International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

An Overview of Data Access Control in Security for Multi authority Cloud Storage Systems

R. Nagarajan*[1], Dr. G. Maria Priscilla[2]

*[1]Assistant Professor, Department of Computer Science, Sri Ramakrishna College of Arts and Science, Bharthiar University, Coimbatore, India

[2]Professor & Head, Department of Computer Science, Sri Ramakrishna College of Arts and Science, Bharthiar University, Coimbatore, India

ABSTRACT

Cloud computing technologies get more importance with a high level in secure data access control in a semi-trusted cloud storage system. Data access control for multi authority cloud storage systems (DAC-MACS) is a beneficial way to ensure data security of the cloud storage system. The two main challenging issues of the current cloud storage systems are data outsourcing and untrusted cloud servers. However, cloud storage service separates the roles of the data owner from the data service provider, and the data owner does not interact with the user directly for providing data access service, which makes the data access control a challenging issue in cloud storage systems. Because the cloud server cannot be fully trusted by data owners, traditional server-based access control methods are no longer applicable to cloud storage systems. To prevent the untrusted servers from accessing sensitive data, traditional methods usually encrypt the data and only users holding valid keys can access the data. In this research work, survey is conducted towards the attacks on data access control scheme for multi-authority cloud storage system. The security improvements of secret key generation and attribute revocation in data access control scheme to be corrected. Finally, the major overhead of decryption is also securely outsourced to the cloud servers, and the overall overheads of storage, communication and computation of the NEDAC-MACS are superior to that of DACC and relatively same as that of DAC-MACS. The analysed methodologies are implemented using the CloudSim toolkit, which is evaluated to know the performance of every research works. The performance evaluation conducted was proved that the each method has unique advantage and disadvantages among each other.

Keywords : Data Access Control (DAC), Cloud Storage, Attribute revocation, Attacks.

I. INTRODUCTION

Internet technology is growing more and more quickly, and people can process, store, or share with their data by using its ability. Recently, the cloud has emerged to provide various application services to satisfy user's requirement. In the storage service application, the cloud can let the user, data owner, store their data, and share this data with other users via the cloud, because the cloud can provide the pay as you go environment where people just need to pay the money for the storage space they use. It can bring down the cost efficiently for people. But, there is a problem that the data owner has to solve it. The data owner needs to make a flexible and scalable access control policy to command user's access right, so that only the authorized users can access.

Attribute-based Encryption is one of the most suitable schemes for data access control in public clouds for it can ensures data owners direct control over data and provide a fine-grained access control service. Till now, there are many ABE schemes proposed, which can be divided into two categories; Key Policy Attribute based Encryption (KP-ABE) as well as Ciphertext Policy Attribute-based Encryption (CPABE). In KP-ABE schemes, decrypt keys are combined with access structures and in ciphertexts it is labeled with special attribute sets, for attribute management and key distribution an authority is responsible. The authority may be the human resource department in a company, the registration office in a university, etc. The data owner defines the access policies and encrypts the data according to the defined policies. Every user will be issued a secret key reflecting its attributes. A user can decrypt the data whenever its attributes match the access policies. The issues of cloud storage system are listed below.

- ✓ Data Encryption /Decryption in Cryptanalysis
- ✓ Data Access Control on Security
- ✓ Secure Attribute Revocation
- ✓ Key Generation and Data Confidentiality in Cloud Server

The contribution of this analysis work is to discuss the various methodologies that are introduced to overcome the issues that are mentioned above. In this work, merits and demerits of all the methodologies are discussed shortly, so that one can understand and improve the demerits present in the previous research works to create novel proposed approach. Finally, the performance evaluation was conducted in all the discussed methodologies to show which one of the algorithm is effective in nature by avoiding the security issues.

The organization of this work is given as like follows: In this section, short introduction about the focus of this research is discussed. In section 2 discusses about various research methodologies. In section 3 performance, evaluation that was conducted to know the better research methodology that can overcome the security issues considerably. In section 4, the findings of this overall research work is concluded shortly.

II. LITERATURE REVIEW

A data access control for the multi-authority cloud storage (DAC-MACS) is an efficient revocation and decryption schemes. This model provides enhanced backward and forward security by proposing a cipher-text policy attribute-based encryption schemes for efficient decryption and attribute revocation. The decryption is done using a token-based method. The revocation technique is an immediate attribute revocation method which also results in less computation cost.

In the DAC-MACS method in order to provide more efficiency the proxy re-encryption method the cipher text update is delegated to the server. Thereby, the non-revoked users are not allowed to reveal the update keys received to the revoked users for increasing the security over the critical data. Based on the performance wise analysis the improved DAC-MACS is quite efficient over the storage process, communication and computational cost level as it is incurred to be quite low.

The problem with unsecured cloud servers or the untrusted cloud servers, data access control to various vendors becomes a challenging and most unsecured issue in cloud storage systems. In the following sub sections, different research methodologies secured in data access control on multi authority cloud storage system are discussed shortly.

The secured cloud storage takes some fewer methodologies to encrypt and decrypt the files. There are various research works had been conducted which focuses on achieving the cloud security where the cloud service providers cannot decrypt the data’s that are sent by the cloud users. Some of the research work has been discussed below shortly.

Goyal et al. [2] proposed a scheme called Key Policy Attribute Based Encryption, based on the Attribute Based Encryption. In the KP-ABE, the data owner encrypts the data by associating the set of descriptive attributes and the access structure is associated with the decryption key. The access tree has leaf nodes and non-leaf nodes. The leaf nodes acts as the attributes and the non-leaf nodes acts as the threshold gates. Only when the attributes associated with the ciphertext matches with the access structure of the decryption key, the user will be able to decrypt the ciphertext.

Yu et al. [4] proposed concept, the access policies are framed using the data attributes and most of the computational tasks of the user revocation process has been outsourced or delegated to the third-party cloud server, without disclosing the data content. The proposed scheme combines the Attribute Based Encryption scheme with proxy re-encryption and lazy re-encryption to achieve the efficiency. The proposed scheme also maintains the accountability to some extent. The Attribute History List (AHL) is maintained for tracing the evolution of attribute versions and proxy re-encryption keys (PRE keys). It also maintains the UserList (UL) for logging the IDs of all the verified and legitimate users in the system.

Lin et al. [1] proposed a threshold proxy re-encryption scheme and integrate it with a decentralized erasure code such that a secure distributed storage system is formulated. The distributed storage system not only supports secure and robust data storage and retrieval, but also lets a user forward his data in the storage servers to another user without retrieving the data back.

The main technical contribution is that the proxy re-encryption scheme supports encoding operations over encrypted messages as well as forwarding operations over encoded and encrypted messages. This method fully integrates encrypting, encoding, and forwarding. It analyze and suggest suitable parameters for the number of copies of a message dispatched to storage servers and the number of storage servers queried by a key server. These parameters allow more flexible adjustment between the number of storage servers and robustness.

Yang et al. [5] proposed the complete framework called DAC-MACS to achieve and increase the efficiency of the attribute revocation and user decryption operations. The proposed scheme concentrates on the multiauthority cloud storage system for processing the different attributes together. This achieves both forward and backward security by framing efficient attribute revocation method through the assignment of version number for each attribute. It also achieves decryption efficiency through the token based model. The ciphertext update process is delegated to the cloud server itself.

In the research work, above discussion under various methodologies that are reviewed in terms of data encryption/decryption operations. The cloud users are willing to share their information to multiple users would require some intermediate services for resource sharing is done. At that time, the cloud resource providers who are third party server may attempt to decrypt the data's which are store by the cloud users. This security violation may reduce the number of cloud users who are willing to share their sensitive information. There are various research works had been conducted which focuses on achieving the cloud storage system where the cloud services providers cannot decrypt the data's that are sent by the cloud users. In this review work, the various methodologies, merits and demerits are describes in Table 1.

The data access control is an important issue to improve the security from the unauthorised users and from some malicious attacks done by the third party with authenticate keys. In this research, there are new methodologies are used for update the secret keys while sharing the data from the cloud storage. Those methods are discussed shortly below.

Green et al. [9] proposed two ABE schemes that outsource the decryption to the server. In their schemes, the authority separates the traditional secret key into a user secret key and a transformation key. However, their schemes are designed only for the single authority systems and do not support for the multi-authority systems. That is because each authority may generate different user's secret key, such that the transformation keys cannot be combined together to transform the ciphertext into a correct intermediate value.

Wei et al. [7] proposed a threshold multi-authority CP-ABE access control scheme for public cloud storage, named TMACS, in which multiple authorities jointly manage a uniform attribute set. In TMACS, taking advantage of (*t; n*) threshold secret sharing, the master key can be shared among multiple authorities, and a legal user can generate his/her secret key by interacting with any *t* authorities. Security and performance analysis results show that TMACS is not only verifiable secure when less than *t* authorities are compromised, but also robust when no less than *t* authorities are alive in the system.

Further, by efficiently combining the traditional multi-authority scheme with TMACS, construct a hybrid one, which satisfies the scenario of attributes coming from different authorities as well as achieving security and system-level robustness.

Hong et al.[8]analyzed the shortcoming of DAC-MACS in dealing with attribute revocation. And found that, if a revoked user wants to access the unauthorized content whose access policy can be satisfied by his/her revoked attributes, the only thing to do is to use author's proposed attack algorithm to transform the new-version ciphertext to the old-version one if he/she can collude with the cloud service provider to get enough ciphertext update keys.

The security vulnerability exists because DAC-MACS wrongly use a bidirectional re-encryption scheme in the ciphertext updating procedure. This vulnerability allows any party to re-encrypt the ciphertext between old-version and new-version, only if he/she can get the CUKs between these two versions.

In [15], give two attacks on the two schemes. By the first attack, the revoked user can eavesdrop to obtain other users' Key Update Keys to update its Secret Key, and then it can obtain proper Token to decrypt any secret information as a nonrevoked user. In addition, by the second attack, the revoked user can intercept Ciphertext Update Key to retrieve its ability to decrypt any secret information as a nonrevoked user. Secondly, we propose a new extensive DAC-MACS scheme (NEDAC-MACS) to withstand the above two attacks so as to guarantee more secure attribute revocation. Then, formal cryptanalysis of NEDAC-MACS is presented to prove the security goals of the scheme. Finally, the performance comparison among NEDAC-MACS and related schemes is given to demonstrate that the performance of NEDAC-MACS is superior to that of DACC, and relatively same as that of DAC-MACS.

Li et al. [6] proposed an attribute-based access control scheme with two-factor protection for multi-authority cloud storage systems. In this scheme, any user can recover the outsourced data if and only if this user holds sufficient attribute secret keys with respect to the access policy and authorization key in regard to the outsourced data. In addition, this scheme enjoys the properties of constant-size ciphertext and small computation cost. Besides supporting the attribute-level revocation, this scheme allows data owner to carry out the user-level revocation.

In this section, various revocation methodologies are discussed. Revocation is the process of eliminating the access permission of malicious users from the environment. Revocation need to be handled with the concern of other user's authentication permission which might violated while trying to remove the authentication permission of revoked users. Some of the research methodologies that concentrated to avoid the revocation concepts are discusses in the following section.

Hideaki Ishii et al. [12] designed a secure data sharing scheme Mona for dynamic groups in an untrusted cloud. In Mona, users are able to share data with others in the group without revealing identity privacy to the cloud. Also, Mona is efficient in user revocation and new user joining. More specially, efficient user revocation can be achieved by public revocation list without updating the private keys of the other remaining users, and new users can directly decrypt files stored in the cloud without their participation. Moreover, the storage overhead and the encryption computation cost are constant. By analysis it is proved that proposed scheme was satisfy the security requirements and efficiency.

Kan Yang et al. [13] proposed a revocable multi-authority CPABE scheme that could support efficient attribute revocation and constructed an effective data access control scheme for multi-authority cloud storage systems. Author also proved that this scheme was provable secure in the random oracle model. The revocable multi-authority CPABE is trustworthy technique, which can be applied in any remote storage systems and online social networks etc.

Taeho Jung et al. [11] proposed schemes achieved fine-grained privilege control and identity anonymity while conducting privilege control depends on user's identity. More important is, this system can tolerate up to N – 2 authority compromise, which is mostly prefer specially in Internet-based cloud computing environment. Also conducted security and performance analysis which shows that AnonyControl both secure and efficient for cloud storage system. The AnonyControl-F inherits the security from the AnonyControl and thus is equivalently secure as it, but extra communication overhead is incurred during the 1-out-of-n oblivious transfer.

Whenever there is a user to be revoked, the system must make sure the revoked user cannot access the associated data files any more. One way to solve this problem is to re-encrypt all the associated data files used to be accessed by the revoked user, but we must also ensure that the other users who still have access privileges to these data files can access them correctly.

Key generation and Data confidentiality in cloud server is one of the pressing challenges in the ongoing research in cloud computing as soon as confidentiality becomes a concern, data are encrypted before outsourcing to a service provider. The data owner stores the confidentiality data at the third party service provider's site. The service provider is responsible for managing and administering the database and allows the data owner and clients to create, update, delete and access the database. There are chances of hampering the security of the data due to untrustworthiness of service provider.

So, to secure the data which is outsourced to third party is a great challenge. The major requirements for achieving security in outsourced databases are confidentiality, privacy, integrity, availability. To achieve these requirements various data confidentiality mechanisms are discussed shortly below.

Bethencourt et al. [3] proposed a scheme called Ciphertext Policy Based Encryption (CP-ABE). The strategy is straight opposite to that of KP-ABE. In the CPABE scheme, the access structure or access policy is associated with the data while the set of attributes are associated with the decryption key. Since the access policy is associated with encrypted data, even if cloud server becomes untrusted, the confidentiality of the data cannot be revealed. Only when the set of attributes associated with the decryption key fulfils the access policy, the user will be able to decrypt the ciphertext. The proposed scheme is safe against collusion and plaintext attacks.

Cheng-Kang Chu et al. [10] proposed key aggregate cryptosystem which is used to protect and manage the secret keys that are generated to protect the data access from the malicious users. This method is based on protecting the secret keys which are used to encrypt the content that are stored in cloud server by aggregating together which would be shared with the cloud users to give them access for data retrieval.
The scalability issues also handled in this work by introducing the constant size cipher text based encryption. These constant size cipher text ids are used to encrypt the data contents in the block level which can then would aggregate together to reduce the burden of handling large volume of data's together. These set of secret keys are aggregated together which would be shared with the cloud users for authentication process. The hackers cannot hack the secret keys while sharing with unknown users from the aggregated keys where the keys are aggregated and encrypted together.

In [14], anonymous authentication process is introduced which would prevent the malicious users from accessing of cloud contents in the secured way. This is done by introducing the mechanism called the attribute based encryption in which cloud contents are encrypted by using the general attributes that are used to differentiate the identity of users without leaking their personal information.
Anonymous authentication is the process of storing and retrieving the contents to the cloud user without revealing their personal information. When the cloud users are approaching to the cloud servers for accessing the cloud-stored contents, the attributes of those users would be collected to match with the attributes that are provided by the data owner. If those attribute values are matches together then the access permission would be granted. Else it would be rejected.

The methodology introduced in this work decentralizes the data accessing permission in order to reduce the burden of cloud servers in the considerable manner. This is achieved by removing the centralized server concept where only the centralized server is responsible for limiting the data access permission. Whenever the data a user approaching the cloud server for accessing the contents, then the key management server resides in the particular region would take care of accessing of contents. This decentralized accessing of cloud may reduce the burden of cloud servers and as well, as improve the data accessing speed.

Data confidentiality is important for users to store their private or confidential data in the cloud. Authentication and access control strategies are used to ensure data confidentiality. The data confidentiality, authentication, and access control issues in cloud computing could be addressed by increasing the cloud reliability and trustworthiness. Because the users do not trust the cloud providers and cloud storage service providers are virtually impossible to eliminate potential insider threat, it is very dangerous for users to store their sensitive data in cloud storage directly. In some work, decentralize the data accessing permission in order to reduce the burden of cloud servers.

The performance analysis of this work is done to identify the merits and demerits of these methodologies. So that, the comparison can be made between the methodologies that were discussed above. The analysis of this work is given in the following table 1.

Table 1: Analysis of discussed Methodology

S.No	Title	Author	Method	Merits	Demerits
1	Attribute based encryption for fine-grained access control of encrypted data,[2], 2006	Goyal, V., Pandey, O., Sahai, A. and Waters, B.	Key Policy Attribute Based Encryption	Do not hide the set of attribute under encrypted data.	encrypting data, is that it can be selectively shared only at a coarse-grained level
2	Cipher text-policy attribute-based encryption,[3],2007	Bethencourt, J., Sahai, A. and Water, B.	Ciphertext Policy Based Encryption (CP-ABE).	secure against collusion attacks	it is increasingly difficult to guarantee the security of data
3	Achieving secure, scalable, and fine-grained data access control in cloud computing,[4],2010	Yu, S., Wang, C., Ren, K. and Lou, W.	fine-grained data access control	1. Highly efficient and provably secure under attacks. 2. More confidentiality against cloud server	Increasing more dummy attributes in security level
4	Outsourcing the decryption of abe ciphertexts,[9],2011	M. Green, S. Hohenberger, and B. Waters	ABE schemes that outsource the decryption to the server	1.the size of the ciphertext and the time required to decrypt it grows more flexible 2. decryption code that needs to reside on a resource constrained user device will be smaller 3. Decrease the size of the trusted code base, removing thousands of lines of complex parsing code.	1. Harderning in code complexity. 2.Increase the parameter validation
5	A secure erasure code-based cloud storage system with secure data forwarding,[1],2012	Lin, H. Y., & Tzeng, W. G.	threshold proxy re-encryption	More flexible adjustment between the number of storage servers and robustness.	The use of distributed key servers increases the level of key protection but makes the analysis harder.
6	DACMACS: effective data access control for multi-authority cloud storage systems,[5],2013	Yang, K., Jia, X., Ren, K., Zhang, B. and Xie, R.	DAC-MACS	1.Prevent from collusion attacks 2. efficiency of decryption and revocation	It's hard to analysis of forward and backward security.
7	Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud,[12],2013	X. Liu, Y. Zhang, B. Wang and J. Yan	Secure multi-owner data sharing scheme MONA	1. Reduced the computation overhead to encrypt files and cipher text size. 2. The ciphertext size is constant and independent of revocation users.	1.User compute revocation parameters to protect the confidentiality 2.computation overhead of the encryption
8	Key-Aggregate Cryptosystem for Scalable	Cheng-Kang Chu, Sherman S.M.	Key-Aggregate Cryptosystem	1.Efficient handling of large volume of data	1.The aggregated key might get corrupted in

	Data Sharing in Cloud Storage,[10],2014	Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng		2.Scalability support	the less secured medium 2.The large volume of data cannot be supported due to presence of constant cipher text id's
9	Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds,[14],2014	Sushmita Ruj, Milos Stojmenovic, Amiya Nayak	Attribute based encryption	1.Decentralized access permission which makes the computation fast 2.More security	More burden of handling large volume of attributes
10	Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage,[13],2014	Kan Yang and Xiaohua Jia	Attribute revocable multi-authority CP-ABE scheme	1. It incurs less communication cost and computation cost, and is secure 2. It can achieve both backward and forward security	Lack of efficiency
11	Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption,[11],2015	Taeho Jung, Xiang-Yang Li, Zhiguo Wan, and Meng Wan	Privilege control scheme AnonyControl AnonyControl-F	1. Able to protect user's privacy against single authority. 2.Tolerant against authority	1. Data confidentiality 2. Personal information defined by each user's attributes set is at risk 3.Resilient in security breach.
12	DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems"/Security Analysis of Attribute Revocation in Multiauthority Data Access Control for Cloud Storage Systems,[8],2015	Hong, J., Xue, K., & Li, W.	Comments and corrections of CP-ABE	Analyze the shortcoming of DAC-MACS in dealing with attribute revocation, main construction proved it secure	Security vulnerability
13	TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage,[7],2015	Wei Li, Kaiping Xue, Yingjie Xue, and Jianan Hong	Threshold multi-authoriy ciphertext-policy(CP)ABE accesscontrol sceme(TMACS)	1. It satisfies the scenario of attributes from different *AA*s 2. It can achieve security and system-level robustness.	Reusing of the master key shared among multiple attribute authorities (*AA*s).
14	On the security of Data Access control for Multiauthority Cloud Storage Systems,[15],2017	Wu, X., Jiang, R., & Bhargava, B	a new extensive DAC-MACS scheme (NEDAC-MACS)	More efficiency incommunication overhead and computation cost. Same as DAC-MACs Performance.	Fewer Complexes to recover outsourced data. Compare than TFAC-MACS
15	Two-factor data access control with efficient revocation for multi-authority cloud storage systems.,[6],2017	Li, X., Tang, S., Xu, L., Wang, H., & Chen, J.	two-factor protection for multi-authority	More efficiency incommunication overhead and computation cost.	Complex to recover outsourced data.

From this analysis table, we can conclude that the every methodologies proposed previously consists of various merits and demerits in their way of application. All the merits and demerits involved in these works are considered for the review from which new methodology can be proposed by combining the merits of all the methodologies. The performance analysis were conducted to check the consistent level of the various proposed methodologies which is described detailed in the following sections.

III. SURVEY RESULT

The performance evaluation is done to know the improvement of various research methodologies, which was plotted in the graphical representation. This comparison was done based on the parameters called the storage overhead and computation overhead which is done to compare the effectiveness of algorithms discussed previously. The performance evaluation is done based many performance metrics. To validate the efficiency of existing NEDAC-MACS, performance comparisons are carried out in terms of execution time and computation cost among CP-ABE schemes of DAC-MACS, NEDAC-MACS, and TFAC-MACS.

Execution time

The execution time with difference workloads are evaluated and compared with the existing algorithms. The below graph shows the comparison of various methodologies in terms of execution time which is observed for different file sizes.

Computation cost

Figure 1 describes the comparison of computation cost in attribute-level revocation. In this research work, TFDAC-MACS are efficient through the comparison results. In our simulation experiments, the computation cost of user-level revocation for our TFDAC-MACS is 0.616s when revoking one user. Maybe this result is a little expensive. Because the data owner in user revocation needs to compute a large number of exponentiation operations.

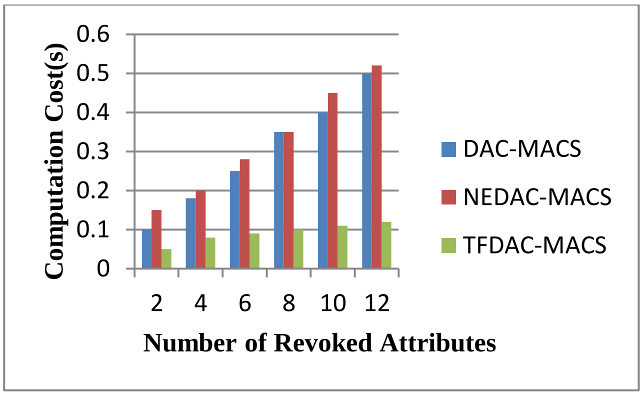

Figure 1. Comparison of Computation Cost

IV. RESULT

Data access control for multiauthority cloud storage systems (DAC-MACS) is a beneficial way to ensure data security of the cloud storage system. The two main challenging issues of the current cloud storage systems are data outsourcing and untrusted cloud servers. In this survey paper theoretical analysis of various kinds of security threats and various issues that affect the data access in the cloud storage. Also the methodologies used to solve the security threats occurred in the real time cloud environment is discussed. The detail explanation of these techniques is briefed and also summarizes the advantages with parameters of the different techniques in cloud storage system. Various types of possible ways to overcome these issues are discussed and different types of mechanisms that are used to resolve the security threats are analysed. At the end of this survey, conclude that effective mechanism is proposed to provide the effective prevention from the security attacks as well as better privacy preservation for the data outsourcing and untrusted cloud servers.

V. REFERENCES

[1]. Lin,H. Y.,& Tzeng,W. G. (2012). A secure erasure code-based cloud storage system with secure data forwarding. IEEE transactions on

parallel and distributed systems,23(6),995-1003.

[2]. Goyal,V.,Pandey,O.,Sahai,A. and Waters,B. (2006) 'Attribute based encryption for fine-grained access control of encrypted data',Proceedings of the ACM Conference on Computer and Communications Security,CCS'06,Alexandria,VA.

[3]. Bethencourt,J.,Sahai,A. and Water,B. (2007) 'Cipher text-policy attribute-based encryption',IEEE Symposium on Security and Privacy,SP'07,pp.321-334.

[4]. Yu,S.,Wang,C.,Ren,K. and Lou,W. (2010) 'Achieving secure,scalable,and fine-grained data access control in cloud computing',Proceedings of the IEEE Conference on Computer Communications,INFOCOM'2010,pp.1-9

[5]. Yang,K.,Jia,X.,Ren,K.,Zhang,B. and Xie,R. (2013) 'DACMACS: effective data access control for multi-authority cloud storage systems',IEEE Transaction on Information Forensics and Security,Vol. 8,No. 11.

[6]. Li,X.,Tang,S.,Xu,L.,Wang,H.,& Chen,J. (2017). Two-factor data access control with efficient revocation for multi-authority cloud storage systems. IEEE Access,5,393-405.

[7]. Wei Li,Kaiping Xue,Yingjie Xue,and Jianan Hong,"TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage",IEEE Transactions on parallel and distributed systems,VOL.24,NO. 06,October 2015.

[8]. Hong,J.,Xue,K.,& Li,W. (2015). Comments on "DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems"/Security Analysis of Attribute Revocation in Multiauthority Data Access Control for Cloud Storage Systems. IEEE Transactions on Information Forensics and Security,10(6),1315-1317.

[9]. M. Green,S. Hohenberger,and B. Waters,"Outsourcing the decryption of abe ciphertexts," in Proceedings of the 20th USENIX Security Symposium. USENIX Association,2011.

[10]. Cheng-Kang Chu,Sherman S.M. Chow,Wen-Guey Tzeng,Jianying Zhou,and Robert H. Deng,"Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage",IEEE Transactions on Parallel and Distributed Systems,Vol. 25,No. 2,February 2014

[11]. Taeho Jung,Xiang-Yang Li,Zhiguo Wan,and Meng Wan,"Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption",IEEE transactions on information forensics and security,VOL. 10,NO. 01,January 2015.

[12]. X. Liu,Y. Zhang,B. Wang and J. Yan,"Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," in IEEE Transactions on Parallel and Distributed Systems,vol. 24,no. 6,pp. 1182-1191,June 2013.

[13]. Kan Yang and Xiaohua Jia,"Expressive,Efficient,and Revocable Data Access Control for Multi-Authority Cloud Storage",IEEE Transactions on parallel and distributed systems,VOL. 25,NO. 07,July 2014.

[14]. Sushmita Ruj,Milos Stojmenovic,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.

[15]. Wu,X.,Jiang,R.,& Bhargava,B. (2017). On the security of data access control for multiauthority cloud storage systems. IEEE Transactions on Services Computing,10(2),258-272.