ABSTRACT:

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. One important service provided by cloud computing to the data owners to outsource their data in cloud is cloud storage.

Index Terms:
Access control, multi-authority, CP-ABE, attribute revocation, cloud storage.

1. INTRODUCTION:

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.
In this paper, we first propose 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. As described in Table 1, our attribute revocation method is efficient in the sense that it incurs less communication cost and computation cost, and is secure in the sense that it can achieve both backward security (The revoked user cannot decrypt any new ciphertext that requires the revoked attribute to decrypt) and forward security (The newly joined user can also decrypt the previously published ciphertexts, if it has sufficient attributes). Our scheme does not require the server to be fully trusted, because the key update is enforced by each attribute authority and not by the servers. Even if the server is not semi-trusted in some scenarios, our scheme can still guarantee the backward security. Then, we apply our proposed revocable multi-authority CP-ABE scheme as the underlying techniques to construct the expressive and secure data access control scheme for multi-authority cloud storage systems.

DATA ENCRYPTION BY OWNERS:

Before outsourcing the data to cloud, the data owner first partitions the data into several components according to logical granularities as \( m = \{m_1, \ldots, m_n\} \). For example, data can be partitioned into \{name, address, employee, salary, contact number\}, next the data components are encrypted with different content keys \( \{k_1, \ldots, k_n\} \) using symmetric encryption method, last the access structure mechanism \( M_i \) is defined for each content key \( k_i \). The encryption algorithm takes \( GPP \) as input, a collection of public keys for all AAs and outputs \( CT = GPP, \{PK_{aid}k_i\} \). The decryption by users is achieved by decrypting the content key with the help of the aggregated key and corresponding access permission id. In this work the data anonymity level is increased by wrapping the data values before data transmission.

That is user request is achieved by wrapping around the user access permission details with the data before transmitting storing it in the server. Hence only the user who satisfies the corresponding access permission details like verification information only will gain access to it. Based on the access permission given to the users, the new encryption key will be generated for individual users. By using the encryption that is generated for the unique user, each user can down load the data which is only accessible to them. In our scheme, the key update is done by each attribute authority and not by the servers. The semi trusted natures of authorized user are eliminated where the data are hidden from the authorized users also and it achieves more privacy and security over data.

2 SYSTEM MODEL AND SECURITY MODEL:

2.1 System Model:

The remaining paper is structured as follows. Section II describes the background. Section III describes the structure and the system model. The construction of the data access control scheme is given in section IV. The security analysis is described in section V. The conclusion is givessection VI.

![Diagram](image-url)
The Decrypt(CT,GPKuid,GSKuid[Suid,aid])= (|aid \in \mathcal{EAA}_s| \in \mathcal{K}|aid\in\mathcal{EAAs}_{uid}, ruid...n)= CT,GPKuid,GSKuid

7 CONCLUSION:

In this paper, we proposed a revocable multi-authority CPABE scheme that can support efficient attribute revocation. Then, we constructed an effective data access control scheme for multi-authority cloud storage systems. We also proved that our scheme was provably secure in the random oracle model. The revocable multi-authority CPABE scheme is a promising technique, which can be applied in any remote storage systems and online social networks etc.

ACKNOWLEDGMENT:

This work was supported by the Research Grants Council of Hong Kong under Project CityU.

REFERENCES


Kan Yang received the BEng degree from University of Science and Technology of China, in 2008 and the PhD degree from City University of Hong Kong, Hong Kong, in August 2013. He was a visiting scholar in State University of New York at Buffalo, in 2012. His research interests include cloud security, big data security, cloud data mining, cryptography, social networks, wireless communication and networks, and distributed systems.

He is a Student Member of the IEEE. Xiaohua Jia received the BSc and MEng degrees from University of Science and Technology of China, in 1984 and 1987, respectively, and the DSc degree in information science from University of Tokyo, Japan, in 1991. He is currently Chair Professor at the Department of Computer Science at City University of Hong Kong. His research interests include cloud computing and distributed systems, computer networks, wireless sensor networks and mobile wireless networks. Prof. Jia is an editor of IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS (2006-2009), Wireless Networks, Journal of World Wide Web, Journal of Combinatorial Optimization, etc. He is the General Chair of ACM MobiHoc 2008, TPC Co-Chair of IEEE MASS 2009, Area- Chair of IEEE INFOCOM 2010, TPC Co-Chair of IEEE GlobeCom 2010, Ad Hoc and Sensor Networking Symp, and Panel Co-Chair of IEEE.