International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Privacy Preserving DAC for Data in Cloud

Pankaj R. Chandre[1], Swati S. Gore[2]

[1]Professor, Computer Engineering, SPCOE, Otur, Pune, Maharashtra, India

[2] Computer Engineering, SPCOE, Otur, Pune, Maharashtra, India

Abstract: ***A large amount of information is being stored in the cloud and much of this is sensitive information. Here proposed a new decentralized access control (DAC) scheme for secure data storage in clouds that will support anonymous authentication. In this system, the cloud will verify the authenticity of the series of users without knowing the users identity before storing data in cloud. This system also has the more feature of access control where only valid users are able to decrypt the stored information in cloud. The System prevents replay attacks and supports create, modify, and read data stored in the cloud. This System also addresses user revocation. Also this authentication and access control scheme is decentralized and robust in nature, unlike other access control schemes for clouds which are centralized. The computation and storage overheads in this system are comparatively same to centralized approaches. Much of data stored in cloud is sensitive so this system is efficient. It can be used for various applications such as storing health care information, in online social networking where users store their personal information and share with selected groups of users or communities they belongs to.***

Keywords: Access Control, cloud storage, ABS, ABE.

1. Introduction

Cloud computing is probably the most cost efficient method to use, maintain and upgrade. Storing information in cloud gives you almost unlimited storage capacity. Hence there is no need to worry about running out of storage space or increasing your current storage space availability. It is not only important that we store data in cloud securely but it is also necessary to remain unidentified and unnamed for the user. For example, a user would like to store some sensitive information but does not want to be recognized himself. Suppose the user might want to post a comment on some article, but does not want his/her identity to be known to others. However, the user should be able to prove that he/ she is a valid user to the other users, that he/she stored the information without revealing his or her identity.

Consider now the following example. Patients store their medical information in the cloud. Different users can access different fields. The same fields might be accessed by a selective group of people who are authorized group. For example the patient's medical history and drug administration can be accessed by doctors, nurses but not by hospital management staff.

Access control is very important term in online social networking where members store their personal information, videos, and pictures and share them with selected groups of users or communities they want to. Access control gives accesses to resources by some principles. Such data are being stored in clouds. It is very important that only the authorized users are given access to that information. A similar situation is there when data is stored in clouds, for example, Dropbox, and shared with certain groups of people. The proposed scheme is decentralized, means that there are several KDCs for key management. The authentication provided and access controls are both collusion resistant, meaning that no two users can collaborate and access data and authenticate themselves, if the users are not individually authorized. Revoked users cannot access data in cloud after they have been revoked from the system. The proposed scheme is resilient for replay attacks. A writer whose attributes and keys have been revoked from the system cannot write back the information. The protocol supports multiple read and writes on the data stored in the cloud. The costs are same to the centralized scheme, and the expensive operations are performed by the cloud.

This system uses the cryptographic technique called Attribute Based Encryption (ABE) to achieve access control in clouds. Using ABE, owners encrypt data with attributes that they possess and store the information in the cloud. The cloud is unable to decode stored data. Users are given attributes and secret keys by a key distribution center (KDC). Those with matching set of attributes are able to decrypt the information.

2. Literature Survey

First consider some attribute based encryption schemes best suited for data access control. Sahai and Waters[6] introduced the concept of Attributed-Based Encryption (ABE). In an ABE system, the user's keys and ciphertexts are labelled with sets of descriptive attributes and a particular key can decrypt a particular ciphertext only if there is a match between the attributes of the ciphertext and the user's key. The cryptosystem of Sahai and Waters is allowed for decryption when at least m attributes overlapped between a ciphertext and a private key. While this primitive was shown to be useful for error tolerant encryption using biometrics, the lack of expressibility seems to limit its applicability to larger systems. Identity-based encryption (IBE) was proposed by Shamir and has been extensively studied. Each user in an IBE scheme has a unique identity, and the only public key is the unique information about the user. IBE is a special case of ABE. There are two classes of ABE. In Key-policy ABE or KP- ABE [9], the sender has an access policy to encrypt data. The receiver receives the attributes and secret keys from the attribute authority and is able to decrypt information only if it has matching attributes. In Ciphertext-policy, CP-ABE [7][8] the receiver has the

access policy in the form of a tree, with attributes as leaves and monotonic access structure with gate AND,OR and other threshold gates.

The attribute authority that is KDC in all mentioned protocols is assumed to be honest. However, this may not hold, because in a distributed system, authorities can fail or be corrupt. Chase [11] proposed a multi-authority ABE system, in which there are different KDC authorities (coordinated by a trusted authority) which distribute attributes and secret keys to users. Chase and Chow[13] devised a multi-authority ABE protocol which required no trusted authority. However, the main problem was that a user required at least one attribute from each of the authorities, which might not be practical. Recently Lewko and Waters[12] proposed a fully decentralized ABE, where users could have zero or more attributes from each authority and did not require a trusted server. Their protocol has been recently used to achieve access control in intelligent transport system. This helps the vehicles to transmit messages, such that only authorized vehicles can receive them.

ABS (Attribute Based Signature) was proposed by Maji et al. [14]. In ABS, users have a claim predicate associated with their message. The claim predicate helps to identify the user as an authorized one, without its identity to be revealed to other. Other users or the cloud can verify the user and the validity of the message stored. ABS can be combined with ABE to achieve authenticated access control without disclosing the identity of the user to the cloud. Attribute-based signature (ABS) enables users to sign messages over attributes without revealing any information other than the fact that they have attested to the messages [10]. However, heavy computational cost is required during signing in ABS, which grows linearly with the size of the predicated formula. As a result, this presents a significant challenge for resource-constrained devices (such as mobile devices or RFID tags) to perform such heavy computations independently.

3. Existing System

Consider a situation in which owners want to store their information in the cloud while users want to access the same information from the cloud. Here do not consider computations in cloud. In a health-care example, owners can be the patients who store their records in the cloud, and doctors, nurses, researchers, insurance companies can retrieve them. There are multiple KDCs which may be even servers that are located in different countries that generate secret keys for the users.

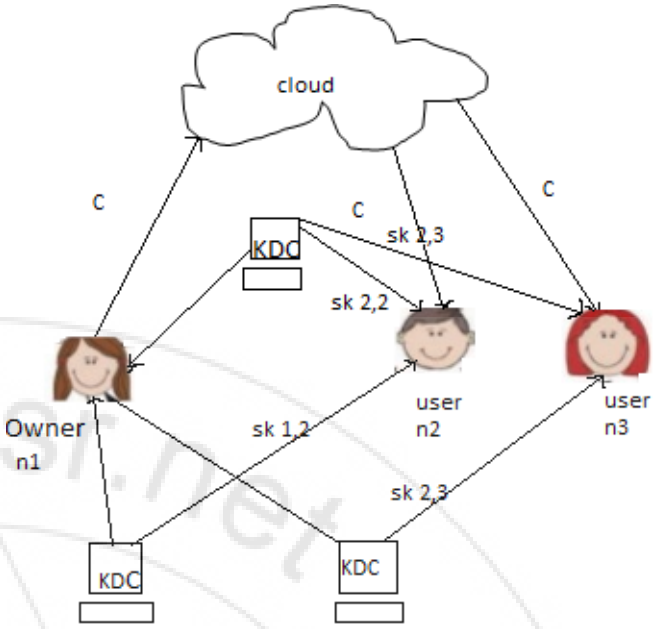

Figure 1: Existing System

KDCs can be government organizations which give different credentials to users. These servers can be maintained by separate companies, so that they do not collude with each other. This differs from the traditional concept of cloud. A particular cloud is maintained by one company, thus if KDCs are a part of the cloud then they can collude and find the secret keys of users. Users and owners are denoted by n_i, KDCs are servers which distribute attributes and secret keys sk to users and owners. KDCs are not part of the cloud. The owner has permission to encrypt message and store the ciphertext C in the cloud. Here one limitation is that cloud knows the access policy of the user who stores the information.

4. Proposed System

According to this scheme of Privacy Preserving Decentralized Access control for Data in Cloud, a user can create a file and store it securely in the cloud. The limitations in previous scheme are removed. Cloud does not know the access policy of the user. This scheme consists of use of the two protocols ABE and ABS. Now discuss this scheme in details. Refer to the Fig. 2. There are three users a creator, a reader, and writer. Creator receives a token γ from the trustee, who is assumed to be honest. A trustee can be someone like the federal government who is responsible for managing social insurance numbers etc. On presenting her/his id (like health/social insurance number), the trustee gives her/him a token γ.

There are multiple KDCs used in this system, which can be scattered at different location. For example, these can be different servers in different parts of the world. A creator when gives the token to one or more KDCs they receives keys for encryption or decryption and signing. In the Fig. 2, sk is secret key given for decryption, kx is key used for signing. The message is encrypted under the access policy. The access policy will decides who can access the data stored in the cloud. The creator will decide on a claim policy, to prove her/his authenticity and signs the message under this claim.

The ciphertext with signature is C, and give to the cloud. The cloud verifies the signature and it stores the ciphertext C. When a reader wants to read the data in cloud, the cloud sends ciphertext C. If the user has attributes matching with given access policy, it can decrypt and get its original message. Write proceeds in the similar way as file creation.

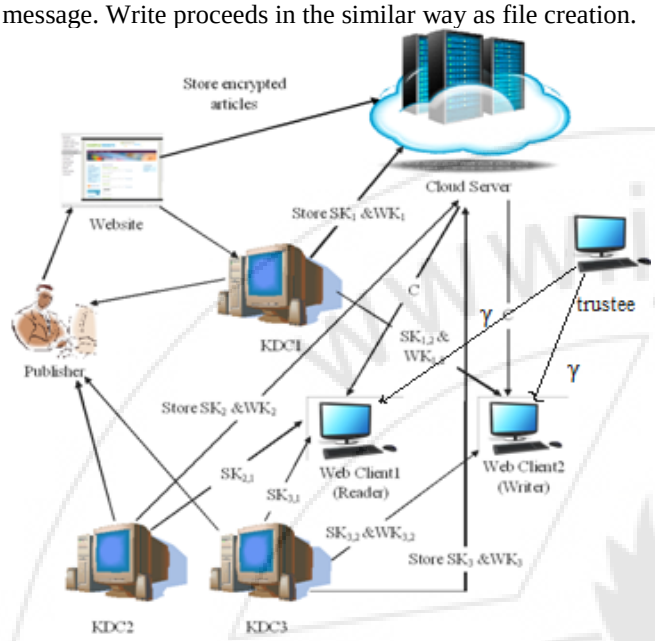

Figure 2: Proposed System

By assigning the verification process to the cloud, it will help to relieve the individual users from the required time consuming verifications. When a reader needs to read some data stored in the cloud, it will tries to decrypt it using the secret keys it receives from the KDCs. If there is sufficient attributes matching with the access policy, then it decrypts the information stored in the cloud.

5. Conclusion

Here proposed secure cloud storage using decentralized access control with anonymous authentication. Revocation is the important scheme that should remove the files of revoked users from the system. The cloud does not know the identity of the user who stores the information. Key distribution is done in decentralized manner. Cloud is unknown to the access policy for each record stored in the cloud.

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. Gentry, "A Fully Homomorphic Encryption Scheme," PhD dissertation, Stanford Univ., http://www.crypto.stanford.edu/ craig, 2009

[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] Sushmita Ruj, Amiya Nayak and Ivan Stojmenovic "DACC: Distributed Access Control in Clouds" *International Joint Conference of IEEE TrustCom*-11/IEEE ICESS-11/FCST-11, 2011

[5] 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.

[6] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. Ann. *Int'l Conf. Advances in Cryptology (EUROCRYPT)*, pp. 457-473, 2005.

[7] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. *IEEE Symp. Security and Privacy*, pp. 321-334, 2007.

[8] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption," Proc. *ACM Symp. Information, Computer and Comm. Security (ASIACCS)*, pp 343-352, 2009.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. *ACM Conf. Computer and Comm. Security*, pp. 89-98, 2006.

[10] Jingwei Li, "Secure Outsourced Attribute-based Signatures", *IEEE Transactions on Parallel & Distributed Systems*, no. 1, pp. 1, PrePrints PrePrints, doi:10.1109/TPDS.2013.2295809

[11] M. Chase, "Multi-Authority Attribute Based Encryption," Proc. *Fourth Conf. Theory of Cryptography (TCC)*, pp. 515-534, 2007.

[12] A.B.Lewko and B.Waters, "Decentralizing attribute-based encryption," in EUROCRYPT, ser. Lecture Notes in Computer Science, K. G. Paterson, Ed., vol. 6632. Springer, 2011, pp. 568–588.

[13] M. Chase and S. S. M. Chow, "Improving privacy and security in multi- authority attribute-based encryption," *in ACM Conference on Computer and Communications Security*, 2009, pp. 121–130.

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