IJRRECS/January 2016/Volume-4/Issue-1/5142-5146 **ISSN 2321-5461**

**INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE**

# TOWARDS A DISTRIBUTED APPROACH FOR MANAGING ANONYMOUS VERIFICATION

**S.Mahendran[1], N.Vijaya Sunder Sagar[2], M.Nagesh[3], Kommuri Navya[4]**

[1,3]Assistant Professor, Dept of CSE, Ashoka Institute of Engineering and Technology, Malkapur, Hyderabad, T.S, India

[2]Assistant & HOD, Dept of CSE, Ashoka Institute of Engineering and Technology, Malkapur, Hyderabad, T.S, India

[4]M.Tech Student, Dept of CSE, Ashoka Institute of Engineering and Technology, Malkapur, Hyderabad, T.S, India

**ABSTRACT:**

Cloud computing is an interesting issue which has received attention in the recent times. In the technology of cloud computing, users will assign their computation as well as storage towards servers by means of Internet which frees users from bothering of maintaining resources. Access control is an importance issue considered in online networking where users store personal data in clouds. It is extremely important that only authorized users are agreed to access to that information. In our work we spotlight that cloud must take decentralized approach during distribution of secret keys as well as attributes towards users and we propose a system of access control which is novel and decentralized mainly for securing of data storage in clouds that manages the anonymous process of verification. In this scheme, cloud will verify authenticity of series devoid of knowing user identity earlier than storage of data. Our structure also has additional feature of access control where simply valid users are capable to decrypt stored information. This method additionally allows writing numerous times which was not allowed in our previous works.

***Keywords: Cloud computing, Access control, Data storage, Decentralized, Authenticity, Attributes, Anonymous, Secret keys.***

## 1. INTRODUCTION:

Clouds provide services, and infrastructures help developers to develop applications. Cloud applications will hold user answerable for data it outsources, and also, cloud is responsible for services it makes available. Despite of technical solutions to guarantee privacy, there is furthermore a requirement for law enforcement [1]. Most part of data that is stored up within clouds is extremely sensitive hence privacy is an important issue to be considered within cloud computing. User have to validate itself previous to initiation of any transaction, and in contrast, it have to be certified that cloud does not interfere with the outsourced data. User privacy is compulsory in order that cloud users do not be familiar with user identity. In our work we propose a system of access control which is novel and decentralized mainly for securing of data storage in clouds that manages the anonymous process of verification. In this system, cloud will verify authenticity of series devoid of knowing user identity earlier than storage of data. Our projected system is resistant towards replay attacks, where user replaces fresh information by out of date data from earlier write, even if it does not contain applicable claim policy. Efficient process of search above encrypted information is moreover an important issue in clouds. The clouds should be capable to return records that convince query and it is by means of searchable encryption. In our work we highlight that cloud must take decentralized approach during distribution of secret keys as well as attributes towards users [2][3]. Our system has feature of access control where simply valid users are capable to decrypt stored information. To provide protected data storage, data desires to be encrypted but data is frequently modified and this is considered while scheming of well-organized confined storage techniques.

## 2. AN OVERVIEW OF RELATED WORKS:

Security protection inside clouds is explored by lots of researchers such as Wang et al has tackled storage security by means of Reed-Solomon erasure-correction codes. User authentication by means of public key

cryptographic methods was studied. Many techniques of homomorphic encryption were suggested for making sure that cloud is not capable to read data during computations on them. By means of homomorphic encryption, cloud will receive cipher-text of data and carry out computations on cipher-text and returns encoded result. There are three of access control types and they are user-based, role-based, as well as attribute-based access control. In user based mechanism, list of access control contains users list that are sanctioned to access data.

In role-based mechanism, users are classified according to their individual roles. Attribute-based access control is more extensive, in which users are specified attributes. Access control is interesting issue in cloud system as it is essential that only sanctioned users contain access towards applicable service. In our work we propose a system of access control which is novel and decentralized mainly for securing of data storage in clouds that manages the anonymous process of verification. In this system, cloud will verify authenticity of series devoid of knowing user identity earlier than storage of data. Our system also has additional feature of access control where simply valid users are capable to decrypt stored information. There are cryptographic methods such as ring signatures, mesh signatures, and group signatures. Ring signature method is not a possible choice for clouds in which there are huge users. Group signatures will assume pre-existence of group which may not be promising in clouds. Mesh signatures technique will not make sure if message is from particular or else numerous users [4]. Hence for these reasons, a novel protocol recognized as attribute-based signature was applied in which users encompass a claim predicate that is connected by message. The claim predicate will identify user as an official one, devoid of revealing its identity. Attribute-based signature was combined with attribute-basis encryption to attain authentic access control devoid of disclosing identity of user to cloud. Earlier works that were made by Zhao et al. have provided access control of privacy preserving in cloud. On the other hand, authors get centralized approach in which a distribution center of single key will distribute secret keys as well as attributes on the way to all users. Distribution center of single key is not just a particular point of failure but hard to sustain due to large users that are maintained in cloud setting. Hence in our work we

highlight that cloud must take decentralized approach during distribution of secret keys as well as attributes towards users.

## 3. AN OVERVIEW OF PROPOSED SYSTEM:

Accountability concerning cloud system is an extremely difficult task and it involves issues of technical problems as well as law enforcement. It is essential to contain log of transactions performed; on the other hand, it is a main concern to make a decision of how much data to maintain in log. Access control within cloud environment is interesting as it is essential that only sanctioned users contain access towards applicable service. There are three of access control types such as user-based, role-based, as well as attribute-based access control. Attribute-based access control is wide-ranging, in which users are specified attributes. A huge total of information is being stored up within cloud, and most of this is susceptible data and care needs to be taken for assuring of access control of sensitive data which often relates to health or else even personal information. Using attribute-basis encryption, records are encrypted in various access policies and stored up within cloud. Users are specified attributes sets as well as corresponding keys and only when users contain corresponding set of attributes, can decrypt data that is stored up in cloud [5]. Previous works get centralized approach in which a distribution centre of single key will distribute secret keys as well as attributes on the way to all users. Distribution centre of single key is not just a particular point of failure but hard to sustain due to large users that are maintained in cloud setting. It is also relatively normal for clouds to contain numerous key distribution centers in various locations. We make use of attribute-based signature to attain authenticity as well as privacy. This protocol was applied in which users encompass a claim predicate that is connected by message. Attribute-based signature was combined with attribute-basis encryption to attain authentic access control devoid of disclosing identity of user to cloud. We suggest a system of access control which is novel and decentralized mainly for securing of data storage in clouds that manages the anonymous process of verification [6]. In this system, cloud will verify authenticity of series devoid of knowing user identity earlier than storage of data. In our work we highlight that cloud must take decentralized approach during distribution of secret keys as well as

attributes towards users. Our proposed system is resistant towards replay attacks, where user replaces fresh information by out of date data from earlier write, even if it does not contain applicable claim policy. This is a significant asset since a user, revoked of its attributes, might perhaps not able to write to cloud. Our method in addition allows writing numerous times which was not allowed in our previous works.

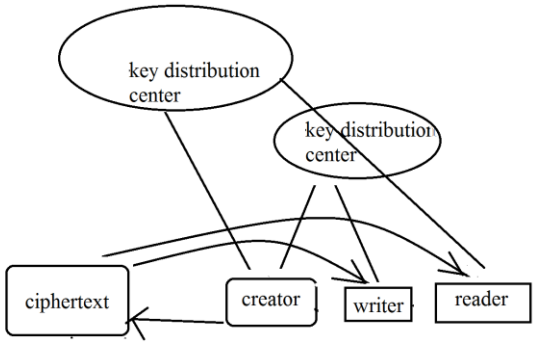


Fig1: secure cloud storage illustration

## 4. CONCLUSION:

Existing works on access control within cloud are centralized and it is not enough to store up contents strongly in cloud but it is also necessary to make sure anonymity of user. We introduce a system of access control which is novel and decentralized mainly for securing of data storage in clouds that manages the anonymous process of verification. We emphasize that cloud must take decentralized approach during distribution of secret keys as well as attributes towards users. In this structure, cloud will verify authenticity of series devoid of knowing user identity earlier than storage of data. Our projected system is resistant towards replay attacks, where user replaces fresh information by out of date data from earlier write, even if it does not contain applicable claim policy. Our system also allows writing numerous times which was not allowed in our previous works. Our structure also has additional feature of access control where simply valid users are capable to decrypt stored data.

## REFERENCES

[1] R.L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT), pp. 552-565, 2001.

[2] X. Boyen, "Mesh Signatures," Proc. 26th Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 210-227, 2007.

[3] D. Chaum and E.V. Heyst, "Group Signatures," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 257-265, 1991.

[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.