Volume No:2, Issue No:3 (August-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Options for Managing and Decentralized Anonymous Authentication Information Stored in the Cloud

N.Swetha
M.Tech Student,
Dept of Computer Science Engineering,
Prasad College of Engineering.

P.Mounika
Assistant Professor,
Prasad College of Engineering.

ABSTRACT:

We provide a way to control decentralized new opportunities for storage security, supporting the authentication of the unknown. The scheme aims to prove the authenticity of the line does not know the identity of users before storing data. Also, we have a system as an addition of access control can decrypt user documents stored data. The system prevents repeated attacks and support the creation, modification, and read the data stored in the cloud. We also use memory. Moreover, our decentralized and agile authentication and access control scheme, unlike other access control system designed for such centralized. Communications, financial planning and arranging the same centralized manner.

INTRODUCTION:

Existing wok access to the centralized nature of the head. Other programs use resources based encryption (ABE). The program uses a symmetric key and to support authentication. It supports authentication scheme. Earlier work by providing confidential Zhao options for saving management certificate in the cloud. However, the authors of the centralized approach in which a distribution center (KDC) to distribute secret keys and values for all users. Unfortunately, one KDC only one part of the failure, but it is difficult to maintain due to the number of users supported in an environment when. Therefore, the stress will be a decentralized approach when distributing keys and hidden meaning for users. It is also natural that the existence of multiple KDC at different places in the world. Although Jang proposed a decentralized way, their way to authenticate users, who wish to remain anonymous while receiving head. In recent work, it was determined Sep way to control the distribution of access to the cloud. However, since the authentication program users. Another drawback is that the user can store the file and other users cannot read the file. are not allowed Book Group, except clams users. In the first edition, we expanded our work to date and additional parts cannot recognize the validity of posts, without revealing the names of consumers who are in the cloud. In this issue we also used the recall, do not talk. We use the basic signature program to realize the true against privacy.Our program to re-attack, where a user can change the data and information stolen from a recent letter, although the proposal as much a political document. a property important for the customer cancels their property, may not be able to write during the day. Therefore, this part of our program and the need to change. Also, our program has a lot of time is not allowed in our first job. The main contribution of this report are: 1) the information to control the distributed approach that are in the cloud, to allow customers and quality can be found. 2) user authentication for storage and changing data on the cloud. 3) The user identity is protected until duringauthentication.4) architecture is decentralized, which means that the KDC Management Center. 5) access control and authentication resistance collusion, which means two users can access information and collusion or authenticate yourself, if approved each of them. 6) cancellation can be achieved by using the information after the recall. 7) The program is designed to resist attack players. The author means the key has been revoked cannot write the information age. 8) The Agreement supports read and write data stored in the cloud. 9) The price is equal to the existing centralized and seems very expensive to work during the day. Available as found attention, because only allows users to have a significant service. A large amount of information stored in the cloud, and a lot of sensitive information. should be available to control access to the sensitive information is often related to health, important documents or personal information. There are three types of access control: user-based access control (Ubac), role-based approach control (RBAC), and information-based Access Control (ABAC). In Ubac, Access Control List (ACL) contains a list of users who are authorized to receive the information. Fair at the forefront of what most users.

Volume No:2, Issue No:3 (August-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

In RBAC, users are classified based on their individual responsibilities. Information can be found through the use of roles is similar. explained role in the system. For example, teachers and senior should be available, but with the clerk. ABAC is the most public in general, which provides users and granted access to information policy. Only users with a series of policy documents that meet the space, you can find information. For example, in the example data, you can find teachers and more than 10 years of research experience or higher with experience more than 8 years. discuss the advantages and disadvantages of RBAC and Sabac. There has been some work on ABAC during the day. All these operations are used for encryption primitive called encryption based on an attribute (Abe). It was suggested that control markup language Ektensible Access to ABAC during the day. The city used by the public the possibility of keeping healthy. used as the sensitivity of data storage to provide patients access to medical experts, hospital staff, scientists and politicians. It is important to control access to information that only users authorized to access the information. Using Abe, the data encrypted under certain policies and stored in the cloud. using a set of given characteristics and a key connection.

Once the appropriate set of characteristics, they cannot decipher data stored in the cloud. tested approach to maintaining health. Access control a significant increase in social networks on the Internet to users (people) to store personal information, photos, videos and share them with selected user groups or societies to which they belong. Access to social networks on the network under investigation. Information is stored in the cloud. It is important that only authorized users access to this information. A similar situation occurs when storing data in the cloud such as Dropbox and sharethem with specific groups of people. It is not enough to save it in a safe in the cloud, but it may also be necessary to ensure the anonymity of the user. For example, you want the user to store sensitive information, but do not want to know. You may want to write the user information for an article, but does not want to reveal his / her identity. However, it should be used to prove the other person is used to / as store information allows users without revealing identity. In the cryptographic protocols which alarm network signature, signature pieces, which can be used in the case. signature of mercy is not an easy decision for the material in a wide range of users. Group considers the signing of the pre-existence the group may not be able to go. Mesh signing to a message from a user or people who use a lot of conspiring together.

For these reasons, the signature of a new agreement called primary (ABS) is used. ABS planned to Maji. In ABS, users have logged predicate associated with the message. The need to help the predicate to identify the user as the only authorized, without revealing his identity. Viewers can or must be able to prove that the use and effect of the message warehousing. can be combined ABS and Abe received certificates Access Control without revealing the names of users in the cloud.

SYSTEM PRELIMINARIES:

1. System Initialization Module.
2. KDC Module
3. Trustee Module
4. Signature Module.

SYSTEM INITIALIZATION:

The introduction of our models cloud for storage and ideas that we have made in the newspaper. The head of the faithful-a-curious, which means that interest the manager must look concerned, but you cannot change. It can be used to read or write or access to a file stored in the cloud. All communication between the users / certificate before. To write to a file that is already there, to be sent in a message to the user to designate the policies made at the time of creating the file. Approved policy needs, and if the truth is allowed to write to the file.

KDC MODULE:

Note that, although they will need a decentralized approach when distributing secret keys and the means for users. It is also natural that the existence of multiple KDC at different places in the world. The architecture is decentralized, which means that the KDC Management Center. Thanks generations.Algorithm approval Mark S γ-themed TV using signature verification signature TPK.

TRUSTEE MODULE:

Commissioner may be some federal government manages the public social security number, etc. In this his ID (such as health / social security number), issued by the trustee to give him a sign. Several KDC, which can be disseminated. For example, they can serve different parts of the world. As creators submit proof of one or more KDC received keys for encryption / decryption and signing.

Volume No:2, Issue No:3 (August-2016) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

SIGNATURE MODULE:

Access policy determines who can access the data stored in the cloud. Creative policy planning applications and confirms its right message character in accordance with this proposal. C ciphertext and signature C, and sent to the cloud. Certified as a signature and save the ciphertext C. When the readers to read, send and C. If the user has the necessary assets to policy, you can decrypt and recover process prior authorization messages .the day, relieves users from consuming approval. When you read will read the data stored in the cloud, in an attempt to decipher with the keys on the secret comes from the KDC.

RELATED WORK:

Abe was designed by Sahai and water [26]. In Abe, a user with a set of attributes, as well as its unique ID. There are two types of Abes. The benchmark interest or a KP-Abe Abe, the sender has access policy for data encryption. The author means the key has been revoked can not write the information age. Finding available for the key secrets of nature and can decrypt the data if the same meaning. In politics Ciphertext CP-Abe receiver has access to the policy in the form of wood, as well as a display and monotone access structure and AND, OR gates and doors. all centralized way and leave only one KDC, a part failure. Chase suggested another manager Abe, which is the number of KDC (coordinated by the Trust Management) distribute the secret key users. Various authorities Abe studied agreement that does not require reliable power required by the user, each character from the KDC. Recently Levko and Vaters Abe proposed decentralized perfect can be used as or more characteristics of the individual and does not require the employee trust. In all these cases, the computation intensive decryption of the end user. To be able to use this technique when you can get customers through their mobile devices. To overcome this problem, the proposed Green decryption work to engage representatives of workers, allowing the user to read a minimum of resources (such as handheld devices). But it is a member and a key distribution center for less than a strong decentralized manner. These methods are a way to authenticate users discover. Jang gives climate, loyal customers, who wish to remain anonymous while receiving head. To ensure that learning about authentication using the principles identified by the sign of the Maya. There is also a centralized system.

The program was recently the author himself is a decentralized manner and provide authentication without revealing the identity of the user. But, as mentionedbefore the first group under the influence of repeated attacks.

CONCLUSION:

We provide a way to control access through decentralized anonymous authentication, which gives the user the gap and prevent relapses. Do you know the name of the customer, store information, but only confirms the character profile. The distribution of key policy decentralized. One limitation is that while entering information policy for each data stored in the cloud. In the future we want to hide assets and access policies for users.

REFERENCES:

[1] S. Ruj, M. Stojmenovic, and A. Nayak, “Privacy Preserving Access Control with Authentication for Securing Data in Clouds,” Proc. IEEE/ACM Int’l Symp.Cluster, Cloud and Grid Computing, pp. 556-563, 2012.

[2] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, “Toward Secure and Dependable Storage Services in Cloud Computing,” IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.- June 2012.

[3] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, “Fuzzy Keyword Search Over Encrypted Data in Cloud Computing,” Proc. IEEE INFOCOM, pp. 441-445, 2010.

[4] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc. 14th Int’l Conf. Financial Cryptography and Data Security, pp. 136- 149, 2010.

[5] 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.

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

[7] 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.

Volume No:2, Issue No:3 (August-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

[8] R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B.S. Lee, "Trustcloud: A Framework for Accountability and Trust in Cloud Computing," HP Technical Report HPL-2011-38, http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html, 2013.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 282-292, 2010.

[10] D.F. Ferraiolo and D.R. Kuhn, "Role-Based Access Controls," Proc. 15th Nat'l Computer Security Conf., 1992.

[11] 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.

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

[13] 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.

[14] G. Wang, Q. Liu, and J. Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services," Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp. 735-737, 2010.

[15] F. Zhao, T. Nishide, and K. Sakurai, "Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems," Proc. Seventh Int'l Conf. Information Security Practice and Experience (ISPEC), pp. 83-97, 2011.

[16] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," Proc. IEEE 10th Int'l Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), 2011.

[17]http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-cs-01-en.pdf, 2013.

[18] http://securesoftwaredev.com/2012/08/20/xacml-in-the-cloud, 2013.

[19] S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), 2011.

[20] 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.