ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Preserving Cloud Data Security & Auditing By Considering Effective Strategy of Access Control

Amgoth Linga
M.Tech Student,
Department of CSE,
Sri Indu College of Engineering and Technology,
Hyderabad, T.S, India

T.Charan Singh
Assistant Professor
Department of CSE,
Sri Indu College of Engineering and Technology,
Hyderabad, T.S, India.

Abstract:
Huge information is stored in the system of cloud, and for the most of this data is sensitive information. In the process of cloud computing consideration of privacy and security are important issue that are to be handled. Managing of access within cloud system has gained concentration for the reason that it is essential that only allowed users will have permission towards applicable services. We make available distributed access control of information that is stored up within cloud system with the intention that only approved users with official attributes can have permission towards them. It is authentication as well as decentralized and robust, and is dissimilar from other methods of access control that are considered for centralized clouds and has additional trait of access control where simply actual users are capable to decrypt stored data. The strategy prevents replay attacks where user restores new information with old data from an earlier write, although it no longer contains legitimate claim policy.

Keywords: ***Cloud computing, Replay attacks, Decentralized, Authentication, Access control, Distributed access, Security.***

1. Introduction

In the procedure of cloud computing, users outsource the storage to servers by means of Internet services. In the recent times, Wang et al. has provided effective cloud storage that is moreover consistent. Servers of cloud systems are prone towards Byzantine breakdowns, in which a server stops working in random way [1]. The cloud system is prone towards modification process of data as well as server colluding attacks. In these attacks, opponent makes a compromise towards storage servers, with the intention that it makes alteration to data files on condition that they are constant from inside.

For provision of effective storage of data, there is an encryption of data on the other hand, data is altered and this property should be considered during the scheming of well-organized methods of secure storage. The cloud manages user answerable for the data has outsourced, and similarly, cloud is responsible for services it has provided. The authority of the user who store up the information is moreover verified. Apart from technical elucidations for making sure of security as well as privacy, there is requirement for enforcing of law. Wang et al. have tackled the security of storage by means of Reed-Solomon codes of erasure-correcting. Managing of effective process of search on encrypted information is a significant issue within cloud system. The clouds must not identify the query but have to return records that assure query and it is gained by searchable encryption. In our work, we provide a decentralized method of access control for managing of effective data storage in cloud system supporting unidentified confirmation [2][3].

Our proposal also has additional trait of access control where simply actual users are capable to decrypt stored data and is moreover usual for cloud system to hold many key distribution centres in many separate locations worldwide. Our access control method is authentication as well as decentralized and robust, and is dissimilar from other methods of access control that

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

are considered for centralized clouds. Our proposal also has additional trait of access control where simply actual users are capable to decrypt stored data

2. METHODOLOGY:

User in the cloud system has to confirm itself earlier than introduction of any transaction, and it has to be guaranteed that cloud does not interfere with the outsourced data. Generally there are several types of managing access within cloud system and they are access control based on user, based on role, as well as access control based on attributes.

In the access control based on attributes, users are specified attributes, and data has fixed access policy. In these users by a convincing set of attributes, convince the access policy and provide permission towards data. Managing of access is moreover important in online social networking in which the user can store up their personal data, and distribute them with particular groups of users. It is especially necessary that just authorized users are provided permission to access the information. It is not sufficient to manage the content protection within the cloud process but it should be compulsory to make sure user anonymity. The works that are made earlier regarding access control in the cloud system are centralized. The authors consider an approach of centralized in which particular key distribution centre allocates secret keys towards the entire users [4]. Particular key distribution centre is not the particular point of breakdown but tricky to maintain due to huge number of users that are managed in the system of cloud.

Hence the clouds have to consider a decentralized approach in while there is a distribution of secret keys towards users. While Yang et al has provided a decentralized method, their procedure does not validate users, who remain unidentified during accessing of cloud. In our work we provide distributed access control of information that is stored up within cloud system with the intention that only approved users with official attributes can have permission towards them. Here cloud makes verification of accuracy of series devoid of identification of user identity earlier than storing of information. This technique is authentication as well as decentralized and robust, and it is dissimilar from other methods of access control that are considered for centralized clouds [5].

Our scheme supports verification of privacy preserving, and moreover supports revocation of user which is not supported by others. It is moreover normal for the cloud system to contain many key distribution centres in many separate locations globally. The proposed access control and verification are collusion resistant and no two user's access data when they are independently not approved. The proposed strategy is moreover challenging to replay attacks where user restores new information with old data from an earlier write, although it no longer contains legitimate claim policy and it is an essential property since a user, revoked of attributes, can be no longer capable to write to cloud.

3. AN OVERVIEW OF PROPOSED SYSTEM:

While the previous approaches considers a centralized method and permits simply one key distribution centre, which is a particular failure point. In our work the cloud system is considered as honest-but-curious, and hence the cloud managers are concerned in viewing of the user content, but are not able to modify it. The representation of honest-but-curious regarding adversaries does not interfere with data hence they manage the functioning of the system in normal condition.

User holds read or write accesses towards a file that is stored in system of cloud. We offer a decentralized method of access control for managing of effective data storage in cloud system supporting unidentified confirmation. In the proposed system, cloud will not know user identity user who regarding the stored information, however only confirms credential of user.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Our technique is authentication as well as decentralized and robust, and is dissimilar from other methods of access control that are considered for centralized clouds and moreover is normal for the cloud system to contain many key distribution centres in many separate locations. In the system cloud makes verification of accuracy of series devoid of identification of user identity earlier than storing of information.

Our proposal also has additional trait of access control where simply actual users are capable to decrypt stored data. The approach is moreover helps in prevention of replay attacks where user restores new information with old data from an earlier write, although it no longer contains legitimate claim policy [6]. The scheme manages making, alteration, as well as reading data that is stored within cloud. Our scheme is sturdy and decentralized and moreover supports verification of privacy preserving, and moreover supports revocation of user which is not supported by others.

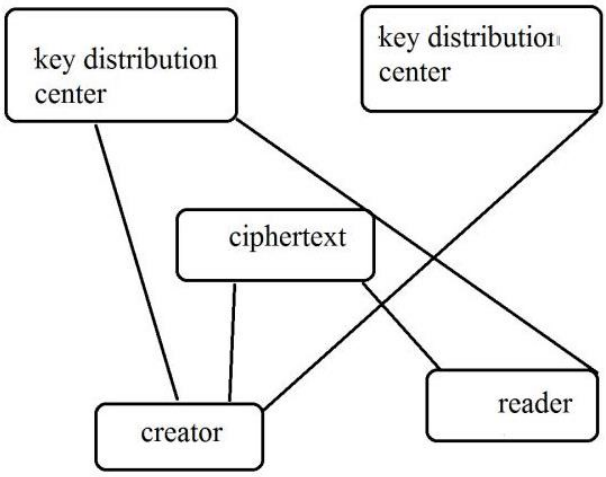

Fig1: Secure cloud storage.

4. CONCLUSION:

Privacy of user is necessary for the purpose that cloud or else other users do not identify user identity. Assuring of cloud data privacy is an important task and considers the technical concerns as well as law enforcement. Clouds consider a decentralized approach in while there is a distribution of secret keys towards users. We provide distributed access control of information that is stored up within cloud system with the intention that only approved users with official attributes can have permission towards them. It is usual for the cloud system to contain many key distribution centres in many separate locations globally.

The access control as well as verification is collusion resistant and no two user's access data when they are independently not approved. In the system, cloud makes verification of accuracy of series devoid of identification of user identity earlier than storing of information. Our method is authentication as well as decentralized and robust, and is dissimilar from other methods of access control that are considered for centralized clouds. It has added characteristic of access control where simply actual users are capable to decrypt stored data.

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] D.R. Kuhn, E.J. Coyne, and T.R. Weil, "Adding Attributes to Role- Based Access Control," IEEE Computer, vol. 43, no. 6, pp. 79-81, June 2010.

[5] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'l ICST Conf.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Security and Privacy in Comm. Networks (SecureComm), pp. 89-106, 2010.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 261-270, 2010.