ISSN 2349-0292
Impact Factor 2.365

Global Journal of Advanced Engineering Technologies and Sciences

SECURE MULTI OWNER DATA SHARING

Shaharukh Pathan*, Pramod Mahale
*Student of Computer Engineering AAEMF'S COE & MS, Bhima Koregaon Pune, India

Abstract
Here is a Major problem in public clouds about the sharing of documents on attribute based policies, sharing data in a dynamic groups. With the help of advantage of low maintenance, cloud computing gives the effective solution for sharing group resource among cloud users. As the sharing of documents with different keys like attribute based encryption (ABE) approach has some weaknesses so, it cannot handle efficiently adding/revoking users and attributes of identification. Unfortunately, there is still a challenging issue, to share a data in multi-owner manner and preserve data and their confidentiality. In this paper, we propose Multi-Owner Data Sharing scheme, using attribute based encryption method. By using maximum advantage group signature, signed receipts and dynamic broadcast encryption techniques, any can share the data on the cloud. As the result we achieve the secure data sharing in the cloud we expect to combine the group signature and dynamic broadcast encryption techniques.

Keywords: Cloud computing, shared data, access control, dynamic groups.

Introduction
Cloud computing is the use of computing resources(hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers. The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games. Cloud computing is recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful datacenters. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its staffs in the same group or department to store and share files in thecloud. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud.

Literature Survey
1)Scalable Secure File Sharing on Untrusted Storage. Plutusis a cryptographic storage system that enables secure file sharing without placing much trust on the file servers. In particular, it makes novel use of cryptographic primitives to protect and share files. Plutus features highly scalable key management while allowing individual users to retain direct control over who gets access to their files. We explain the mechanisms in Plutus to reduce the number of cryptographic keys exchanged between users by using file groups, distinguish file read and write access, handle user revocation efficiently, and allow an un trusted server to authorize file writes. We have built a prototype of Plutus on Open AFS.

2)Securing Remote Untrusted Storage This paper presents SiRiUS, a secure file system designed to be layered over insecure network and P2P file systems such as NFS, CIFS, Ocean Store, and Yahoo! Briefcase. SiRiUS assumes the network storage is untrusted and provides its own read-write cryptographic access control for file level sharing. Key

management and revocation is simple with minimal out-of band communication. File system freshness guarantees are supported by SiRiUS using hash tree constructions. SiRiUScontains a novel method of performing file random access in a cryptographic file system without the use of a block server. Extensions to SiRiUS include large scale group sharing using the NNL key revocation construction. Our implementation of SiRiUS performs well relative to the underlying file system despite using cryptographic operations.

3)Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage In 1998, Blaze, Bloomer, and Strauss (BBS) proposed an application called atomic proxy re-encryption, in which a semi trusted proxy converts a cipher text for Alice into a cipher text for Bob without seeing the underlying plaintext. We predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS reencryption has been hindered by considerable security risks. Following recent work of Dodis and Ivan, we present new re-encryption schemes that realize a stronger notion of security and demonstrate the usefulness of proxy reencryption as a method of adding access control to a secure file system. Performance measurements of our experimental file system demonstrate that proxy re-encryption can work effectively in practice.

Proposed Methodology And Discussion

A secure multi-owner data sharing scheme is provided. It implies that any user in the group can securely share data with others by the un trusted cloud. Our proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users. A secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource, is provided. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur. A rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead. Advantages of Proposed System:

- Any user in the group can store and share data files with others by the cloud.
- Group manager can check all details of user.
- A new user can directly decrypt the files stored in the cloud before his participation.

IMPLEMENTATION
Modules:
Cloud Module:

In this module, we create a local Cloud and provide priced abundant storage services. The users can upload their data in the cloud. We develop this module, where the cloud storage can be made secure. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to we assume that the cloud server is honest but curious.

Group Manager Module:

ISSN 2349-0292
Impact Factor 2.365

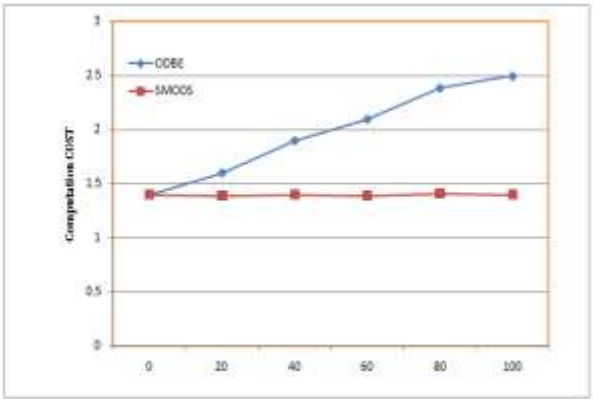
Group manager takes charge of followings,
1. System parameters generation,
2. User registration
3. User revocation the real identity of a dispute data owner.

Group Member Module:

Group member takes charge of followings,
1. File Security Module
2. Group Signature Module
3. User Revocation Module

Experimental Results

Comparison on computation cost for file generation between SMODS and ODBE



Above digram shows about computation cost of file generation process in SMODS and ODBE. We list the comparison on computation cost of clients for data generation operations between Mona and the way that directly using the original dynamic broadcast encryption (ODBE). It is easily observed that the computation cost in SMODS is irrelevant to the number of revoked users. On the contrary, the computation cost increases with the number of revoked users in ODBE. The reason is that the parameters Pr; Zr can be obtained from the revocation list without sacri_cing the security in Mona, while several time-consuming operations including point multiplications in G1 and exponentiations in G2 have to be performed by clients to compute the parameters in ODBE. From Figs. we can find out that sharing a 100-Mbyte one, cost a client about 0.2 and 1.4 seconds in our scheme, respectively, which implies that the symmetrical encryption operation domains the computation cost when the file is large.

Conclusion

In proposed scheme for dynamic groups in an un trusted cloud have been designed. In multi owner, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

Refference

1. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A View of Cloud Computing,”Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.
2. S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc. Int’l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.
3. S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing,” Proc. IEEE INFOCOM, pp. 534-542, 2010.
4. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, “Plutus: Scalable Secure File Sharing on UntrustedStorage,” Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.
5. E. Goh, H. Shacham, N. Modadugu, and D. Boneh, “Sirius: Securing Remote Untrusted Storage,” Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.
6. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage,” Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.
7. R. Lu, X. Lin, X. Liang, and X. Shen, “Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing,”Proc. ACM Symp.Information, Computer and Comm. Security, pp. 282-292, 2010.
8. B. Waters,“Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,”Proc. Int’l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography,
9. http://eprint.iacr.org/2008/290.pdf, 2008.