International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Survey Paper on User Anonymous Authentication Scheme for Decentralized Access Control in Clouds

Afsha Pathan[1], M. D. Ingle[2]

[1]M.E(Computer) Department of Computer Engineering, Jaywantrao Sawant College of Engineering, Pune, India, Savitribai Phule University of Pune, Maharashtra, India -411007

[2]M.E Coordinator and Assistant Professor (Computer) Department of Computer Engineering, Jaywantrao Sawant College of Engineering, Pune, India, Savitribai Phule University of Pune, Maharashtra, India -411007

Abstract: ***The idea is to propose a new decentralized access control scheme for achieving security in data stored in clouds that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the series without knowing the user's identity before storing data in cloud. Here we also have added feature of access control so that only valid users are able to decrypt the data i.e. stored in cloud. The proposed scheme also prevents replay attacks and supports alteration of data and reading data stored in the cloud. We also address user revocation. Moreover, the proposed authentication and access control scheme is decentralized and robust, unlike the existing access control schemes that are centralized. So that here communication, computation, and storage overheads are comparable to centralized approaches.***

Keywords: Decentralized, Authentication, Attribute based encryption, Attribute based signatures, Access Control

1. Introduction

Cloud computing is a promising computing model which currently has drawn far reaching consideration from both the educational community and industry. By joining a set of existing and new procedures from research areas, for example, Service-Oriented Architectures (SOA) and virtualization, cloud computing is viewed all things considered a computing model in which assets in the computing infrastructure are given as services over the Internet.

It helps associations and government offices fundamentally decrease their financial overhead of data administration, since they can now store their data reinforcements remotely to third-party cloud storage suppliers as opposed to keep up data centers on their own. Numerous services like email, Net banking and so forth… are given on the Internet such that customers can utilize them from anyplace at any time. Indeed cloud storage is more adaptable. The three points of this issue are availability, confidentiality and integrity.

Most of our data is stored on to the cloud. But the data i.e. stored on to the cloud is highly sensitive because here we are trusting on third party who will maintain our data. Sensitive data can be medical records and social network data. So here Security and privacy are two main issues while storing data on clouds. So that whenever user wants to access data on cloud, he should authenticate himself before initiating any transaction. Preservation of user's privacy is also important so that other user and cloud also don't know the identity of the owner of file.

Anonymous authentication is the procedure of accepting the client without the details of the client. So the cloud server doesn't know the details of the client, which gives security to the clients. Security and privacy assurance in clouds are analyzed and tested by numerous researchers. [3] Gives storage security utilizing Reed-Solomon eradication correcting codes. Utilizing homomorphism encryption, [4] the cloud gains cipher text and furnishes an encoded value of the result.

To understand the concept in detail here we take one example, Suppose A engineering student John, wants to send some reports about some mismanagement by higher authorities of institute A to all the professors of institute A, all the institutes in country and all the students of engineering department. And he also wants to remain anonymous by providing all the evidence of mismanagement. He will store all the data on to cloud. And he will provide access only to authorized users. Here access control scheme is important.

Access control in cloud is gaining much attention because it is important to give access only to the authenticate user. As much amount of information is stored on cloud. This is information can be person's health information (medical record), personal information (social networks data). So to keep this sensitive information safe access control is important. There are mainly three types of access control: user based access control(UBAC), role-based access control(RBAC), attribute based access control(ABAC).In user based access control scheme, we'll maintain one list of users who are allowed to access data. But this is not flexible scheme for cloud because there are many users and it not possible to maintain such long list of user. In role based access control scheme, access right is given depend upon the role of the person. Here role can be professor, assistant professor, or student [6].ABAC is the extended version of these both. In this user is given some set of attribute, and the data is attached to access policy. The users who will have the valid set of attributes only allow to access the data. For example according to above example the professor having 10 years of teaching experience are allowed to access the data stored on the cloud. The advantages and disadvantages of RBAC and ABAC are discussed in [7].

It is not just that user can store sensitive information on cloud but there is another issue of user's anonymity. Such that it is necessary to ensure the anonymity of user .For example, if user wants to store some information but doesn't want to recognized. Suppose one wants to post some comment about article but wants to remain anonymous. However user should prove to the other users that he is valid user and the data created by him is also valid. Some Cryptographic protocols such as ring signatures [12], mesh signatures [13], Group signature [14] are used whenever such situation occurs.

2. Literature Survey and Related Work

Existing system on access control is totally centralized in nature [8].In [8] online patients personal record is maintained that will enable patient to maintain his/her personal medical record. But this scheme maintains data in centralized way. When user wants to store his personal data on to the cloud, he will first encrypt that data so that no one can access to that data. Another scheme [20] and [11] that uses attribute based encryption. But scheme used in [20] doesn't support authentication.

The existing scheme described in [9] provides privacy preservation and access control in cloud. It uses single key distribution centre (KDC) that distributes secret keys to the users. Unfortunately there is disadvantage of single point failure. And also it is difficult to maintain because there are large number of users in cloud and it is difficult for single KDC to generate such a large number of secret keys. So that in proposed scheme we are using decentralized scheme. Another scheme proposed in [10] also provides distributed access control to cloud. But it doesn't provide user authentication. But there are some disadvantages that are user only can read the file stored on the cloud. Write access is not given to the common user; it is given only to the creator. In the previous paper [1] all the other existing work is extended by checking the validity of each message without revealing the user's identity.

ABE (Attribute based encryption) was proposed by Sahai and Waters [16].In ABE; user is given a set of attributes along with its unique ID. There are two main classes of ABE: Key policy based ABE (KP-ABE) and Cipher policy based ABE (CP-ABE). In KP-ABE, the cipher text is associated with the set of attributes and secret key is associated with the access policy. The encryptor needs to define the set of attributes required to decrypt the cipher text, the trusted party who generates the secret key for user also defines combination of attributes for which secret key can be used. In CP-ABE the concept is totally reversed, here cipher text is associated with the access policy and secret key is associated with set of attributes. Here encrypting will decide under which policy the data is decrypted.

All these system we have seen till uses centralized approach and having only one KDC which is efficient because there are chances of single point failure. The system proposed by Chase [17] is multiauthority ABE, which having several KDC's and it'll secret keys for the user and distribute it among different user. Multiauthority ABE i.e. given in [18] and [19] it requires that user must have the attributes from all the KDC's. But all these cases the main limitation is that computation is intensive so that it might be inefficient when user access the data via mobile device. So to address this limitation, Green et.al. Proposed a scheme to outsource the decryptions task on to the proxy server. But the presence of one KDC and one proxy makes it less robust. Yang et.al [20] presents a scheme in that it allows authentication of user while remain anonymous.

3. Proposed System

The new system provides the user privacy as well as data security. It also provides the access control over the data. The user privacy is maintained by anonymous authentication.

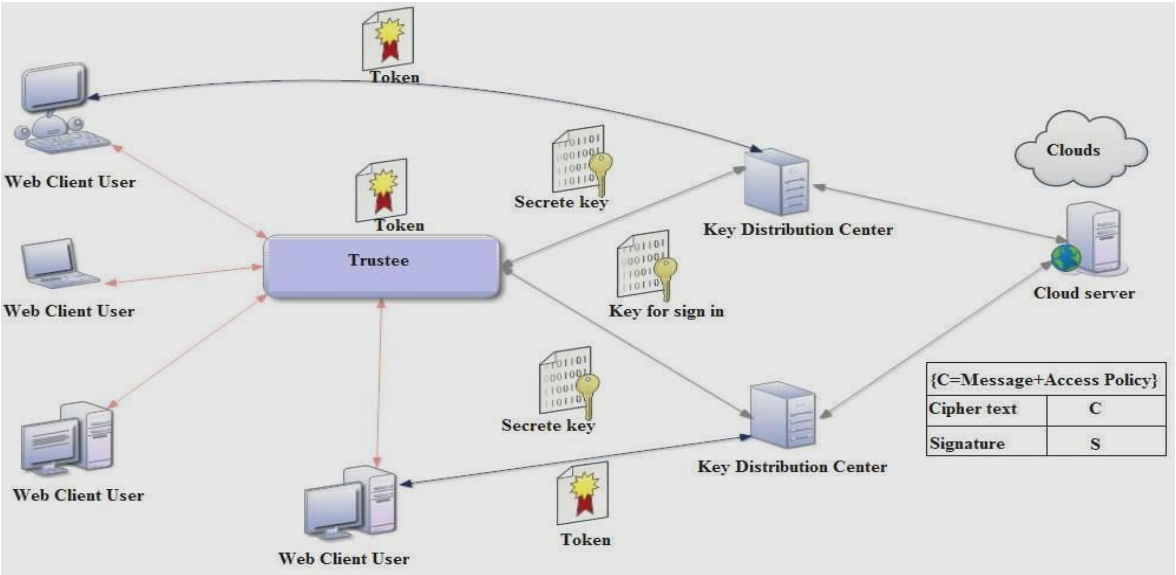

Figure 1: System Architecture of Proposed System

In Proposed scheme, we can securely store the data on to the cloud using decentralized access control with anonymous authentication. The architecture of a proposed scheme given in Figure 1. is decentralized, meaning that there can be several KDCs for key management. The access control and authentication are both collusion resistant, meaning that no two users can collude and access data or authenticate themselves, if they are individually not authorized.

Uploading and downloading of a file to a cloud with standard Encryption/Decryption is more secure. Revocation is the important scheme that should remove the files of revoked policies. So no one can access the revoked file in future. The policy renewal is made as easy as possible. The renew key is added to the file. Whenever the user wants to renew the files he/she may directly download all renew keys and made changes to that keys, then upload the new renew keys to the files stored in the cloud.

4. Conclusion

In this paper, I have presented a decentralized access control scheme with anonymous authentication, which provides user revocation and prevents replay attacks. Here cloud doesn't know the identity of the creator of data, but only verifies the user's credentials. In decentralized way key distribution is done.

So we have achieved security in proposed system using decentralized access control with anonymous authentication. The files are associated with file access policies, that used to access the files placed on the cloud. In future the file access policy can be implemented with Multi Authority based Attribute based Encryption. Here cloud knows the access policy of the user so that it can be the limitation in same case. So that in future I would like to hides the attributes of the user from cloud. So that data stored on cloud can be more secure

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] D.F. Ferraiolo and D.R. Kuhn, "Role-Based Access Controls, " Proc.15th Nat'l Computer Security Conf., 1992.
[6] 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.
[7] 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.
[8] 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.
[9] http://securesoftwaredev.com/2012/08/20/xacml-in-the-cloud, 2013.
[10] R.L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret, "Proc.Seventh Int'l Conf. Theory and Application of Cryptology and InformationSecurity (ASIACRYPT), pp. 552-565, 2001.
[11] X. Boyen, "Mesh Signatures, " Proc. 26th Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 210-227, 2007.
[12] D. Chaum and E.V. Heyst, "Group Signatures, " Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 257-265, 1991.
[13] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures, " Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.
[14] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption, " Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, 2005.
[15] M. Chase, "Multi-Authority Attribute Based Encryption, " Proc.Fourth Conf. Theory of Cryptography (TCC), pp. 515-534, 2007.
[16] 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.
[17] 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.
[18] K. Yang, X. Jia, and K. Ren, "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems, " IACR Cryptology ePrint Archive, p. 419, 2012.
[19] W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and Efficient Access to Outsourced Data, " Proc. ACM Cloud Computing Security Workshop (CCSW), 2009.
[20] W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and Efficient Access to Outsourced Data, " Proc. ACM Cloud Computing Security Workshop (CCSW), 2009.

Author Profile

Ms. Afsha A.Pathan, is currently pursuing M.E (Computer) from Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. She received her B.E (Computer) Degree from UCOER, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. His area of interest is Network Security and Cloud Computing.

Asst Prof. M.D Ingle, received his M Tech. (Computer) Degree from Dr. Babasaheb Ambedkar Technological University, Lonere, Dist. Raigad-402 103, Maharashtra, India. He received his B.E (Computer) Degree from Govt college of Engineering, Aurangabad, Maharashtra, India.He is currently working as M.E coordinator and Asst Prof (Computer) at Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India - 411007. His area of interest is network security and Cloud Computing.