International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

A Survey on Anonymous User Authentication using Decentralized Key Distribution Architecture

Purva Chavan[1], Prof. B. P. Vasgi[2]

[1, 2]Sinhgad College of Engineering, Pune, Maharashtra, India

Abstract: ***One of the powerful features of Cloud Computing is storing data at the third party site without the hassles of maintenance, storage space, etc. Decentralized access control scheme can be used for securely storing data onto clouds. The scheme enables anonymous authentication of users by hiding user's details from the cloud before storing the data. The access control scheme enables the owner of data to grant read and write access only to those who satisfy certain attributes specified by the owner and thus are the valid users. It supports decentralized architecture which prevents single point of failure and workload on a single system. The scheme is thus robust. Also it supports user revocation to prevent stale entry of data.***

Keywords: access control, authentication, key distribution center, attribute based encryption, cloud storage

1. Introduction

Cloud computing provides anywhere anytime ubiquitous service using the internet which has made it popular in today's technology oriented world. One of the powerful features of cloud is enormous storage at third party site. It frees the users from the overhead of maintaining resources on site and also services are provided at lower costs whenever needed.

Cloud provides the facility of storing innumerous amount of data along with easy access. But this comes with concerns like privacy and security because much of the data stored in cloud contains highly sensitive information like medical records and social networks. Thus, proper techniques need to be implemented to safeguard the outsourced data. **Major Headings**

1.1. User Privacy and Data Security

User Privacy refers to keeping the identity of users confidential. There are situations where a user who created the data wants to remain anonymous.

Example: Bob is a law student and wants to send a series of reports about malpractices being carried out by the authorities of some university X to all the chairpersons, professors, students of that university. He wants to remain anonymous while publishing all evidences. All the information is stored in cloud. Here it is important the identity of Bob should not be revealed to others. For this purpose a claim message is also need to be sent which guarantees that message came from a valid source[10].

Data security is commonly referred to as the confidentiality, availability, and integrity of data. It is the practice of ensuring that the data is safe from unauthorized access and use, ensuring that the data is reliable and accurate and is available for use whenever it is needed[10].

2. Related Work

In the year 1992, D.F. Ferraiolo and D. R. Kuhn gave the concept of Role-Based access control where the user holding certain role was only allowed to access stored data. This scheme did not give fine grained access control. More powerful schemes were derived later. In the distributed systems users should be able to access the data only if a user possesses certain set of attributes. Attribute-Based encryption for fine grained access control of encrypted data was the scheme proposed by V. Goyal, O. Pandey A. Sahai, B. Waters in the year 2006[1]. User satisfying the attributes was only able to access the data. Access policy containing set of attributes was defined which defines the kind of users having access to data. Key Policy based schemes allowed for the policy as part of the key and ciphertexts carry attributes. Ciphertext Policy attribute based encryption concept given by Z. Liu, Z. Cao, Duncan S. Wong[2] embeds the policy or circuit as to who can decrypt the data as part of the ciphertext. In 2013, sauthors Ming li, Shucheng Yu[8] came up with the concept of securely maintaining Personal Health Records at the third party site. The PHR service allowed the patient to create and manage their medical history in one place by means of web. The data stored was encrypted first before outsourcing it onto semi-trusted cloud. In 2014, Decentralized access control architecture with anonymous authentication concept was laid by S. Ruj, M. Stojmenovic amd A. Nayak[10]. The scheme is robust, secure and hides the identity of owner of the data. Keys are distributed in a decentralized fashion, thus avoids single point of failure which means there can be several KDC's (Key Distribution Center) for key management. Only users with valid set of attributes are able to access data stored on cloud. User whose access rights have been revoked cannot enter data on cloud. Thus, preventing stale data entry in the storage environment and is resilient to replay attacks. Unlike previous scheme, it supports multiple reads and writes.

Information is at major risk at the third party site. Recent years have seen much technological advancement in the field of security for data stored in cloud. Continuous efforts have led to some secure mechanisms like Attribute Based encryption, use of Key Management Centers for the

distribution of Keys, inclusion of third party agencies for verification of users, etc.

Following table lists out the advancements and technique that has been implemented to enhance the security level of data stored in cloud.

3. Comparison Chart

Ref. No	Title	KDC Approach	Technique	Advantages	Disadvantages
[1]	Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data	Centralized	Key-policy based system is used for fine-grained sharing of encrypted data. The scheme associates ciphertext with set of attributes defined by the creator of the message. ABE algorithm allows users to encrypt and decrypt messages based on user attributes. Access policy determines which user is able to decrypt the data.	a)Eliminates the need to rely on the storage server for preventing unauthorized data access.	a) User identity revealed. b) Increased complexity because policies are embedded in user's key
[2]	Ciphertext-Policy Attribute-Based Encryption.	Centralized	The system attributes are used to describe user credentials, and a party encrypting data determines a policy for who can decrypt. In this, the policy or the circuit as to who can decrypt the data is embedded as the part of the ciphertext and the keys are associated with the attributes. Attribute based encryption binds the access-control policy to the data and the users (clients) instead of having a server mediating access to files.	a) Encrypted data is kept confidential even if storage server can't be trusted. b) Secure against collusion attacks.	a) User identity revealed. b) Access Control is not distributed giving rise to single point of failure.
[3]	Adding Attributes to Role-Based Access Control	Centralized	Explosion of roles results in thousands of separate roles assigned for various kinds of permission thus providing more fine-grained access control	a) More defined roles results in greater security. b) Ease of user provisioning c) Ability to quickly determine the maximum permissions available for a user d) Covers every possible contingency for permission sets that might be required by users.	a) User identity revealed. b) Access Control is not distributed giving rise to single point of failure.
[4]	Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings	Centralized	Personal health records are stored online in a centralized fashion. Leveraging the data to cloud enables scalable computing power, reduced operational cost and maintenance. Attribute based encryption is used to ensure security of data stored onto cloud. Key distribution overhead is reduced by dividing the system into multiple security domains where each domain manages only a subset of users	a) Control over one's own privacy b) Reduces key distribution complexity	a) Load on a single system because of single KDC
[5]	Attribute based data sharing with attribute revocation.	Centralized	Ciphertext-Policy Attribute based encryption (CP-ABE) technique enables fine-grained access control of data stored on clouds. It associates each user with a set of attributes and only user's with matching attributes are able to decrypt the data. In addition it supports revocation of user attributes. This task is accomplished by integrating technique of proxy re-encrypt with CP-ABE. Most of the major tasks are handed over top proxy servers.	a) Fine grained access control b) Enhanced security because of proxy servers c) Users whose attributes are revoked cant access data	a) Single KDC architectures acts a point of failure
[6]	Efficient Generation of Linear Secret Sharing Scheme Matrices from Threshold Access Trees	Centralized	Linear Secret Sharing Scheme (LSSS) matrices are commonly used for implementing monotone access structures in highly expressive Ciphertext-Policy Attribute-Based Encryption (CP-ABE) schemes. AND and OR gates are the special cases of the general (t; n)-threshold gates, not only an optimization, but also is this new algorithm a generalization of the Lewko-Waters algorithm.	a) Reduces ciphertext size	a) Only special gates which is AND and OR are used.
[7]	Decentralizing Attribute based Encryption	Centralized	In the Multi-Authority Attribute based systems, any party can become owner or authority of the data outsourced to cloud. The owner of the data acts as ABE authority and encrypts the data using its public key and distributing the private	a) Collusion resistant b) No dependency on any central authority	a) Lack of efficient key management

			key to the users satisfying the attributes for decryption of data.		
[8]	Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption	Centralized	Personal health records are stored at the third party site. The data is encrypted using ABE scheme before outsourcing. The users in the PHR system is divided into multiple security domains.	a) High degree of patient's privacy b) Dynamic modification of access policy c) User revocation d) Break glass access e)Reduced key management	a) Centralized KDC acts as point of failure
[9]	DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems	Decentralized	Cipher text Policy attribute based access control technique requires a trusted authority to manage and distribute keys and attributes in the cloud environment. The attributes are distributed among different authorities. Whenever user requests for attributes they come from different domains each managed by different authorities.	a) No Single point of failure b) Workload distributed	a) User identity revealed
[10]	Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds.	Decentralized	The scheme supports anonymous authentication of the user and has a decentralized approach supporting multiple KDC's. The scheme applies attribute based encryption mechanism. Here, access control mechanism is used using which only authorized user satisfying the attributes are able to decrypt the data. It is resilient to replay attacks, supports creation, modification and reading of data stored onto clouds.	a) User anonymity b)Decentralized approach for key distribution avoids single point of failure. c) Collusion resistant d) Resilient to replay attacks. e) Multiple reads and writes	a)Attributes not hidden from cloud can suffer from attack

4. Problems Addressed

- More fine-grained access mechanism needed.
- Centralized KDC mechanism can become a single point of failure and also can get overloaded because of multiple incoming requests.
- Prevent entry of stale data entry in the cloud

5. Conclusion

We have presented the survey on decentralized key distribution architecture which encompasses multiple KDC's for the distribution of keys. The data is encrypted using Attribute based encryption technique before outsourcing it to the cloud. This provides security of data. It also supports user anonymous authentication of data which enables to hide the identity of the owner of the data. It is resilient to replay attacks. User's whose attributes are revoked cannot make stale data entry in the storage environment. Thus, the scheme makes the system robust, private and secure against various powerful attacks.

References

[1] Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data, 89–98.
[2] Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-Policy Attribute-Based Encryption. 2007 IEEE Symposium on Security and Privacy (SP '07), 321– http://doi.org/10.1109/SP.2007.11
[3] Richard, D., Edward, J., & Timothy, R. (2010). Adding Attributes to Role-Based Access Control, 43(6), 79–81.
[4] Li, M., Yu, S., Ren, K., & Lou, W. (2010). Securing Personal Health Records in Cloud Computing : Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings, 89–106.
[5] Yu, S., Wang, C., & Lou, W. (n.d.). Attribute Based Data Sharing with Attribute Revocation Categories and Subject Descriptors, 261–270.
[6] Liu, Z., & Cao, Z. (2010). On Efficiently Transferring the Linear Secret-Sharing Scheme Matrix in Ciphertext-Policy Attribute-Based Encryption. IACR Cryptology ePrint Archive, 2010, 374.
[7] Lewko, A., & Waters, B. (2011). Decentralizing Attribute-Based Encryption, 02(subaward 641), 568–588.
[8] Li, M., Yu, S., Zheng, Y., & Member, S. (2013). Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption, 24(1), 131–143.
[9] DAC-MACS : Effective Data Access Control for Multi-Authority Cloud Storage Systems. (n.d.)., 59–83. doi:10.1007/978-1-4614-7873-7
[10] Sushmita Ruj, Member, Ieee, Milos Stojmenovic, Member, Ieee, And Amiya Nayak," Decentralized Access Control With Anonymous Authentication Of Data Stored In Clouds" Ieee Transactions On Parallel And Distributed Systems, Vol. 25, No. 2, February 2014.