t o that data. Managing of access control is important in online social networking in which users store up their pictures and videos and share them to particular users [4]. It is incredibly significant that only official users are provided access to that information and hence we propose a decentralized approach of access control that is used for securing of data storage within cloud system that maintains the process of anonymous authentication. In proposed technique, cloud will make verification of series accuracy without user identity information previous to data storage process. The decentralized approach of access control used for securing of data storage by means of anonymous authentication will provide user revocation as well as prevents from replay attacks. Existing works that are made on access control within cloud system are centralized natured. Single key distribution centre is single failure point and it is tricky for maintenance due to more users who are maintained in cloud setting as a result we focus that clouds have to consider a decentralized method during distribution of secret keys as well as attributes for users [5]. It is general for cloud system to contain lots of key distribution centres in various locations. Our approach will support an authentication method of privacy preserving that is not supported by others. For the most of the existing do not support user revocation, whereas our proposed system will supports it. Our proposed approach will contain the additional feature concerning access control where only applicable users will decrypt stored information.

3. AN OVERVIEW OF PROPOSED SYSTEM:

Cloud is unable to identify user identity who store up information, but verifies credentials of user. Cloud will identify access policy

for every record that is stored up in cloud system. Cloud servers that are prone to Byzantine failure, in which storage server will not succeed in random way. The cloud is prone towards data modification as well as server colluding attacks. In the attacks of server colluding, adversary compromises storage servers, for making of modification to data files on condition that they are inside constant. Cloud system dependability is typical task and involves various issues of technical problems as well as law enforcement. In our work we suggest a decentralized approach of access control that is used for securing of data storage within cloud system that maintains the process of anonymous authentication. The proposed approach of access control used for securing of data storage by means of anonymous authentication will provide user revocation as well as prevents from replay attacks. In this method, cloud will make verification of series accuracy without user identity information previous to data storage process. Our proposed system is decentralized and dynamic whereas most of the existing works that are made within cloud system are centralized natured. Our approach will support an authentication method of privacy preserving that is not supported by others. For the most of the existing do not support user revocation, whereas our proposed system will supports it. The proposed access control used for securing of data storage by means of anonymous authentication will provide user revocation as well as prevents from replay attacks. Our proposed approach will contain the additional feature concerning access control where only applicable users will decrypt stored information [6]. The scheme will support process of formation, alteration, as well as reading of data that is stored in cloud system. The cloud is assumed to be an honest but curious, where cloud administrators are concerned in viewing of the user content, but cannot change it. This model of honest but curious representation of adversary does not interfere with data with the intention that they maintain system performance normally and stay on hidden. Users can contain an option of moreover read or else write or else both the types of accesses towards file that is stored up in the cloud.

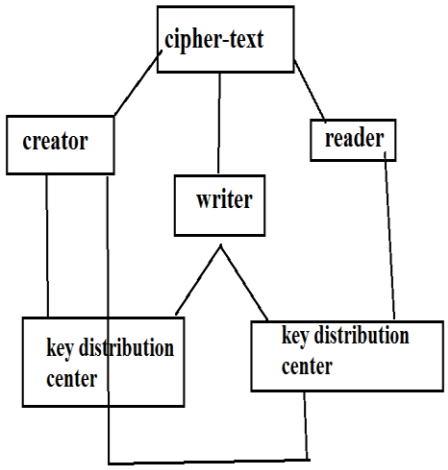

Fig1: An overview of secure cloud storage

4. CONCLUSION:

Protection of privacy along with security in the system of clouds was explored by a lot of researchers. The cloud will make user responsible for the outsourced data, and similarly, cloud makes itself answerable for provision of services. It is considerable to handle accessing of data with the intention that only official users can have permission t o that data. Single key distribution centre is single failure point and it is tricky for maintenance due to more users who are maintained in cloud setting thus we focus that clouds have to consider a decentralized method during distribution of secret keys as well as attributes for users. In our work we recommend decentralized approach of access control that is used for securing of data storage within cloud system that maintains the process of anonymous authentication. In decentralized approach, cloud will make verification of series accuracy without user identity information previous to data storage process. The decentralized scheme of access control used for securing of data storage by means of anonymous authentication will provide user revocation as well as prevents from replay attacks. Our system is decentralized and dynamic whereas most of the existing works that are made within cloud system are centralized natured. It will support an authentication method of privacy preserving that is not supported by others.

REFERENCES

[1] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentication for Cloud Computing," Proc. First Int'l Conf. Cloud Computing (CloudCom), pp. 157-166, 2009.

[2] C. Gentry, "A Fully Homomorphic Encryption Scheme," PhD dissertation, Stanford Univ., http://www.crypto.stanford.edu/ craig, 2009.

[3] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-Based Cloud Computing," Proc. Third Int'l Conf. Trust and Trustworthy Computing (TRUST), pp. 417-429, 2010.

[4] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, 2005.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

Vusa Sobha Rani received her B.Tech degree in Computer Science and Engineering in the year 2013 and pursuing M.Tech degree in Computer Science and Engineering from Krishnaveni Engineering College for Women.

K.T.Chowdary received her M.Tech degree in Computer Science and Engineering and B.Tech degree in Information Technology. He is currently working as an Asst Professor in Krishnaveni Engineering College for Women.