IJRRECS/June 2015/Volume-3/Issue-6/3960-3964 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

EFFECTIVE DATA STORAGE FOR MANAGING ANONYMOUS VERIFICATION IN CLOUD SYSTEM

M.Sravani[1], K.Ramesh Babu[2]

[1]M.Tech Student, Dept of CSE, Malla Reddy Engineering College for Women, Hyderabad, T.S, India

[2]Professor, Dept of CSE, Malla Reddy Engineering College for Women, Hyderabad, T.S, India

ABSTRACT:

Access control within cloud system has been gaining concentration since it is significant that only approved users contain access to applicable service. There has been several works on attribute-based access control in clouds and these works make use of a cryptographic primitive well-known as attribute based encryption. We suggest a decentralized access control system for effectual storage of data in cloud system by means of unspecified authentication, which recommend user revocation and put off replay attacks. In the projected system, the cloud does not identify the identity of user who accumulates information, but merely verifies user's credentials earlier than storing data. Our system moreover has added feature of access control in which merely valid users are able to decrypt accumulated information. The system suspends replay attacks and continues creation, modification, as well as reading data stored within the cloud. Our authentication in addition to access control system is decentralized and strong, contrasting from other access control systems that are considered in support of centralized clouds.

Keywords: Cloud system, Anonymous, Cryptographic, Attribute based encryption, Access control, Decentralized.

1. INTRODUCTION:

In recent times, a lot of consideration has been gained in cloud computing from academic as well as industrial worlds. Users in cloud system can outsource their storage towards servers by means of Internet. For the most part of cloud data is extremely susceptible [1]. Security and privacy are, consequently, extremely essential issues within cloud platform. Privacy of user is moreover necessary with the intention that cloud or else other users do not recognize distinctiveness of the user. The cloud holds user who is responsible for the outsourced data, and similarly, the cloud is itself responsible for services it provides. Efficient search above encrypted data is also significant concern within cloud system. The clouds should not recognize the query but must be able to return records that convince the query and is achieved by searchable encryption. Securities as well as privacy protection in cloud system are being looked at by numerous researchers. Responsibility of clouds is an extremely demanding task and involves technical issues as well as law enforcement [2][3]. A huge quantity of information is being accumulated in cloud, and much of this is responsive information. To make available protected data storage, data needs to be encrypted. On the other hand, the data is often customized and this vibrant property needs to be considered while scheming of well-organized secure storage techniques. It is just not sufficient to accumulate the contents strongly in the cloud but it may be essential to make sure anonymity of user. In our work we have introduced a decentralized access control method by means of anonymous authentication, which offer user revocation and put off replay attacks. Our authentication as well as access control system is decentralized and tough, contrasting from other access control systems that are considered in support of centralized clouds. The cloud does not recognize the identity of user who accumulates information, but merely verifies user's credentials.

2. METHODOLOGY OF PROPOSED SYSTEM:

There are generally three categories of access control schemes such as user-based access control, attribute-based access control and role-based access control. Access control list enclose list of users who are allowed to access data in user-based access

control and it is not possible in clouds where there are numerous users. In role-based access control users are organized on the basis of their individual roles. Data is accessed by means of users who enclose matching roles which are described by the system. Attribute-based access control is more extended in capacity, in which users are specified attributes, and data contain attached access policy. Only users with suitable set of attributes, fulfilling access policy, can access data. There has been a number of works on attribute-based access control in clouds and these works make use of a cryptographic primitive well-known as attribute based encryption. We put forward a decentralized access control method for effective storage of data in cloud system by means of anonymous authentication, which offer user revocation and put off replay attacks [4]. Our authentication as well as access control system is decentralized and tough, contrasting from other access control systems that are considered in support of centralized clouds. In the introduced system, the cloud does not recognize the identity of user who accumulates information, but merely verifies user's credentials earlier than storing data. The projected system is decentralized denote that there can be quite a lot of key distribution centres for key management. Numerous homomorphic encryption methods were suggested to make sure that cloud is not capable to read data while performing computations on them. By means of homomorphic encryption, cloud receives cipher-text of data and carries out computations on it and returns encoded value of result. Our scheme also has additional feature of access control in which merely valid users are able to decrypt accumulated information. The system put off replay attacks and maintains creation, modification, as well as reading data stored in the cloud [5].

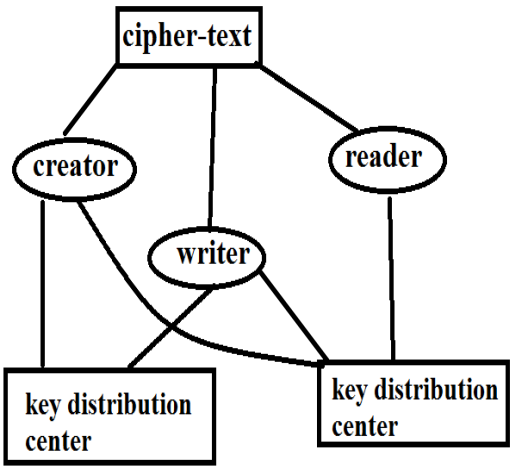

Fig1: An overview of secure cloud storage representation

3. AN OVERVIEW OFPRIVACY PRESERVING ACCESS SCHEME:

Authors consider a centralized means where a particular key distribution centre allocates secret keys as well as attributes to each and every user. Unfortunately, a single key distribution centre is not only a particular point of failure but tricky to continue due to huge number of users that are maintained in a cloud setting. We, highlight that cloud has to take a decentralized approach whereas distributing secret keys and attributes towards users. It is also quite usual for clouds to contain many key distribution centres in several locations. There has been several works on attribute-based access control in clouds and these works make use of a cryptographic primitive well-known as attribute based encryption. Our scheme is strong and decentralized; most of others are centralized and supports privacy preserving authentication, which is not maintained by others. The proposed system is decentralized; mean that there can be quite a lot of key distribution centres for key management. The proposed system is resilient towards replay attacks. We put forward our privacy preserving authenticated access control method and according to our system a user can produce a file and store it strongly in cloud. The proposed system consists of usage of two protocols such as attribute based encryption and attribute based signature. The cloud does not recognize the identity of user who accumulates information, but merely verifies user's credentials. There are creator, reader, as well as writer entities within the system. Creator obtains a token from trustee, who is supposed to be honest. On providing their identity, trustee provides their token. There are numerous key distribution centres which can be scattered. A creator on provision of token towards one or additional key distribution centre obtains keys for encryption or decryption and signing [6]. The access policy makes a decision that can access data accumulated in cloud. The creator makes a decision on a claim policy to verify their legitimacy and signs message under this claim. The cipher-text with signature is sent towards cloud. The cloud confirms signature and stores cipher-text. When a reader needs to read, cloud sends cipher-text. If the user contains attributes corresponding with access policy, it can decrypt and retrieve original message. Write carry on in same way as file creation. By means of designating verification procedure towards the cloud, it relieves individual users from time consuming confirmation. When a reader needs to read several data

stored in cloud, it attempt to decrypt it by means of the secret keys it receives from the key distribution centre. If it contains sufficient attributes corresponding with access policy, subsequently it decrypts the information accumulated in the cloud.

4. CONCLUSION:

Resourceful search above encrypted data is moreover important concern within cloud system. We propose a decentralized access control method for effective storage of data in cloud system by means of anonymous authentication, which recommend user revocation and put off replay attacks. In initiated system, the cloud does not distinguish distinctiveness of user who accumulates information, but merely verifies user's credentials earlier than storing data. We suggest our privacy preserving authenticated access control scheme and consistent with our system a user can generate a file and store it strongly in cloud. Our system also has added feature of access control in which just applicable users are able to decrypt accumulated information. The system postpones replay attacks and maintains creation, modification, as well as reading data stored within the cloud. Our authentication in addition to access control system is decentralized and strong, complementary from other access control systems that are considered in support of centralized clouds. The system which was introduced consists of usage of two protocols such as attribute based encryption and attribute based signature.

REFERENCES

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

[2] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance," IACR Cryptology ePrint Archive, 2008.

[3] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.

[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.