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. 4, Issue 11, November 2016

Secure Data Access Control and Efficient CP-ABE 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: To provide secure data storage in cloud, we proposed decentralized access control mechanism. This mechanism is useful for user authentication, key generation, and key management. It supports multi authority, data storage & its retrieval. CP-ABE is suitable technique for accessing data securely as it provides multiple access control in multi-authority system. But system complexity increases while revoking the user. We are mainly focusing on multi-authority scheme with CP-ABE mechanism with efficient user revocation. Along with decentralized access control mechanism we provide data mirroring and data integrity checking. Backup servers are used to preserve data backup copies. The Third Party Auditor (TPA) allows user to check data integrity. Our proposed attribute revocation method can efficiently achieve forward security. Data mirroring and integrity check provide data backup i.e. backward security.

KEYWORDS: Ciphertext-policy Attribute-based encryption (CP-ABE), cloud storage, data access control, multi-authority, TPA, Attribute Revocation, Forward Backward Security and Data Mirroring

I. INTRODUCTION

In recent era, cloud computing is widely used to store data and preserve that data for longtime [1]. Cloud supplies multiple services for data owners to upload their data on cloud and it also provides the facility to gain access for stored data on cloud from any location. This stored can be shared among multiple users. Recently, end user get such type of facility from market applications such as Google cloud, dropbox, Microsoft cloud. According to the perspective of security, data access control is a very challenging work in cloud computing [3]. Data Encryption is the only process to hide information from cloud as well as third party user. Further it required access rights and with this access rights user get permitted for decryption of required data from cloud. We proposed Cipher text-Policy Attribute-based Encryption (CP-ABE) system as the best solution for previously occurring problems of data security and confidentiality about accessing data as well as user revocation. Our proposed system is based on CP-ABE scheme [5][7]. It helps for attribute management and key distribution for authority. This authority can be a onetime registration in university. In our system data owner is responsible to define access policies of data as well as encryption of that data according to define policies. A user can decrypt the data only when its attributes satisfy the access policies [6]. Our proposed system contains a revocable multi-authority CP-ABE scheme.

Our scheme is capable for solving the attribute revocation problems that are raised in previous system [13]. Our system works efficiently. We also proposed a secure revocation method. In this scenario user can stored some sensitive information that cannot identified or accessed by other users. In our system data owner have ability to prove that other users that he/she is a valid user or not as they aim to shared data may not revealing its identity. The Third Party Auditor (TPA) allows users to view the files on the cloud server, it also give information about which file is stored in which server [12]. TPA provides guarantee of security to the Cloud server. Therefore, attacker may not attack the server for hacking or damaging the stored data. In our system we provide a framework to deal with key management aspect, securing user identity, secure data upload and data backup.

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. 4, Issue 11, November 2016

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

Our proposed system focused on efficient and secure cloud storage functionality in decentralized data storage environment. Key servers are responsible for key generation and management. In our system we called these servers as AA- Attribute Authority. In our system user identity may not revealed its identity to the cloud server. User registration details are present on the certificate authority server. Cloud server is responsible for data storage. Mirror server preserves 2 backup copies of user data. Third Party auditor server is responsible for data integrity checks.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. Following are the important phases of system.

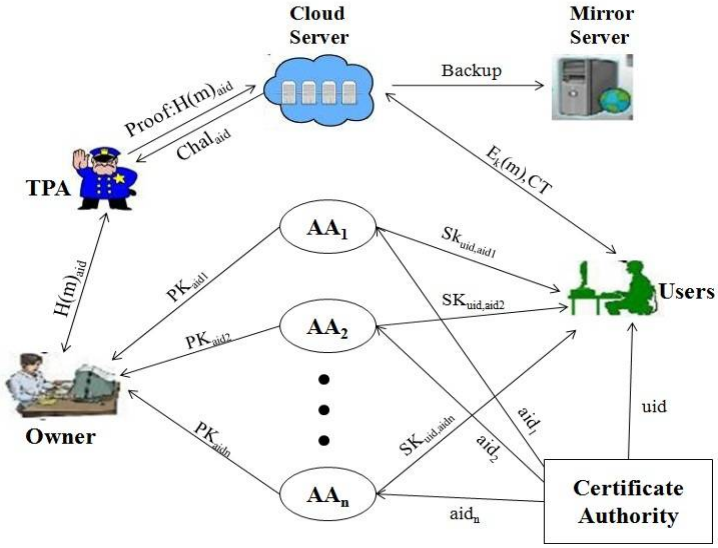


Figure 1: System Architecture

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. 4, Issue 11, November 2016

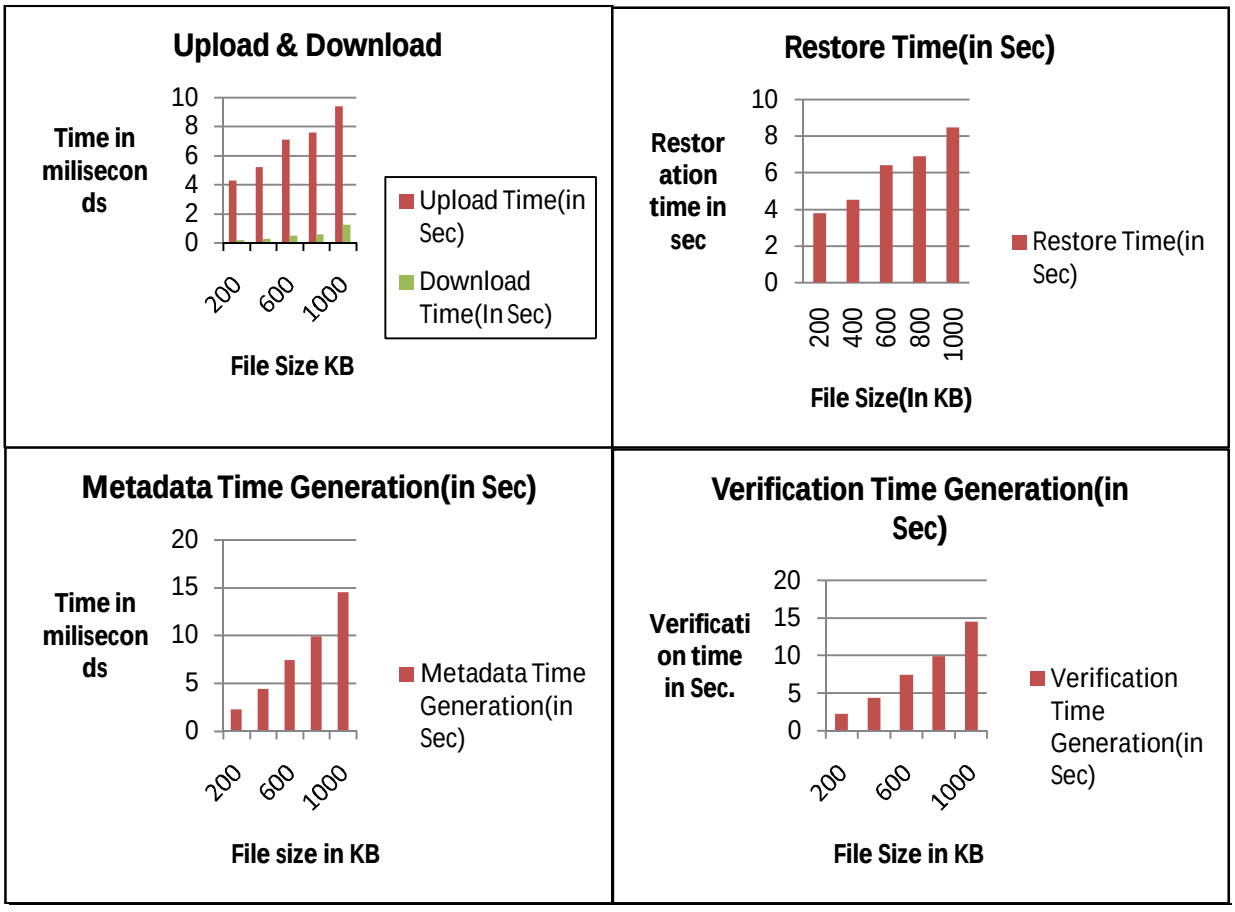
The Fig.1 represented seven types of entities in the system: a certificateauthority (CA), attribute authorities (AAs), TPA (Third Party Auditor), data owners(owners), the cloud server (server),data consumers (users) and Backup server.

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 users 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 in the form of metadata and send it to TPA for integrity checking.

The access control happens inside the cryptography. Cloud server will then challenge the TPA for data integrity check and TPA will send the document to upload on cloud with proof. That is only when the users 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.

IV. RESULT ANALYSIS

The experimental analysis carried out on operating system with processor corei3, 1GB RAM, with windows 7 operating system. The further section describesdifferent datasets used in data extraction from multiple data sources. And onthe basis of all records, analysis gives the brief idea about which input datais used to get the result and analyze the data extraction with similar system.Another method used is graphical representation view for the analysis. On thebasis of the time in ms, the performance of the system is been measured.



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. 4, Issue 11, November 2016

We have tested file uploading and downloading, Restore backup files by Backup server, Metadata generation by TPA and File verification on datasets. Above figure shows different results of the system.

To overcome the file crashes due to barrier we have created restore server which basically restores the files that uploaded on cloud server. It required less time to than new file upload as it only shifts the content from one server to another server. Figure represents the file restoration time in seconds

Metadata is created when user uploads new file and/or data is updated or restore. For metadata creation we have divided the file in no. of blocks. Random blocks are selected for metadata generation. SHA-1 algorithm is used for metadata generation.

After sending data verification request from user cloud generates metadata. TPA is responsible for metadata verification. It verifies metadata uploaded by user with newly generated metadata proof. After verification TPA sends the verification result to the user via mail.

V. CONCLUSION AND FUTURE WORK

The proposed system is decentralized system in which distributed nodeswork together for data security on cloud by implementing encryption facility ,also these nodes manages multi user tasks like sharing , writing data , readingdata etc. the third party CA server manages the user records and hide user identity from other servers and hence provide data user specific data confidentiality.Due to this decentralized approach keys are managed at different node hencecloud is not having keys for decryption hence data security is assured. Also Attribute authority is distributed and not having data hence only encryption keysare not useful to it. Data mirroring facility is provided to the user to retrievebackup copied of data in case of any disaster. Three types of user like owner,writer and reader has respective access control to the data. Hence this systemis also manages hierarchical scenarios as far as users role is concern.

In this scheme effective data sharing process can developed in future.Also data back-up management protocols can be developed. While sharing encrypted data, key management will be an issue. This key managementbottle neck problem can be resolved in future by key aggregation technique.

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. IEEE Symp. Security and privacy (S&P’07), 2007, pp. 321-334.

[4] 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.

[5] V. Goyal, A. Jain, O. Pandey, and A. Sahai, ‘‘Bounded Ciphertext Policy Attribute Based Encryption,’’ in Proc. 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, 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.

[7] M. Chase, ‘‘Multi-Authority Attribute Based Encryption,’’ in Proc. 4th Theory of Cryptography Conf. 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, ‘‘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, and W. Lou,1‘‘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. s131-143, 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.