International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 08
July 2017

A New Approach of Multi Authority Data Access Control for Secure Cloud Storage

SRINIVAS KALIME
Assistant Professor, Department of CSE,
Jayamukhi Institute Of Technological Sciences,Warangal, Telangana, India

Abstract: Now days, many users are storing their large amount of data's in cloud, as a results of it provides storage flexibility. But the foremost drawbacks in cloud square measure information security. Cipher text-Policy Attribute-based cryptography (CP-ABE) is believed to be one in all the foremost acceptable technologies for data access management in cloud storage; as a results of it offers information householders lots of direct management on access policies. Throughout this work to propose associate data access management for multiauthority for validating the integrity of associate un-trusted and outsourced storage by third party auditor. In addition, this project proposes methodology based on probabilistic question and periodic verification for up the performance of audit services. It ensures efficiency of security by protecting from unauthorized users. These experimental results not alone validate the effectiveness of these approaches; but conjointly show our audit system verifies the integrity with lower computation overhead and requiring less extra storage for audit knowledge.

Keywords **– Cloud Storage, CP-ABE, Data Access Control, Multi Authority.**

I. Introduction

Now a day's cloud computing is associate showing intelligence developed technology to store knowledge from variety of consumer. Cloud computing permits users to remotely store their knowledge over cloud. Remote backup system is that the progressive technique that minimizes the price of implementing a lot of memory in a company. It helps government agencies and enterprises to scale back money overhead of information management. they will extract their knowledge backups remotely to 3rd party cloud storage suppliers than maintaining their own knowledge centres. a private or a company doesn't need buying the storage devices. Instead they will store their knowledge to the cloud and archive knowledge to avoid info loss just in case of system failure like hardware or code failures. Cloud storage is a lot of versatile, however security and privacy ar offered for the outsourced knowledge becomes a heavy concern. to attain secure knowledge group action in cloud, appropriate cryptography methodology is employed. the info owner should when secret writing of the file, store to the cloud. If a 3rd person downloads the file, they will read the record if that they had the key that is employed to rewrite the encrypted file. to beat the matter Cloud computing is one in all the rising technologies, that contains open distributed system. It's vital to guard the info and privacy of user. Attribute-based secret writing is one in all the foremost appropriate schemes for knowledge access management publicly clouds for it will ensures knowledge homeowners direct management over knowledge and supply a fine-grained access management service. Till now, there ar several ABE schemes projected, which may be divided into 2 categories; Key Policy Attribute-based secret writing (KP-ABE) still as Ciphertext Policy Attribute-based secret writing (CPABE). In KP-ABE schemes, rewrite keys ar combined with access structures and in ciphertexts it's tagged with special attribute sets, for attribute management associated key distribution an authority is accountable. The authority could also be the human resource department during a company, the registration workplace during a university, etc. the info owner defines the access policies and encrypts the info in line with the outlined policies. each user are going to be issued a secret key reflective its attributes. A user will rewrite the info whenever its attributes match the access policies. Access management strategies make sure that approved user access knowledge of the system. Access management may be a policy or procedure that permits, denies or restricts access to system. It additionally monitors and record all makes an attempt created to access a system. Access

management may also determine unauthorized users trying to access a system. it's a mechanism that is incredibly abundant vital for cover in laptop security. The Cloud storage may be a vital service in cloud computing. The Cloud Storage offers services for knowledge homeowners to host their knowledge over cloud surroundings. a giant challenge to knowledge access management theme is knowledge hosting and knowledge access services. as a result of knowledge homeowners don't utterly trust the cloud servers additionally they will not have confidence servers to try and do access management, that the knowledge access management becomes a difficult issue in cloud storage systems.

For Efficient Computation, there are three operations required namely

1. Encryption
2. Decryption
3. Revocation

In Efficient Attribute Revocation, there are two requirements

1. Backward Security
2. Forward Security

In this paper, we design a new fortified multi-authority CP-ABE scheme with efficient decryption and offer an efficient attribute revocation method, and then an operative access control scheme for multi-authority cloud storage system is designed by applying the proposed methods.

II. Related Work:

[1] J. Bethencourt, A. Sahai, and B. Waters, Cipher text- Policy Attribute-Based Encryption

In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute-Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we provide an implementation of our system and give performance measurements.

[2] Kan Yang and Xiaohua Jia, Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage

Data access control is an effective way to ensure the data security in the cloud. Due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage, because it gives data owners more direct control on access policies. However, it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. In this paper, we design an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to issue attributes independently. Specifically, we propose a revocable multi-authority CP-ABE scheme, and apply it as the underlying techniques to design the data access control scheme. Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis and simulation results show that our proposed data access control scheme is secure in the random oracle model and is more efficient than previous works.

[3]Kan Yang, Xiaohua Jia, Kui Ren, Bo Zhang, DAC-MACS: Effective data access control for multi-authority cloud storage systems

Data access control is an effective way to ensure the data security in the cloud. However, due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Existing access control schemes are no longer applicable to cloud storage systems, because they either produce multiple encrypted copies of the same data or require a fully trusted cloud server. Ciphertext-Policy Attribute-based

Encryption (CP-ABE) is a promising technique for access control of encrypted data. It requires a trusted authority manages all the attributes and distributes keys in the system. In cloud storage systems, there are multiple authorities co-exist and each authority is able to issue attributes independently. However, existing CP-ABE schemes cannot be directly applied to data access control for multi-authority cloud storage systems, due to the inefficiency of decryption and revocation. In this paper, we propose DAC-MACS (Data Access Control for Multi-Authority Cloud Storage), an effective and secure data access control scheme with efficient decryption and revocation. Specifically, we construct a new multi-authority CP-ABE scheme with efficient decryption and also design an efficient attribute revocation method that can achieve both forward security and backward security. The analysis and the simulation results show that our DAC-MACS is highly efficient and provably secure under the security model.

III. System Work:

The summary of constraints and techniques is given within the system. The development of access management theme consists of 5 phases: System initialisation, Key Generation, encryption, information cryptography and Attribute Revocation.

The major constraint to style the info access management theme is to develop the revokable multi-authority CP-ABE protocol. This protocol isn't directly deployed as a result of the 2 major reasons:

1) Security Constraint: The central authority holds the key of the system and is allowed to decode the ciphertexts.

2) Revocation Constraint: Attribute revocation isn't supported by this protocol. supported single-attribute CP-ABE a recent revokable multiauthority CP-ABE protocol. During this technique, to forestall nonlegal co-operation, we have a tendency to mix the key keys made by numerous authorities for same user. The practicality of authority is separated as world certificate authority (CA) and multiple attribute authority (AAs). The system is setup up by CA and registration of the user's and AAs ar accepted. For every user, a world user identity uid and for every attribute authority, a world authority identity aid is appointed. As a result of the globally distinctive uid, the key key issued by numerous AAs for same user is combined along for cryptography. To beat the safety constraints, despite of exploitation the system distinctive public key to inscribe information, our technique desires all attribute authorities to supply their own public key to inscribe information combined with world public parameter. during this theme the certificate authority is prevented from decrypting the ciphertext. The attribute revocation drawback is resolved by assignment the version range for every attribute. Associate attribute revocation happens only if the elements related to the revoked attribute on the QT keys and ciphertext has to be updated. Once the user's attribute is revoked from its corresponding AA, it generates a recent version key for this revoked attributes and update secret is generated. With the generated update key all user who are holding the revoked attribute will update its secret key. The revoked attribute will be updated to redo exploitation the update key. The potency will be improved by exploitation the proxy re-encryption technique for choosing the employment of ciphertext update, so freshly joined user will able to decode the info that was revealed earlier.

A. System Initialization : The system initialization consists of 2 steps: CA setup and AA setup.

1. CA Setup Taking input as security parameter, the CA sets up the system victimisation the CAsetup rule. The CA registers each user and AA. User Registration: throughout system low-level formatting every and each user ought to register to CA. the worldwide distinctive user id uid is appointed to user by the CA, if the user could be a legal user. AA Registration: throughout system low-level formatting the AA ought to register to CA. The CA assigns a world attribute authority identity aid if the AA is that the legal authority.

2. AA Setup during this rule, the set of user attributes and information owner attributes are hold on in information set, that provides the key key obtained by matching the general public key combine AAaid as input.

keyGen(GPP,GPKuid,GPkuid,GSKuid,SKaid,Suid, aid…)=={GPK,(PKaid1..n)withuidK}=SKuidnaidn

B. Secret Key Generation: once information house owners source their information with some attributes and is encrypted by attributes identity (aid) then it authenticates with user identity (uid), that is issued by CA.

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 08
July 2017

C. Encryption: Before outsourcing the owner data's to cloud, the info owner 1st partitions the info into many parts per logical granularities as m={m1,…,mn}. For instance, information will be divided into , next the info parts is encrypted with completely different content keys victimisation interchangeable encoding methodology, last the access structure mechanism Mi is outlined for every content key ki(i=1,…,n). The encoding rule takes GPP as input, a group of public keys fpr all AAs and outputs the ciphertext E. information coding BY USERS In existing state of affairs, user login in to the CSPs and also the data's will be downloaded with the traditional registration, however in existing system the CA can check the user authentication entity. The user will obtain the content key only if it satisfies the access structure outlined within the ciphertext CT.

TABLE I: Comparison Year	Name of Paper	Method	Result	Advantages	Drawbacks
2006	Cipher text policy attribute based encryption	Cipher text policy attribute based encryption	Secure against collusion attacks	In untrusted server the encrypted data can be kept confidential	It is proved secure under the generic group heuristic
2009	Improving privacy and security in multi-authority attribute-based encryption	Multi-authority ABE scheme	Removes the trusted central authority, and protects the users privacy	System does not rely on a central authority	Concern of security of the encryption and privacy of the users
2010	Attribute based data sharing with attribute revocation	Cipher text policy Attribute based encryption	It enables the authority to revoke user attributes with minimal effort	It places minimal load on authority upon attribute revocation events	CP-ABE schemes are not able to achieve provable security and user revocation is extremely hard
2011	Attribute-based access control with efficient revocation in data outsourcing systems	Cipher text policy attribute-based encryption	System is efficient and scalable to securely manage the outsourced data	Enabling user access control enhances the backward/forward secrecy of outsourced data	Revocation of any attribute or any single user in an attribute group would affect the other users in the group
2011	DACC: distributed access control in clouds	Distributed access control in clouds	The cipher texts cannot be decrypted by the cloud	The secret keys can be distributed using key distribution centers (KDCs)	This technique is only efficient in honest net-works, if not then we have to take care of net-work
2013	Scalable and secure sharing of personal health records In cloud computing using ABE	Attribute-based encryption	Through implementation and simulation, it occurs that system is both scalable and efficient	It enables dynamic modification of access policies, supports efficient on-demand user/attribute revocation	The scheme has much smaller secret key size

.

IV. Conclusion:

In this paper, we tend to introduce a revocable multi-authority CP- ABE mechanism which will handle sizeable attribute revocation. Then, we tend to style a robust information access restriction methodology for multi-authority cloud storage systems. Our methodology is expeditiously protects the system within the absolute oracle model. The revocable multi-authority CP-ABE is AN economical methodology, which can be tailored in any remote storage systems and on-line social networks etc. we tend to additionally used proxy signature and ring signature. A proxy signature methodology could be a variation of the common digital signature methodology that permits a proxy user to supply signatures on place of a clever user. Ring signature to styles homomorphic verification, so that public user is ready to analysis and share information while not fully downloading it, and yet it cannot be confirm who's that the user on every block.

References:

[1] J. Bethencourt, A. Sahai, and B. Waters, ‘‘Cipher text-Policy Attribute-Based Encryption,’’ in Proc. IEEE Symp. Security and privacy (S&P’07), 2007, pp. 321-334.
[2] 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.*
[3] Kan Yang, Xiaohua Jia, Kui Ren, Bo Zhang, DAC-MACS: Effective data access control for multi-authority cloud storage systems , 14-19 April 2013

[4] P. Mell and T. Grance, ‘‘The NIST Definition of Cloud Computing,’’ National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2009.
[5] B. Waters, ‘‘Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,’’ in Proc. 4th Int’l Conf. Practice and Theory in Public Key Cryptography (PKC’11), 2011, pp. 53-70.
[6] V. Goyal, A. Jain,O. Pandey, andA. Sahai, ‘‘Bounded Ciphertext Policy Attribute Based Encryption,’’ in Proc. 35th Int’l Colloquium on Automata, Languages,
and Programming (ICALP’08), 2008, pp. 579-591.

[7] A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters, ‘‘Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption,’’ in Proc. Advances in Cryptology-EUROCRYPT’10, 2010, pp. 62-91.

[8] M. Chase, ‘‘Multi-Authority Attribute Based Encryption,’’ in Proc. 4th Theory of Cryptography Conf. Theory of Cryptography (TCC’07), 2007, pp. 515-534.

[9] M. Chase and S.S.M. Chow, ‘‘Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,’’ in Proc. 16th ACM Conf. Computer and Comm. Security (CCS’09), 2009, pp. 121-130.

[10] A.B. Lewko and B. Waters, ‘‘Decentralizing Attribute- Based Encryption,’’ in Proc. Advances in Cryptology- EUROCRYPT’11, 2011, pp. 568-588.

[11] S. Yu, C. Wang, K. Ren, and W. Lou, ‘‘Attribute Based Data Sharing with Attribute Revocation,’’ in Proc. 5th ACM Symp. Information, Computer and Comm. Security (ASIACCS’10), 2010, pp. 261-270.

[12] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, ‘‘Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,’’ IEEE Trans. Parallel Distributed Systems, vol. 24, no. 1, pp. 131- 143, Jan. 2013.

[13] J. Hur and D.K. Noh, ‘‘Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,’’ IEEE Trans. Parallel Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.