IJRRECS/August 2015/Volume-3/Issue-8/4530-4534 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN EFFICIENT ACCESS CONTROL STRATEGY FOR MANAGING OF CLOUD DATA VERIFICATION

L.Wilson[1], H.Saidulu[2]

[1]**M.Tech Student, Dept of CSE, Vivekananda Institute of Engineering and Technology, Bogaram (V), Keesara (M), R.R (Dist), T.S, India**

[2]**Assistant Professor, Dept of CSE, Vivekananda Institute of Engineering and Technology, Bogaram (V), Keesara (M), R.R (Dist), T.S, India**

ABSTRACT:

Security and privacy are vital issues in cloud environment and these issues are being explored by many researchers. Cloud accountability is an extremely difficult task and that involves technical issues. We put forward distributed access control of data that is stored within cloud so that certified users with applicable attributes can access them. The proposed decentralized scheme of access control is novel and efficient used for safe data storage within clouds that supports unidentified authentication. Here in this structure cloud verifies accuracy of series devoid of knowing user's identity before data storage. Moreover the system has additional feature of access control where valid users decrypt stored information and the structure prevents replay attacks as well as manages making, alteration, and understanding of data stored in cloud. In the proposed decentralized structure there can be quite a lot of key distribution centres for key management and supports numerous read and writes on cloud data.

Keywords: Cloud accountability, Access control, Key management, Key distribution centre, Decentralized scheme, Replay attacks.

1. INTRODUCTION:

The cloud makes user responsible for data it outsource, and equally cloud is itself held responsible for services it provides. User should verify prior to initiation of any transaction, and in contrast, it should be

ensured that cloud does not tamper with outsourced data. User privacy is necessary in order that cloud or else other users do not distinguish user identity [1]. Proficient search above encrypted information is an essential issue in clouds. The clouds must not recognize the query however should return records that assure the query and this is managed by searchable encryption. In cloud system, access control is important concept since only allowed users contain access to official service. Huge data is being stored within cloud, and most of this information is sensitive. Care must be taken to make sure access control of responsive information. Usually there are three types of access control such as access control based on user, based on role, as well as attribute-based access control. Attribute-based access control is extended in range, where users are specified attributes, and data has attached access policy. The problems regarding access control, verification, as well as privacy protection has to be resolved at the same time. In our work we propose a decentralized scheme of access control that is novel and efficient used for safe data storage within clouds that supports unidentified authentication. We study on distributed access control of data stored within cloud. Our method is robust and decentralized; and supports privacy preserving verification and support user revocation. It is challenging in the direction of replay attacks, where a user can put back fresh information by out of date data from a prior write, although it no longer has applicable claim policy [2][3]. Our proposed verification as well as access control method is decentralized and tough, contrasting from other access control schemes that are intended for clouds which are centralized.

2. METHODOLOGY:

In cloud computing, users outsource their storage to clouds servers by means of Internet. The cloud is prone to data alteration as well as server colluding attacks in which adversary compromise storage servers, with the intention that it modifies data files till they are consistent internally. To provide effective storage of data, data needs to be encrypted but it should be modified and this energetic property has to be considered during scheming of resourceful storage techniques. Either clouds or users have to deny operations performed and it is significant to contain log of transactions executed; on the other hand, it is a significant concern to decide

information log. It is just not sufficient to store contents efficiently in cloud however it might be essential to make sure user anonymity. User should prove to other users regarding the valid user who stored information devoid of revealing identity. Clouds have to consider decentralized approach during distribution of secret keys as well as attributes to users. It is normal for clouds to contain lots of key distribution centers in various locations of world. We propose a decentralized scheme of access control that is novel and efficient used for safe data storage within clouds that supports unknown verification. In proposed structure cloud verifies accuracy of series devoid of knowing user's identity before data storage. In this structure there can be quite a lot of key distribution centres for key management. Our system has additional feature of access control where valid users decrypt stored information and the structure prevents replay attacks as well as manages making, alteration, and understanding of data stored in cloud. Our scheme is challenging towards replay attacks, where a user can put back fresh information by out of date data from a prior write, although it no longer has applicable claim policy [4]. It is an important property since user, revoked of its attributes, may no longer be competent to write to cloud hence we, add this additional feature in our proposal that moreover allows writing numerous times which was not allowed in earlier work.

3. AN OVERVIEW OF PROPOSED SYSTEM:

We make a study on distributed access control of data that is stored within cloud with the intention that simply certified users with applicable attributes can access them. Our proposed access control method is decentralized and tough, contrasting from other access control schemes that are intended for clouds which are centralized. Here the cloud verifies accuracy of series devoid of knowing user's identity before data storage and user identity is protected from cloud during the process of authentication. In decentralized structure there can be quite a lot of key distribution centers for key management. The access controls as well as authentication are collusion resistant; hence no two users collude and make an access towards data, if they are individually not approved. The proposed decentralized structure supports numerous read and writes on cloud data. The costs are comparable to traditional

centralized approaches, and high-priced operations are mainly made by cloud. Our method is robust and decentralized; and supports privacy preserving verification and support user revocation. In our work cloud is assumed as honest-but-curious, so that cloud administrator can only view user content, but cannot change it. Honest-but-curious representation of adversaries does not interfere with data with the intention that they can maintain system functioning regularly and remain unnoticed. Users can either read or else write or both accesses towards a file stored in cloud. User privacy is necessary in order that cloud or else other users do not distinguish user identity. He should verify prior to initiation of any transaction, and in contrast, it should be ensured that cloud does not tamper with outsourced data. User has to prove to other users regarding the valid user who stored information devoid of revealing identity. Decentralized approach was to be considered during distribution of secret keys as well as attributes to users [5]. It is normal for clouds to hold lots of key distribution centres in various locations of world. We recommend privacy preserving authentic access control scheme and according to this scheme a user create a file and store it efficiently in cloud. There are three users, in our system such as creator, a reader, and writer. Creator gets a token from trustee, who is honest. A trustee manages social insurance numbers. The access policy makes a decision of accessing data that is stored in cloud. The creator makes a decision on a claim policy to prove validity and signs message in this claim. The cloud confirms signature and stores cipher-text [6]. When user contains attributes that match with access policy, it decrypts and retrieve original message. When a reader read some data that is stored in cloud, it tries to decrypt it by means of secret keys it receives from the key distribution centres.

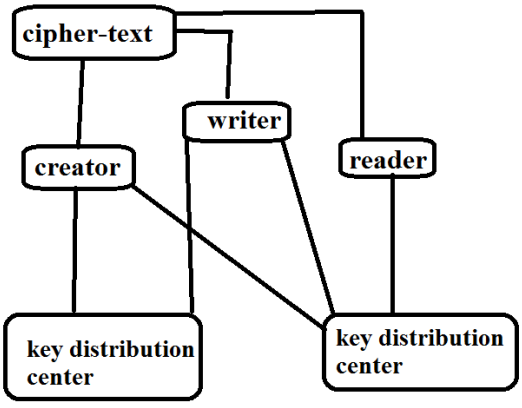

Fig1: An overview of secure cloud storage representation

4. CONCLUSION:

In cloud system, access control is important because only allowed users contain access to

official service and hence we should make sure access control of responsive information. In our work we study on distributed access control of data that is stored within cloud with the intention that simply certified users with applicable attributes can access them. Decentralized scheme of access control is efficient for safe data storage within clouds that supports unidentified authentication. It is challenging to replay attacks, where a user can put back fresh information by out of date data from a prior write, although it no longer has applicable claim policy. Moreover our proposed system is decentralized and tough, contrasting from other access control schemes that are intended for clouds which are centralized and has additional feature of access control where valid users decrypt stored information and the structure prevents replay attacks as well as manages making, alteration, and understanding of data stored in cloud. Our proposed structure is robust and decentralized; and supports privacy preserving verification and support user revocation.

REFERENCES

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

[2] 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.

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

[4] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure Threshold Multi- Authority Attribute Based Encryption without a Central Authority," Proc. Progress in Cryptology Conf. (INDOCRYPT), pp. 426-436, 2008.

[5] M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. Computer and Comm. Security, pp. 121-130, 2009.

[6] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the Decryption of ABE Ciphertexts," Proc. USENIX Security Symp., 2011.