Volume No:1, Issue No:7 (December-2015) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

Anonymous Cloud Storage to Centralize Access Control

Hareesh Dharmapuri
M.Tech Student,
Department of CSE,
Adam's Engineering College.

B.Simmi
Associate Professor & HOD,
Department of CSE,
Adam's Engineering College.

ABSTRACT:

Under the proposed system, the user is unaware of the identity authenticated by a series of data stored in the cloud. Valid only for users of our plans feature access control is added to decrypt the data stored. The plan has been attacked and stored in the cloud, creating change, and information to prevent the reading support. We also address the cancellation to the user. In addition, unlike other access control schemes designed our centralized authentication and access control schemes for the cloud, decentralized and strengthened. The calculation of the communication, and storage costs are similar to the centralized approach.

I.INTRODUCTION:

Both academic and industrial research in line with the Cloud and a lot of attention is. And Cloud, (also known as clouds) Internet users under their external servers can be calculated and collected. Users of this site equipment maintenance armed conflict free. Applications for writing applications (eg, Google Apps, Microsoft Online), infrastructure (eg, Amazon EC2, Eucalypts, Nimbus) cloud platform and services, such as various types of investors (eg, help can be provided, Amazon S3, Windows Azure). Many data, for example, medical records stored in the cloud and social media are extremely sensitive.

Security and privacy, said, cloud computing, they are very important. On the one hand, the user must authenticate himself before starting any transaction, on the other hand, it is not sure that the plutonium should be outsourced cloud data. Unknown user privacy and user identity from clouds or other users are required. Clouds can be held responsible for the user, and so, give details of the cloud service provider should be responsible for it. The data collected will also contribute to user testing. In addition to technology solutions to ensure security and privacy, law enforcement will need.

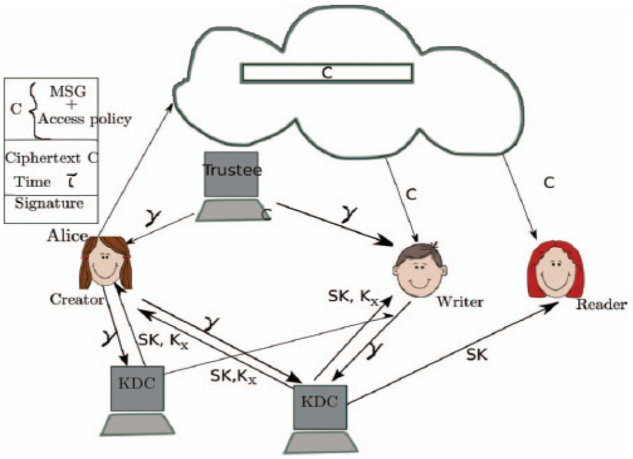
Cloud data storage has led to ensure that we give support to establish the identity of an anonymous access control scheme proposed decentralized news. Under the proposed system, the user is unaware of the identity authenticated by a series of data stored in the cloud. Valid only for users of our plans feature access control is added to decrypt the data stored.

II.RELATED WORK:

Many data, for example, medical records stored in the cloud and social media are extremely sensitive. Security and privacy, said, cloud computing, they are very important. On the one hand, the user must authenticate himself before starting any transaction, on the other hand, it is not sure that the plutonium should be outsourced cloud data. Unknown user privacy and user identity from clouds or other users are required.

Clouds can be held responsible for the user, and so, give details of the cloud service provider should be responsible for it. The data collected will also contribute to user testing. In addition to technology solutions to ensure security and privacy, law enforcement will need.loud ensure that we support anonymous authentication for secure data collection plan to propose a new decentralized access control. Under the proposed system, the user is unaware of the identity authenticated by a series of data stored in the cloud.

Valid only for users of our plans feature access control is added to decrypt the data stored. The plan has been attacked and stored in the cloud, creating change, and information to prevent the reading support. We also address the cancellation to the user. In addition, unlike other access control schemes designed our centralized authentication and access control schemes for the cloud, decentralized and strengthened. The calculation of the communication and storage costs are similar to the centralized approach.



Figure(1) : Context Diagram of Project

III.SYSTEM PREMELERIES:

A.System Initialization:

We represent our cloud storage model assumptions anti-paper model. User Content Administrators strange-but the honest, down to the cloud can be interested, but it can not be changed. Users either or both read and write access to files can be stored in the cloud. Users / All communication between the cloud is secure. Write file already exists, the user must send a message files created in the policy statement. The cloud that policy, and the user is authorized, will write on the file.

B.KDC Module:

When stressed that the distribution of keys and clouds for users, access points should be decentralized. It is also very natural, with many KDCs, clouds around in different places. It means that the KDCs decentralized management architecture, can be different. TPK is the token signature verification certificates containing the signature algorithm television confirmed using γ.

C. Trustee Module:

Trustee her identity (health / social security number), social insurance number, etc. As one of the federal government's management would like to submit, the trustee can give her a token. Many are KDCs, can be scattered. For example, the server may be different countries of the world. One or more KDCs encryption keys to builder / realm, and the signature symbols on.

D.Signature Module:

Access policy is decided can access data stored in the cloud. Y rights policies and messages signaling decision, saying the Creator to ensure its authenticity. Replacement signed with the cipher text C systems, and will be sent to the cloud. When the reader want to read the signature of cloud storage by a ciphertext C, ensuring user access to cloud policy changes and has qualities, it can decrypt the original message it sends back to C .. Cloud testing process, it relieves personnel from test of time. The reader gets a KDCs using decrypt secret keys stored in the cloud need to read some data.

IV.CONCLUSION:

We canceled the attack back to the user and allows the ruling prevents the anonymous access authentication with decentralized technology. Cloud data storage has to know the identity of the user, but only user certificates are not sure. The main distribution is decentralized manner. Stored in the clouds know the policy limit access to each report. The future, we need to hide user characteristics and usage policy.

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.

[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.