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

Miss. Pradnya K. Bachhav
Asst. Professor, Dept. of Basic Engineering Science,
Guru Gobind Singh College of Engineering & Research Centre
Nashik, India
Mail-id: pradnyak.bachhav@gmail.com

Mr. Mukesh A. Amritkar
Asst. Professor, Dept. of Basic Engineering Science
Guru Gobind Singh College of Engineering & Research Centre
Nashik, India
Mail-id: mukeshamritkar@gmail.com

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.

In this paper we are representing related work in section II then we discussed about proposed system architecture and its flow in section III. Then we define algorithm and mathematical model in section IV&V. Experimental results are given in section VI. Finally, we conclude our system in section VII.

II. Related Work

J. Bethencourt et.al.[1]proposed Cipher text-Policy Attribute-Based Encryption(CP-ABE). It is a promising technique used to design an access control for encrypted data. Implementing this system they achieved Attribute revocation method based attribute revocation scheme. In this system, cloud servers cannot be fully trusted by data owners, therefore, traditional attribute revocation methods are not suitable for cloud storage system.

B. Waters, 2011,[2]represented ciphertext-policy attribute-based encryption systems. It is efficient, expressive, and secure under concrete assumptions. Their construction fall into common procedure required for embedding LSSS problem directly into the public parameters.

V. Goyal et.al.[3]suggested the formation of a cipher text-policy attribute based encryption scheme. This scheme has security proof that is based on a number theoretic assumption as well as they were supporting advanced access structures.

Their formation support access structures. It can be represented by a bounded size access tree with threshold gates as its nodes.

A.B. Lewkoet.al.[4]introduced two fully secure functional encryption schemes namely, a secure “attribute-based encryption” (ABE) scheme and a secure “predicate encryption”(PE) scheme for predicates of inner product. They build ABE scheme in Composite order bilinear groups, from that they prove its security from three static assumptions. Proposed ABE scheme supports arbitrary monotone access formulas. Predicate encryption scheme is constructed through new approach on bilinear pairings using the notion of dual pairing vector spaces.

M.Chase et.al.proposed[5],represents a multi-authority CP-ABE protocol. It cannot be directly applied as the underlying techniques because of two main reasons as: Security Issue and 2) Revocation Issue: Chases protocol does not support attribute revocation.

In Decentralizing Attribute-Based Encryption, A.B. Lewko et.al.[6]discussed a complete decentralized ABE. In this users may have zero or more attributes from each authority and that is not required trusted server. In all these cases, decryption at users end is computationally intensive. So, this technique might be inefficient when users access using their mobile devices.

In Attribute Based Data Sharing with Attribute Revocation S. Yu et.al.[7]introduced an Attribute Based Data Sharing with Attribute Revocation. They mainly used semi-trustable on-line proxy servers. These servers enable an authority to revoke user attributes with minimal effort. This scheme was identically merge a technique of proxy re-encryption with CP-ABE. They also enable the authority to delegate most of laborious tasks to proxy servers. The benefit of this scheme is much more secure against cipher text attacks. One of the drawbacks of this scheme is respect to storage overhead that could be high if proxy-servers keep all the proxy re-key.

M. Li et.al [8] represented Scalable and Secure Sharing of Personal Health Records in cloud computing. They use Attribute-Based Encryption. In this scheme they were considering use of dual system encryption methodology. The encryption techniques from Multi-authority ABE as well as Key-Policy ABE are integrated into a one module. MA-ABE technique proves useful for key management and exile access handled by KP-ABE. The overall security of the system has been improved. Drawback is that Existing attribute revocation methods rely on a trusted server or lack of efficiency also they are not suitable to deal with the attribute revocation problem in data access control in multi-authority cloud storage systems.

C. Wang, Q. Wang, K. Ren, and W. Lou, [9], represent the research of data security in cloud. They proposed a privacy-preserving public auditing system. This system is proposed for managing multiple audit session of different users for their outsourced data files. In this paper, TPA is further extended to perform audits for multiple users efficiently. Authors were auditing protocol properly. It helps in to designing of auditing process to protecting data from “flowing away” towards external parties.

Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li [10], discussed about various verification schemes with public audit ability. In this any TPA act as verifier for evaluating the quality from an objective as well as independent perspective. In this procedure, Merkle Hash Tree (MHT) construction is used to manipulate proof of storage models. It is required for block tag authentication. TPA is used to build the system that aims to develop Dynamic data operation support, Public auditability and Block less verification of storage correctness assurance.

B. Wang, B. Li, and H. Li [11], proposed a scheme for public auditing to share the data with effective revocation of user. They utilize proxy re-signatures for public auditing. This scheme, implements the idea of proxy re-signatures. So that, an efficiency of user revocation is improved much more as well as computational resources are saved. Authors were assuming that cloud is a semi-trusted. In public auditing, public verifier can audit the integrity of shared data. In scalability cloud data can be efficiently shared on large-system.

Kan Yang [12], defined an access control framework for multi-authority system. They aim to solve user revocation problem in multi-authority system. For that they proposed CP-ABE scheme. It is efficient and scalable system.

Sonia Jahid, Prateek Mittal [13], represents EASiER scheme to solve efficient user revocation problem. It is access control architecture for OSN model. They were building prototype for applications such as facebook OSN for encryption.

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.

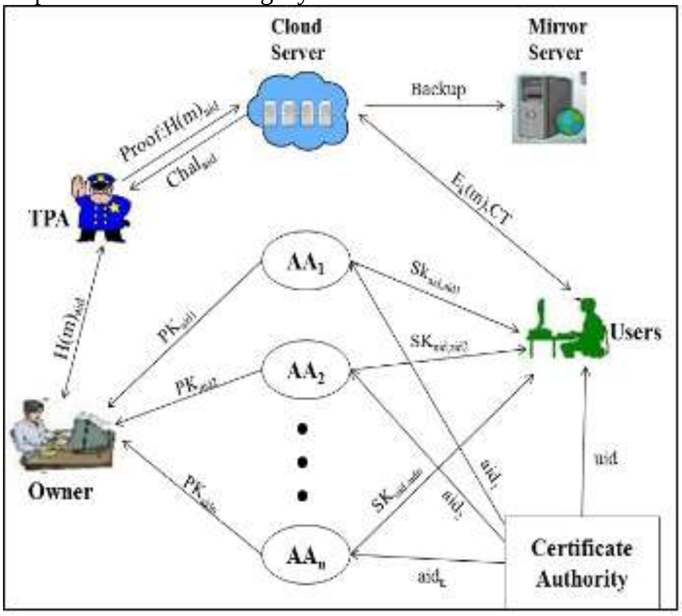

Figure 1: System Architecture

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.

- Setup Phase: CA (Certificate Authority): User & AA Registration
- Key Generation: Generate public and secret keys for user after validation.
- Data Encryption and Signing: Encrypt the data using secret key and sign.
- Metadata Generation: User will create metadata and upload on TPA.
- Data Upload: User enters user rights for other users and its respective attributes .The encrypted data is uploaded on cloud.
- Mirror Generation: When new file upload on Cloud will generate backup copy of uploaded data.
- Data Download: For data access user get key from AA and download respective file from cloud.
- Data Decryption: User decrypt the downloaded file using key received from AA.
- Attribute Revocation: It includes user revocation and add / modify user attribute for previously uploaded files. Data owner can modify these attribute set.
- Data Integrity Check: To check cloud data integrity, TPA generates challenge message to cloud. Cloud generates the proof of data and returns that proof to the TPA. TPA verifies the proof based on metadata and generates the data integrity proof report.
- Restore Data: Data owner can download the data backup copies if certain mishap happens with cloud data files.

IV. Experimental Results

We have developed our system in java. For testing we have hosted each entity on different machines. The cloud, Ca, AA and TPA has core i-3 processor with 4 gb RAM. Client system has i3 processor with 2 gb ram. On every system java runtime environment JRE-1.7 is installed. For development we have used jdk 1.7 and IDE: Eclipse and Netbeans are used. For Database storage we have used mysql 5.3 database.

For implementation of our system we have followed the academic structure of users. Following is the system user's structure with designation.

Consider a scenario, if user wants to share data with HOD and staff of department 1 and 2. Following attributes will be required to generate key.

Departmant1_HOD^Departmant1_staff^
Departmant1_HOD^Department2_staff

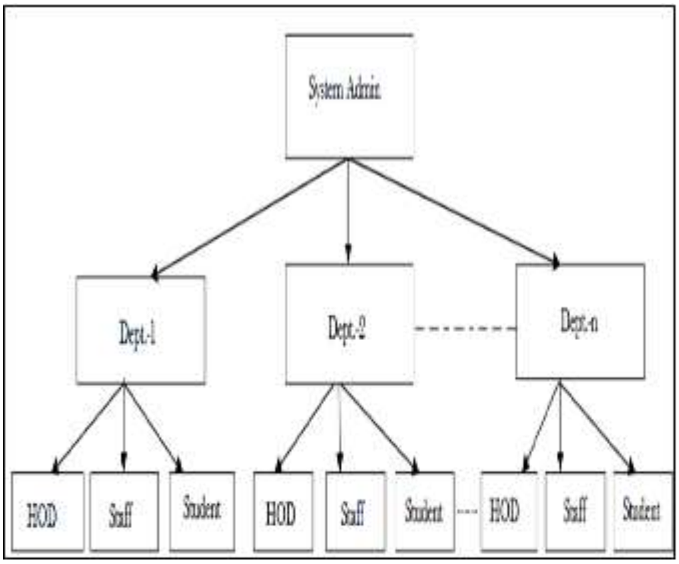

Fig.2. Work Breakdown Structure

Figure 3: Work BreakDown Structure

We have implemented ABE algorithm and calculated its performance.

File size in MB	Key generation Time in milliseconds	Encryption Time in milliseconds	Decryption Time in milliseconds
1	219	5342	7949
2	213	8970	14321
3	214	14307	23579
4	212	17423	27357
5	229	20342	32572

Table 1: Performance Analysis

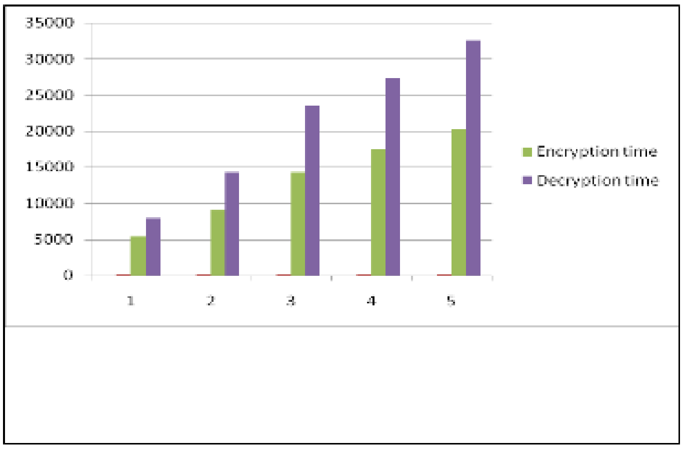

Figure 4: Result Graph

We have evaluated time required for token generation. The average time required for 10 users is 30miliSecndes.

We are working on key distribution servers and key management. After complete system implementation we will evaluate the system performance with

- Upload download time for different files
- File share and key allotment time

V. Conclusion

We proposed decentralized system for data security and data integrity. Multiple nodes work together to manage user identity, user data, data encryption keys, backup copies as well as we introduces 1 third party data auditor for data integrity check. This auditor verifies user data without knowing the original data. Multiuser environment supports data uploading and sharing. Data owner describes user access privileges to the uploaded data. Attribute based encryption technique CP-ABE is useful for efficient data encryption and user revocation.

In future we can implement file search facility for end user over encrypted cloud data.

VIII.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] J.Bethencourt, A.Sahai, and B.Waters, “Ciphertext-Policy Attribute-Based Encryption”, in Proc. IEEE Symp. Security and privacy (SP07), 2007, pp. 321-334.

[3] B. Waters, “Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization”, in Proc. 4th Intl Conf. Practice and Theory in Public Key Cryptography (PKC11), 2011, pp. 53-70.

[4] V. Goyal, A. Jain, O. Pandey, and A. Sahai, “Bounded Ciphertext Policy Attribute Based Encryption”, in Proc. 35th Intl Colloquium on Automata, Languages, and Programming (ICALP08), 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-EUROCRYPT10, 2010, pp. 62-91.

[6] M. Chase, “Multi-Authority Attribute Based Encryption”, in Proc. 4th Theory of
Cryptography Conf. Theory of Cryptography (TCC07), 2007, pp. 515-534.

[7] A.B. Lewko and B. Waters, “Decentralizing Attribute-Based Encryption”, in Proc.Advances in Cryptology-EUROCRYPT11, 2011, pp. 568-588

[8] 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 (ASIACCS10), 2010, pp. 261-270.

[9] 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.

[10] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in Proceedings of the 29th Annual IEEE International

[11] B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud," in Proceedings of the 32nd Annual IEEE International Conference on Computer Communications (INFOCOM'13), Turin, Italy, 2013, pp. 2904-2912.

[12] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," in Proceedings of the 2012 IEEE Fifth International Conference on Cloud Computing (CLOUD '12), Hawaii, USA, 2012, pp. 295-302.

[13] 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.

[14] 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.