INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 4, Issue 2 JUNE 2015

SECURE MULTI AUTHORITY CLOUD STORAGE BASED ON CP-ABE AND DATA ACCESS CONTROL

[1]A. BHAVANI, [2] P. HARI PRIYA

[1] PG Scholar, Dept of CSE, S.V. Engineering College for Women

arigela.bhavani@gmail.com

[2] Asst Professor, Dept of CSE, S.V. Engineering College for Women

hari.pchr@gmail.com

ABSTRACT— Now a days, plenty of users area unit storing their data's in cloud, as a result of it provides storage flexibility. However the most drawbacks in cloud is information security. Cipher text-Policy Attribute-based cryptography (CP-ABE) is thought to be one among the foremost appropriate technologies for information access management in cloud storage; as a result of it offers information house owners a lot of direct management on access policies. during this work to propose an information access management for multi authority for substantiating the integrity of AN un-trusted and outsourced storage by third party auditor. additionally, this project propose methodology primarily based on probabilistic question and periodic verification for up the performance of audit services. It ensures potency of security by protective from unauthorized users. These experimental results not solely validate the effectiveness of those approaches, however conjointly show our audit system verifies the integrity with lower computation overhead and requiring less additional storage for audit data.

INTRODUCTION

Similar to Cloud Computing, Cloud Storage has additionally been growing in quality recently as a result of several of identical reasons as Cloud Computing. Cloud Storage delivers virtualized storage on demand, over a network supported a request for a given quality of service (QoS). there's no necessity to buy storage or in some cases even provision it before storing knowledge. Cloud Storage is associate degree important package of cloud computing, that offers pacts for cloud knowledge vendors to host their knowledge within the cloud. This new model of knowledge hosting and access services introduces an excellent challenge to knowledge access management. Because the cloud knowledge vendors can't be totally trust on cloud server and that they don't seem to be equipped to trust on servers to control the information access. Cipher text-Policy Attribute Based cryptography is viewed in concert of the foremost applicable technologies

for knowledge access management in cloud storage systems, as a result of if offers a lot of direct access management policies and techniques to the cloud knowledge vendors. In CP-ABE theme, there's a definite authority that's responsible for attribute management, key generation, key transfer and key distributions. The authority is the registered workplace situated in numerous locations. The cloud data vendors will state the access ways and write the data per the ways. Every user are going to be supplied a secret key reproducing its attributes. The data can be decrypted the cloud users by substantiate its attributes based on the access ways.

CP-ABE offers two types of systems:

1. Single Authority CP-ABE
2. Multi-Authority CP-ABE

Single Authority CP-ABE: Attributes of the cloud knowledge vendors square measure managed by sole authority. in depth analysis has in serious trouble single authority in cloud storage system, a user might clench attributes issued by multiple authorities and the knowledge house owners might share the data with the user managed to completely different authorities that could be a nice challenge in single authority.

Multi-Authority CP-ABE: Attributes of the various domains and cloud knowledge vendors square measure managed by totally different authorities. Multi-Authority CP-ABE is a lot of apt theme for knowledge access management of cloud storage systems, as users may clench attributes issued by multiple authorities and **data house** owners may additionally share the knowledge mistreatment access policy defined over attributes from totally different authorities. In this paper, we have a tendency to 1st propose a Fortified multi-authority CPABE theme, wherever Associate in Nursing communicative , economical and a lot of secured revocation technique is planned to resolve the attribute revocation and anonymous knowledge access issues in the cloud storage system. potency in computation and attribute revocation square measure the crucial needs whereas designing the access management schemes.

In 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.

The main offerings of this paper work are often condensed as follows.

- we tend to propose a FAC-MACS (Fortified Access management for Multi-Authority Cloud Storage), AN communicative , efficient and a lot of secured information access management theme for multiauthority cloud storage systems, that could be a enhance security theme and has higher performance andefficient computation than existing access managementschemes.
- we tend to construct a replacement Fortified Mutlti-Authority CP-ABEscheme with economical coding and decoding. Specially, we tend to style the most computation of the encryption and decoding by victimization key splitter based mostlymethod.

we tend to additionally style and economical speedy

- attribute revocation method for multi-authority CP-ABE theme that achieves each forward and backward security. It reduces computation and communication value.

SYSTEM AND SECURITY MODEL

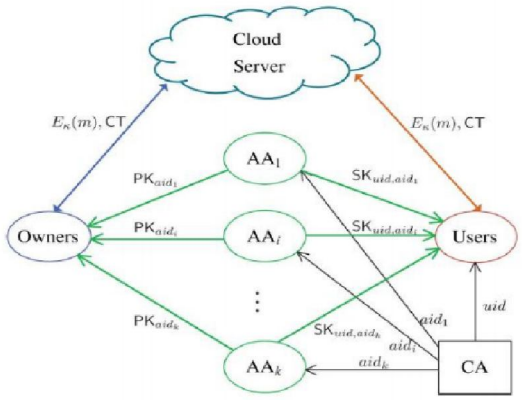
System Model

Figure 1 shows the System Model for data access control in multi-authority cloud storage is considered. There are five types of entities in the system.

1. A certificate authority (CA)
2. Attribute authorities (AAs)
3. Data owners or vendors (owners)
4. Cloud server (server)
5. Data consumers (users)

CA could be a international trustworthy certificate authority within the system. It sets up the system and accepts the registration of all the users and AAs. for every legal user within the system, the CA assigns a worldwide distinctive user identity and additionally generates a global public key for the user. every user are going to be issued a Social Security range (SSN) as its international identity. Every AA is Associate in Nursing freelance attribute authority that's responsible for entitling and revoking user's attributes according to their role or identity in its domain. In the projected theme, each attribute is related to a multiple AA, however every AA will manage Associate in Nursing discretionary number of attributes. AA has full management over the structure and linguistics of its attributes each AA has full control over the structure and linguistics of its attributes. Each AA is liable for generating a public attribute key for every attribute it manages and a Secret key and update key for every user reflective his/her attributes.

Each user contains a international identity within the system. user may be entitled a collection of attributes which can come back from multiple attribute authorities. The user can receive a secret key related to its attributes entitled by the corresponding attribute authorities. the key secret's splitd into N items and keep into multiple key servers. Each owner initial distributes the information into many parts according to the logic granularities and encrypts every knowledge component with totally different content keys by exploitation regular encryption techniques. Then, the owner defines the access policies over attributes from multiple attribute authorities and encrypts the content keys below the policies.



System Model of DAC in Multi Authority Cloud Storage

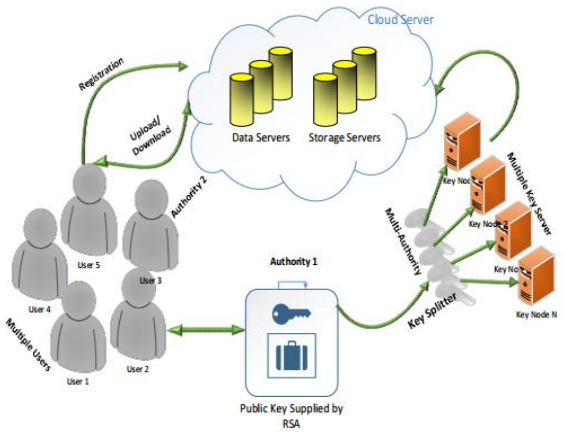
Then, the owner sends the encrypted knowledge to the cloudserver in conjunction with the ciphertexts. they are doing not trust the server to try and do knowledge access management. But, the access management happens within the cryptography. that's only if the user's attributes satisfy the access policy outlined within the ciphertext; the user is in a position to decode the ciphertext. Thus, users with completely different attributes will decode different number of content keys and therefore get totally different granularities of information from a similar data. The proposed theme is in a position to surface the below challenges:

2. Protect user's privacy against each single authority.
3. Tolerant against authority compromise, and compromising of up to (N − 2) authorities does not
   bring the whole system down.

3 Provides the detailed analysis on security and performance to show feasibility of our scheme.
4. The real toolkit of multi-authority based encryption
scheme is implemented.

Security Framework

The framework has been designed mistreatment the below outlined elements of layers. The planned theme is employed to regulate the outsourced data and supply the quality quality of the cloud storage service for the cloud users with Associate in Nursing economical encoding and decryption computations and multiple key server with key splitter techniques. This multi-authority CP-ABE provides authority that's in control of attribute management, economical computation, key distribution and the revocation ways. There area unit seven layers outlined within the planned theme. The practicality of these layers is summarized as follows:



Proposed Security Framwork (FAC-MACS)

- **Proxy layer:** This proxy layer acts as interface between the users and the rest of the servers available in the cloud.
- **Cloud data server layer:** Data server has two different entities can be recognized as the cloud users and thecloud service provider. Multiple data servers are proposed in this scheme to avoid the traffic.
- **Cloud data storage server layer:** All the data and the files are stored in these storage servers which are stored by the both individual customers and organizations. Similar to data server there are multiple storage servers are introduced to handle big volume of data.
- **Cloud Key server layer:** Multiple key servers are proposed in this scheme for efficient computation and attribute revocation method. Key server is used to store the secret key that are encrypted or fragmented by the key splitter.
- **Key splitter:** Key splitter is used to divide cryptographic key K in n safe pieces K1, K2, Kn Such that knowledge of any J pieces can be used to compute K easily. These pieces are assigned to N nodes. Shamir's algorithm is to divide Key in n parts, Kz, Kn such that there is a special part Kt which contains the information of all other parts, and K cannot be computed without Kt. However, K cannot be computed without especial part Kt.
- **Cloud consumers layer:** Cloud users are the one who have the data to be stored in the cloud and depend on

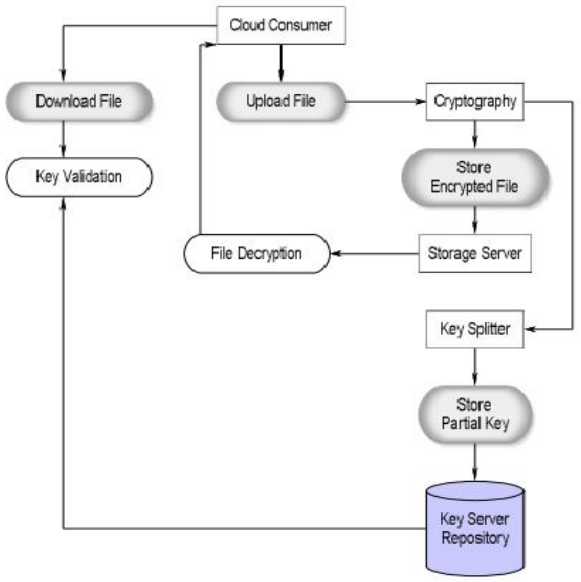
- cloud for data computation and transformation. Cloud consumers can be both customers and individual organizations.
- **Cloud service provider (CSP):** This layer owns, built and manages the storage servers in distributed manner and functions as live cloud computing systems.

FORTIFIED ACCESS CONTROL SCHEME

The existing framework of the theme is changed and to make it additional sensible to cloud storage systems, in which data house owners don't seem to be concerned within the key generation. Specifically, a user's secret secret is not associated with the owner's key, such every user solely must hold one secret key from every authority rather than multiple secret keys associated to multiple house owners. The potency of the attribute revocation technique is greatly improved. Specifically, in our new attribute revocation technique, only the ciphertexts that related to the revoked attribute needs to be updated, all the ciphertexts that associated with any attribute from the authority (corresponding to the revoked attribute) ought to be updated. a replacement revocable multi-authority CP-ABE protocol is planned supported the single-authority CP-ABE planned by Lewko and Waters . that's wont to extend multi authority state of affairs and build it revokable. Apply the techniques in Chase's multi-authority CP-ABE protocol to tie along the key keys generated by completely different authorities for identical user and prevent collusion attack.

1.1 **FAC design**

In FAC design, as mentioned in previous section, we proposed sever bedded design so as to boost the cloud security and accessibility. The planned theme is ready to safe guard every user's privacy once more single or maybe multiple authorities and it's lenient against authority mediation and compromising of up to N-2 node authorities doesn't bring the entire.



System Architecture: Fortified Access Control for MACS

The framework of the theme is changed and to form it more sensible to cloud storage systems, within which information owners don't seem to be listed within the key generation. Specifically, a user's secret secret is not associated with the owner's key, such every user solely must hold one secret key from every authority rather than multiple secret keys associated to multiple house owners. The attribute revocation method's potency is greatly improved. Specifically, during this new planned attribute revocation method, solely the ciphertexts that related to the revoked attribute must be updated, all the ciphertexts that related to any attribute from the authority (corresponding to the revoked attribute) ought to be updated. Moreover, in our new attribute revocation technique, both the key and also the ciphertext may be upgraded by mistreatment the

same update key, rather than requiring the owner to form update info for every ciphertext, such house owners are not needed to store every random range generated during the encoding. The quality of our access control scheme is highly improved, where the limitationthat each attribute can be removed and only appear atmost once in a ciphertext.

FAC Implementation

The below figure shows the system model of fortified access control for multi-authority cloud storage using CP-ABE algorithm. There are five methods proposed in this paper for the fortified access control:

1. Key Generation and Storage

2. Key Splitter

3. Key Transfer

4. Key Retrieval

5. Distributed Key Storage

Methods are summarized as follows:

Key Generation and Storage: User will generate new symmetric science key K or will store already existing science keys PRN victimisation planned technique. Key splitter can split the key into n items and store every half in several server. One main piece lets Kn of key are allotted to client of application. This piece of key has data of all other items and actual key can't be regenerated without this piece.

Key Splitter: User will split the science key K into items and store it into multiple key servers in distributed manner. Key server is situated in different locations so as to tighten the protection of the cloud data. every bit of key's store in distributed server, so hacker cannot access or retrieve the keys directly. Key splitter is one in all intrinsic methodology introduced in fortified access management for multi-authority cloud storage.

Key Transfer: User will transfer utterly computed key or the element of key on public cloud for knowledge processing. Public Key science customary (PKCS7) can accustomed transfer such key that's developed by RSA Laboratories Associate in Nursingd accustomed wrap knowledge in an envelope to firmly transfer it. This protocol accustomed wrap message in Associate in Nursing envelope and signed by sender. Receiver is aware of the coding key to decode the encrypted message.

Key Retrieval: On the request of key retrieval all, the components can fetch the key from key store through computational server. shopper machine can prompt consumer of application to enter his/her piece of key. Original Key can reckon on the fly once taking information from client on consumer's terminal.

Distributed Key Storage: The goal of this module is to divide science key K in n safe items K1, K2, Kn Such that data of any J items is accustomed compute K simply. These items ar allotted to N nodes. Shamir's formula is to divide Key in n components, Kz, Kn such that there exists a special half Kt that contains the information of all different components, and K can't be computed while not Kt. However, K can't be computed without uncommon half Kt.

Shamir's Secret Sharing is associate degree formula in cryptography created by Adi Shamir. it's a variety of secret sharing, where a secret is split into elements, giving every participant its own distinctive half, wherever a number of the elements or all of them area unit required so as to reconstruct the key. Counting on all participants to mix along the key might be impractical, and so generally the threshold theme is employed wherever any of the elements area unit sufficient to reconstruct the first secret.

PERFORMANCE AND SECURITY ANALYSIS OF fac

- data owner to transmit a brand new ciphertext element

PERFORMANCE ANALYSIS

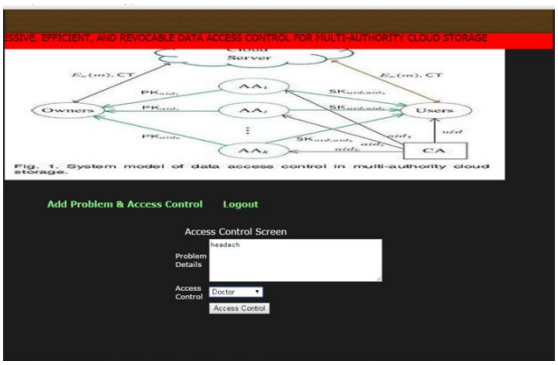
Performance of the cloud storage system is improved with our new planned theme. The performance improvements as follows:

- Separate the practicality of the authority into a worldwide certificate authority and multiple attribute authorities which would increase the enactment of the system.
- Assigns international UID and global AID to every user in the system to tell apart from different user so as to improve the cloud system performance. UID-User Identity, AID-Authority Identity.
- User ' s secret keys generated by the various authorities
  are tied along to stop collision attacks.
- rather than mistreatment the system ' s public key to write in code knowledge, our theme needs all attribute authorities to come up with their own public keys and use them to write in code the info together with international public parameters and prevents certificate authority from decrypting the cipher texts.
- every attribute is appointed with version range to unravel
  Attribute revocation drawback. once associate degree attribute revocation happens solely those parts associated
  with the revoked attribute secretly keys and cipher texts need to be updated.
- Improved potency by authorization the work of cipher texts update to the server by mistreatment the proxy reencryption technique, such the new joined user is also ready to decipher the antecedently revealed knowledge, which are encrypted with the previous public keys, if they need sufficient attributes.
- Less communication price since it does n\'t needs the to every non-revoked user since the management is currently with the cloud users
- The machine price of the access management theme is similar to traditional access management theme. Our schemeincurs abundant less communication and machine
  cost throughout the attribute revocation.
- projected fortified multi-authority CP-ABE theme as the underlying techniques to construct the communicative and economical knowledge access management theme for multiauthority cloud storage systems.

SECURITY ANALYSIS

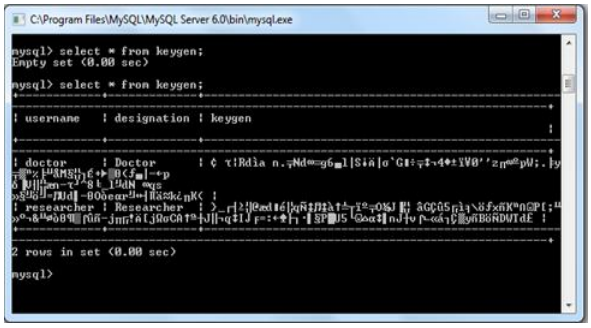
- Proposes nice and increased security challenge to information access management within the cloud storage systems.
- It achieves each forward and backward security. The revoked user cannot rewrite any new ciphertext that requires the revoked attribute to rewrite (backward security). The freshly joined user may rewrite the previously printed ciphertexts1, if it's comfortable attributes (Forward Security).
- This theme doesn't need the server to be totally trusted, as a result of the key update is enforced by every attribute authority not the server.
- Redoubled information and file security, it's terribly tough or Associate in Nursing intruder to access, misuse and destroy the first type of data within the file accessible within the cloud storage system.
- Improve the info and file security publically cloud computing atmosphere by storing file contents in different servers.
- Use of multi key server that improves security. In this

- we generate over one key server. And split the keys in step with the amount of server used. So the attacker can't establish all the keys that ar used whereas storing the info in cloud.
- The quality of our access management theme is highly improved, wherever the limitation that every attribute may be removed and solely seem at the most once in a ciphertext.



Expected Results

In this paper we are proposing CP-ABE. Using CP-ABE the keys will be generated and stored in database as shown below.



Using access policy the user can give the data access to specified person.

Conclusion

This paper chiefly describes concerning the ways and algorithms, that square measure used for providing the high finish of security in cloud storage system and accessing Information effectively and firmly. On measurement the various previous works, we tend to analyzed the benefits and disadvantages of every work and at last we tend to derived the new technique, that over comes the drawbacks of previous work by analyzing all the information's altogether state of exploration and by providing the additional secured cloud atmosphere. Finally we tend to conclude that CPABE scheme provides multiple authorities that square measure accountable
for attribute management and key distribution. during this new scheme, we tend to increased the machine potency, attribute revocation potency and additionally enriched the security within the cloud storage system. This fortified multi authority CP-ABE may be a capable technique, which might be applied in any data systems and on-line social networks and alternative massive information connected applications.

REFERENCES

[1]P. Mell and T. Grance, ''The NIST Definition of Cloud Computing,'' National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2009.

[2]J. Bethencourt, A. Sahai, and B. Waters, ''Ciphertext-Policy Attribute-Based Encryption,'' in Proc. IEEE Symp. Security and privacy (S&P'07), 2007, pp. 321 -334.

[3]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.

[4]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.

[5]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.

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

[7]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.

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

[9]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.

[10]M. Li, S. Yu, Y. Zheng, K. Ren, andW. 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.

[11]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.

[12] S. Jahid, P. Mittal, and N. Borisov, ‘‘Easier: Encryption- Based Access Control in Social Networks with Efficient Revocation,’’ in Proc. 6th ACM Symp. Information, Computer and Comm. Security (ASIACCS’11), 2011, pp. 411 -415.

[13]S. Ruj, A. Nayak, and I. Stojmenovic, ‘‘DACC: Distributed Access Control in Clouds,’’ in Proc. 10th IEEE Int’l Conf. TrustCom, 2011, pp. 91-98.

[14]K. Yang and X. Jia, ‘‘Attribute-Based Access Control for Multi-Authority Systems in Cloud Storage,’’ in Proc. 32th IEEE Int’l Conf. Distributed Computing Systems (ICDCS’12), 2012, pp. 1-10.

[15]D. Boneh and M.K. Franklin, ‘‘Identity-Based Encryption from the Weil Pairing,’’ in Proc. 21st Ann. Int’l Cryptology Conf.: Advances in Cryptology - CRYPTO’01, 2001, pp. 213-229. [16] A.B. Lewko and B. Waters, ‘‘New Proof Methods for AttributeBased Encryption: Achieving Full Security through Selective Techniques,’’ in Proc. 32st Ann. Int’l Cryptology Conf.: Advances in Cryptology CRYPTO’12, 2012, pp. 180-198.

[16]Kan Yang, Student Member, IEEE, and Xiaohua Jia, Fellow, IEEE. “Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage”. IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 7,JULY 2014.