ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

A Survey on Efficient CP-ABE and Secure Data Access Control for Multi Authority Cloud Storage with Data Mirroring

Pradnya P. Shelar[1], Prof. Manisha M. Naoghare[2]

M.E. Student, Dept. of Computer Engineering, SVIT, Chincholi, Nashik, Maharashtra, India[1]

Assistant Professor, Dept. of Computer Engineering, SVIT, Chincholi, Nashik, Maharashtra, India[2]

ABSTRACT: For secure data storage in clouds we used decentralized access control scheme that supports user authentication, Key generation and management as well as multi authority data storage and retrieval. In multi authority system, multiple authorities can access same data copy but having different attribute policies. 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. Hence, in proposed system we are mainly focusing on revocable multi authority scheme with the help of CP-ABE algorithm and to design an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems with data mirroring. 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 with data mirroring.

KEYWORDS: Ciphertext-policy Attribute-based encryption (CP-ABE), Attribute Revocation, Forward & Backward Security and Data Mirroring

I. INTRODUCTION

Cloud computing is the computing technique which describes the combination of logical entities like data, software which are accessible via internet. Cloud computing provides help to the business applications and functionality along with the usage of computer software by providing remote server which access through the internet. Client data is generally stored in servers spread across the globe. Cloud computing allows user to use different services which saves money that users spend on applications. Data owners and organizations are motivated to outsource more and more sensitive information into the cloud servers, such as emails, personal documents, videos and photos, company finance data, government documents, etc.

Cloud storage is an important service of cloud computing, which offers services for data owners to host their data in the cloud. Ciphertext-Policy Attribute-based Encryption (CP-ABE). There are some existing systems on access control in cloud are centralized in nature. All other schemes use attribute based encryption (ABE). These existing systems follow symmetric key approach. The schemes do not support authentication as well. Earlier work provides privacy preserving authenticated access control in cloud. However, the authors take a decentralized approach where a multiple key distribution center (AA) distributes secret keys and attributes to all users. A single Key distribution server is not only a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment.

Also the other drawback of earlier schemes was, user can create and store a file and other users can only read the file. Write access was not permitted to users other than the creator. Hence we need system which is three tier systems. One segment must use to hide identity, second segment must use to manage key distribution and third part must use to save encrypted data. Hence we need a system that manages distant Key Distribution Process, User validations, Encrypted Data Storage. Efficient user attributes management and revocation.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

II.RELATED WORK

In [1] Kan Yang et.al.Proposed a revocable multi-authority CP-ABE scheme, to solve the attribute revocation problem in the system. The attribute revocation method can efficiently achieve both forward security and backward security. Moreover, while updating the cipher texts, all the users need to hold only the latest secret key, rather than to keep records on all the previous secret keys. But this system issues computation efficiency and the revocation method.

In [06], A.B. Lewkoet.al.presented two fully secure functional encryption schemes: a fully secure attribute-based encryption (ABE) scheme and a fully secure (attribute hiding) predicate encryption (PE) scheme for inner product predicates. They constructed their ABE scheme in Composite order bilinear groups, and prove its security from three static assumptions. Their ABE scheme supports arbitrary monotone access formulas. Their predicate encryption scheme is constructed via a new approach on bilinear pairings using the notion of dual pairing vector spaces proposed by Okamoto and Takashima.

In [08] A.B. Lewkoet.al.proposed a fully decentralized ABE where users could have zero or more attributes from each authority and did not require a trusted server. In all these cases, decryption at user's end is computation intensive. So, this technique might be inefficient when users access using their mobile devices.

In [13] S. Ruj et.al used technique that requires owners to re-encrypt the cipertext. The method in need owner to generate the update information during the revocation, where the owner should also hold the encryption secret for ciphertext in the system. This incurs a heavy storage overhead on the owner, especially when the number of ciphertext is large in cloud storage system. Hence there is need of an improved scheme for data access controls in the cloud storage were the cloud servers are not trustworthy.

III.PROPOSED SYSTEM

Cloud storage is an important service of cloud computing, which offers services for data owners to host their data in the cloud. Ciphertext-Policy Attribute-based Encryption (CP-ABE), is regarded as one of the most suitable technologies for data access control in cloud storage systems, because it gives the data owner more direct control on access policies. In CP-ABE scheme, there is an authority that is responsible for attribute management and key distribution. The authority can be the registration office in a university, the human resource department in a company, etc. The data owner defines the access policies and encrypts data according to the policies. Each user will be issued a secret key reflecting its attributes. A user can decrypt the data only when its attributes satisfy the access policies. This system includes a revocable multi authority CP-ABE scheme, where an efficient and secure revocation method is proposed to solve the attribute revocation problem in the system.

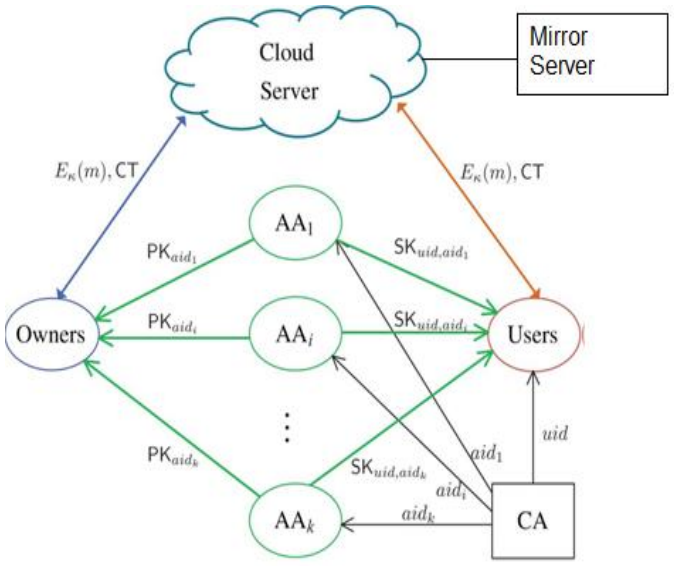

Figure 1: System Architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

There are six types of entities in the system: a certificate authority (CA), attribute authorities (AAs), data owners (owners), the cloud server (server), data consumers (users) and Backup server.

The CA is a global trusted certificate authority in the system. It sets up the system and accepts the registration of all the users and AAs in the system. Every AA is an independent attribute authority that is responsible for entitling and revoking user's attributes according to their role or identity in its domain. Each user has a global identity in the system. A user may be entitled a set of attributes which may come from multiple attribute authorities. Each owner first divides the data into several components according to the logic granularities and encrypts each data component with different content keys by using symmetric encryption techniques. The access control happens inside the cryptography. That is only when the user's attributes satisfy the access policy defined in the ciphertext, the user is able to decrypt the ciphertext. Thus, users with different attributes can decrypt different number of content keys and thus obtain different granularities of information from the same data. In mirror server, in case of new file upload Cloud will generate backup copy of uploaded data. If data is already present on cloud and user fires update command then cloud keep 2 old copied before data updations.

A. Methodology:

1. **Setup phase:**

   CA- certificate authority: This authority is responsible for user registration and its attribute preservation.

   a) **User Registration:** User enters his/her personal information for registration. After registration its unique uid is generated which is used for key generation.
   b) **AA Registration:** We have multiple AA. While system initialization, each Attribute authority register itself with CA. CA assigns unique Aid to each AA. CA sends user's public and private key to AA.

2. **Key Generation:** For keys user is get first validated on respective AA after checking it validity and user rights AA assigns public and secret key (PK and SK) to the user.

3. **Data Encryption:** User will encrypt the data using the secret key received from AA.

4. **Mirror generation:** In case of new file upload Cloud will generate backup copy of uploaded data. If data is already present on cloud and user fires update command then cloud keep 2 old copied before data updations.

5. **Data Decryption:** User decrypt the downloaded file using key received from AA.

6. **Attribute revocation:** It includes user revocation and add / modify user attribute for previously uploaded files. Data owner can modify these attribute set.

7. **Restore Data:** Data owner can download the data backup copies if certain mishap happens with cloud data files.

IV. SECURITY ANALYSIS

Our Data access control scheme is secure where we achieve forward security, backward security, improved security, and data integrity.

1. **Forward Security:** Forward Security is achieved when any new user is joined. If the new user has sufficient attributes new keys will be generated and provided to the new users. Hence the new user can access previously published data also. And the already existed authorized users will also be provided the newly generated keys. Hence the problem is resolved even for them.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

2. **Backward Security:** Each time when the secret key update algorithm runs it provides new secret key to all the authorized users. When any attribute is revoked then user will be automatically removed from the list of that authority and hence he will not get the new key. When the user does not have the attribute and the newly generated key he cannot access the data. Like this the backward security is achieved.

3. **Improved Security:** When the authorized user tries to access the data for which he is not having the attribute at that time this will come into picture. The authorized user will obviously not get that requested data and also he will get blocked. A message informing about this will also be sent immediately after the attack. This reduces security risk of the unauthorized users who have compromised authorized users also.

4. **Data Integrity:** Data integrity is maintained by data owner. Data owner keeps checking the files stored into cloud data base. When any of the attackers attacks and modifies the data stored then data owner will come to know about the attack and the verification of that file. Like this the data integrity is maintained.

V. CONCLUSION AND FUTURE WORK

This system focuses on efficient and secure cloud storage functionality. The cloud data is accessed/shared by multiple authorities. The data on the cloud is in encrypted format. We are mainly emphasizing on key generation and key management as well as on the attribute revocation with both forward and backward security. Multiple attribute authority provides a robust environment for key management unlike other centralized cloud storage schemes. The system generates a mirror copy of cloud data for data recovery.

REFERENCES

[1] Kan Yang, XiaohuaJia, "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

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

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

[4] B. Waters, ''Ciphertext-Policy Attribute-BasedEncryption: An Expressive, Efficient, and ProvablySecure Realization,'' in Proc. 4th Int'l Conf. PracticeandTheoryin Public Key Cryptography (PKC'11),2011,pp. 53-70.

[5] V. Goyal, A. Jain, O. Pandey, and A. Sahai, ''BoundedCiphertext Policy Attribute Based Encryption,'' inProc. 35th Int'l Colloquium on Automata,Languages, and Programming (ICALP'08), 2008, pp.579-591

[6] A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, andB. Waters,''Fully Secure Functional Encryption:Attribute-Based Encryption and (Hierarchical) InnerProductEncryption,'' in Proc.Advances inCryptology- EUROCRYPT'10, 2010, pp. 62-91.

[7] M. Chase, ''Multi-Authority Attribute BasedEncryption,'' in Proc. 4th Theory of CryptographyConf. Theory of Cryptography (TCC'07), 2007, pp. 515-534.

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

[09] S. Yu, C. Wang, K. Ren, and W. Lou, ''AttributeBased Data Sharing with Attribute Revocation,'' inProc. 5th ACM Symp. Information, Computer and Comm. Security(ASIACCS'10), 2010, pp. 261-270.

[10] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou,1''Scalableand Secure Sharing of Personal HealthRecords in Cloud Computing Using Attribute-Based Encryption,'' IEEE Trans. Parallel Distributed Systems, vol. 24, no. 1, pp. s131-143, Jan. 2013.

[11] J. Hur and D.K. Noh, ''Attribute-Based Access Controlwith 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 Networkswith 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,'' inProc. 32th IEEE Int'l Conf. Distributed ComputingSystems (ICDCS'12), 2012, pp. 1-10.