A Secure Cloud Storage System Using Attribute Based Encryption Scheme

Rekha.M[1], Dr. S. Santhosh Kumar[2], Dr.C.Balakrishnan[3]
[1]M.Phil. Scholar Alagappa University, Karaikudi
[2]Assistant Professor, Department of Computer Science and Engineering, Alagappa University, Karaikudi
[3]Assistant Professor, Alagappa Institute of Skill Development, Alagappa University, Karaikudi

ABSTRACT

Cloud storage is a progressively popular application of cloud computing which can provide on-demand outsourcing data services for both organizations and individuals. Attribute Based Encryption (ABE) has been widely used in cloud computing where a Data Provider provides outsources of the user encrypted data to a Cloud Service Provider. However, the users may not fully trust the Cloud Service Providers (CSPs). So, the data provider is very difficult to determine whether the CSPs meet their legal expectations for data security or not. Therefore, it is critical to develop efficient auditing techniques to strengthen data owners trust and confidence in cloud storage. An existing work has developed public auditing scheme for secure cloud storage based on the Dynamic Hash Table (DHT). In that, the DHT is a new two-dimensional data structure located at a Third Parity Auditor (TPA) to record the data property information for dynamic auditing. Differing from the existing works, the proposed scheme migrate the authorized information from the CSP to the TPA, and thereby significantly reduces the computational cost and communication overhead. Meanwhile, exploiting the structural advantages of the DHT, the proposed scheme can also achieve higher updating efficiency than the state-of-the-art schemes. In addition, the proposed scheme extends for the purpose of support privacy preservation by combining the authenticator based on the public key with the random masking which is generated by the TPA. Also, the proposed scheme achieves batch auditing by employing the aggregate BLS (Boneh–Lynn–Shacham) signature technique algorithm which is more secure compared to other algorithms. In this way, the proposed work produces the effective results to secure auditing for cloud storage based on the attributes such as computation complexity, storage costs and communication overhead.

Keywords: *Cloud Storage, Attribute Based Encryption (ABE), Third Party Auditor, Dynamic Hash Table, Cloud Service Provider, Authorized Information.*

INTRODUCTION

In the recent research environment, the Cloud Storage plays an important role in cloud computing. It provides powerful and on-demand outsourcing data services for users exploiting highly virtualized infrastructures. Due to the low cost and high performance of cloud storage, a growing number of organizations and individuals are tending to outsource their data storage to

professional Cloud Service Providers (CSP), which buoys the rapid development of cloud storage and its relative techniques in recent years.

However as a new cutting edge technology, cloud storage still faces many security challenges. One of the biggest concerns is how to determine the security. In that, the cloud security can be checked the cloud storage system and its provider meet the legal expectations of customers for data security or not. This confusion has created by the following reasons.

A cloud users / data owner who is outsourced their data in clouds. It can be no longer verified the integrity of their data via traditional techniques that are often employed in local storage scenarios. In this way, many solutions have been created to overcome this problem. That can be divided into two categories:

- ✓ Private Auditing.
- ✓ Public Auditing.

Private Auditing

Private auditing is the initial model for remote checking of data integrity. In this, the verification operation is performed directly between data owners and CSPs if the auditing is low cost. It cannot provide convincing / better auditing results if the owners and CSPs often mistrust each other or they would not understand each other. Moreover, it is not advisable for the users to carry out the audit frequently, since it would substantially increase the overhead that the users may not afford.

Public Auditing

The public auditing scheme (*Ateniese et al*.) is the second model of auditing scheme. In this, the verification work has done by an authorized Third Party Auditor (TPA). Compared with the creator, the latter can offer dependable auditing results and significantly reduce users unnecessary burden by introducing an independent TPA. Thus, it is more rational and practical, and popularly believed to be the right direction of future development. For this purpose, there have been many of the schemes are proposed for encryption such as simple encryption technique.

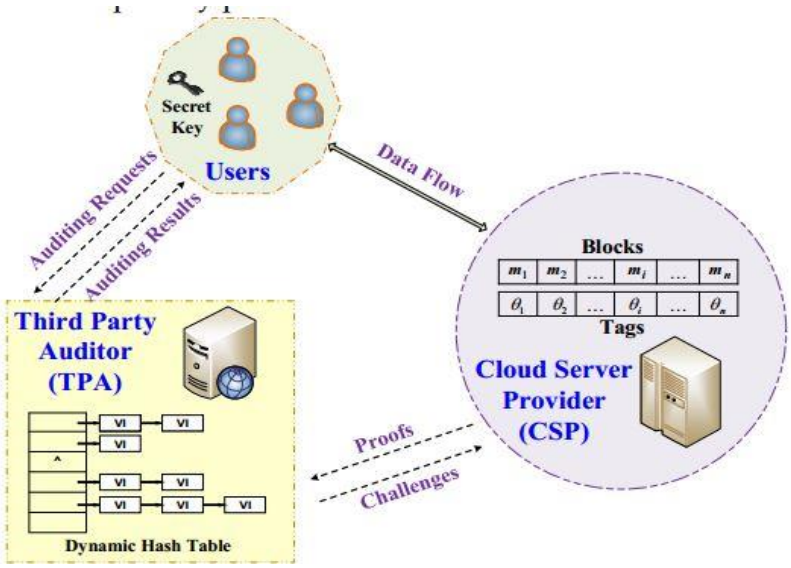


Figure 1: Third-party auditor prototype for cloud storage

Simple Encryption Technique

Attribute-Based Encryption (ABE) scheme which is one of the simple encryption technique which has been developed and modified further into Key Policy Attribute based encryption (KP-ABE) , Cipher-text Policy Attribute Based Encryption (CP-ABE) and further it has been proposed as CP-ASBE and furthermore HABE and HASBE so on. This is according to how flexible, scalable and fine grained access control [10] is provided by each scheme.

Cloud Security

Cloud computing systems and services have become major targets for cyber attackers. To provide strong protection of cloud platforms, infrastructure, hosted applications and data stored in the cloud. It needs to address the security issue from a range of perspectives-from secure data and application outsourcing, to anonymous communication, to secure multiparty computation. This special issue on cloud security aims to address the importance of protecting and securing cloud platforms, infrastructures, hosted applications, and data storage.

There are numerous security issues and challenges in cloud computing because it encompasses many technologies such as networks, databases, operating system, virtualization, resource scheduling, transaction management, concurrent control and memory management [8]. This is very important because the cloud service provider must ensure that the users is not facing any serious problem like data loss and data theft which may cause a great loss depending on the

sensitivity of the data stored in cloud. A malicious user may pretend to be the legitimate users and infecting the cloud.

Data at rest is the major issues in cloud computing because users may store all their common, private, or even sensitive data in the cloud which can be accessed by anyone anywhere. Data theft is a very common issues that are facing by the cloud service providers nowadays. Besides, some cloud service providers even don't provide their own server because of the cost effectiveness and flexibility. There are also incidents like data loss which might be also a serious problem for the users. For example, the server is suddenly shut down and causes data loss of the users. Furthermore, natural disaster might also cause data to be damaged or corrupted. Therefore, physical data location can be considered one of the security issues in cloud computing.

The cloud computing service provider must enforce their own policies to ensure the safety of the data users stored in their cloud model. They must make sure that they realize who is actually accessing the data stored in the cloud and only the authorized person can maintain the cloud service model [9]. The security of cloud computing should be done on the provider side and also the user side. Cloud service provider should provide a good layer of security protection for the users while the users should not tampered with the other user's data. The cloud computing is a good way to reduce the cost and provide more storage if and only if the security is done by both provider and user. [8] Claimed that regulatory reform is essential to protect sensitive data in the cloud since one of the most challenging aspect in cloud computing is to ensures that the consumer have trust in privacy and security of their data.

Cloud computing is a model that helps to speed up and increase the flexibility of data management with reduced cost. It is undeniable that cloud computing has brings us lots of benefits and becoming more popular nowadays. Many large companies start using cloud service in their business. While the cloud computing is widely used, the security becomes a concern to everyone who use cloud services. There is a lot of security arises continuously while there are improvement as well on the security model of the cloud service provided. Despite the increasing use of the cloud service, the user should use the cloud service provided wisely in a way that always ensure good security practices so that this technology have the potential to bring the information technology to the next level. Cloud computing might help us to separate he software from the hardware as more technologies are used as service using cloud and software might have a highly abstract space with

the computer hardware. It is expected that this paper provides some basis or foundation in regards to issues and challenges in cloud computing.

Attribute Based Encryption

Sahai and Waters [6] introduced the notion of Attribute Based Encryption (ABE), and then Goyal et al. [9] formulated Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE) as two complimentary forms of ABE.

First, KP-ABE construction given in [4] realized the monotonic access structures, the first KP-ABE system supporting the expression of non-monotone formulas which was presented [7] to enable more viable access policies, and the first large class KP-ABE system was presented by in the standard model [8]. In this scenario, the KP-ABE is less flexible than CP-ABE because the access policy is determined once the user's attribute private key is issued.

LITERATURE SURVEY

A. Attribute based encryption (ABE)

Sahai and Waters [11] first introduced the attribute based encryption (ABE) for enforced access control through public key cryptography. The main goal for these models is to provide security and access control. The main aspects are to provide flexibility, scalability and fine grained access control. In classical model, this can be achieved only when user and server are in a trusted domain. But what if their domains are not trusted or not same? So, the new access control scheme that is 'Attribute Based Encryption (ABE)' scheme was introduced which consist of key policy attribute based encryption (KP-ABE). As compared with classical model, KP-ABE provided fine grained access control. However it fails with respect to flexibility and scalability when authorities at multiple levels are considered. In ABE scheme both the user secret key and the cipher text are associated with a set of attributes. A user is able to decrypt the cipher-text if and only if at least a threshold number of attributes overlap between the cipher-text and user secret key.

B. Key Policy Attribute Based Encryption (KP-ABE):-

To enable more general access control, *V. Goyal, O. Pandey, A. Sahai, and B. Waters [3]* proposed a key-policy attribute-based encryption (KP-ABE) scheme. It is the modified form of classical model of ABE. Exploring KP-ABE scheme, attribute policies are associated with keys and data is associated with attributes. Encrypted, that is who encrypts the data, is associated with

the set of attributes to the data or message by encrypting it with a public key. Users are assigned with an access tree structure over the data attributes. The nodes of the access tree are the threshold gates. The leaf nodes are associated with attributes. The secret key of the user is defined to reflect the access tree structure. Hence, the user is able to decrypt the message that is a cipher text if and only if the data attributes satisfy the access tree structure. In KP-ABE, a set of attributes is associated with cipher text and the user's decryption key is associated with a monotonic access tree structure [5]. When the attributes associated with the cipher text satisfy the access tree structure, then the user can decrypt the cipher text.

In the cloud computing, for efficient revocation, an access control mechanism based on KP-ABE and an encryption technique used together. It enables a data owner to reduce most of the computational overhead to the servers. The KP-ABE scheme provides fine-grained access control. Each file or message is encrypted with a symmetric data encryption key (DEK), which is again encrypted by a public key, that is corresponding to a set of attributes in KP-ABE, which is generated corresponding to an access tree structure. The encrypted data file is stored with the corresponding attributes and the encrypted DEK. If and only if the corresponding attributes of a file or message stored in the cloud satisfy the access structure of a user's key, then the user is able to decrypt the encrypted DEK. That can be used to decrypt the file or message.

PROPOSED RESEARCH WORK

Future work includes efficient data ownership verification, scheme optimization with hardware acceleration at IoT devices for practical deployment, and development of a flexible solution to support deduplication and data access controlled by either the data owner or its representative agent.In this paper concentrate on the design of an effective public aduditing scheme based on cloud illustrated in which involves the following three entities:User , who stores a great quantity of data files in the cloud, can be an individual or a organization; Cloud service provider(CSP), who manage and coordinates a number of cloud server to offer scalable and on-demand outsourcing data services for user; and Third party Auditor(TPA), who can verify the relaibility of the cloud stroage services (CSS)credibly and dependably on behalf of the user upon request. User can be releived of the burden of stroage and computation while enjoying the stroage and Maintance service by outsourcing their data into the CSP. However,due to the loss of local possession of the data,they are keen to ensure the correctness and integrity of their data periodically. To obtain a

convincing answer as well as alleviate the users' burden potendiatially induced by the frequent verification, the TPA is involved to check the integrity of the users' data stroed in the cloud. However, in the whole verification procedd, the TPA is not expected to be able to learn the actual content of the users; data for privacy protection.

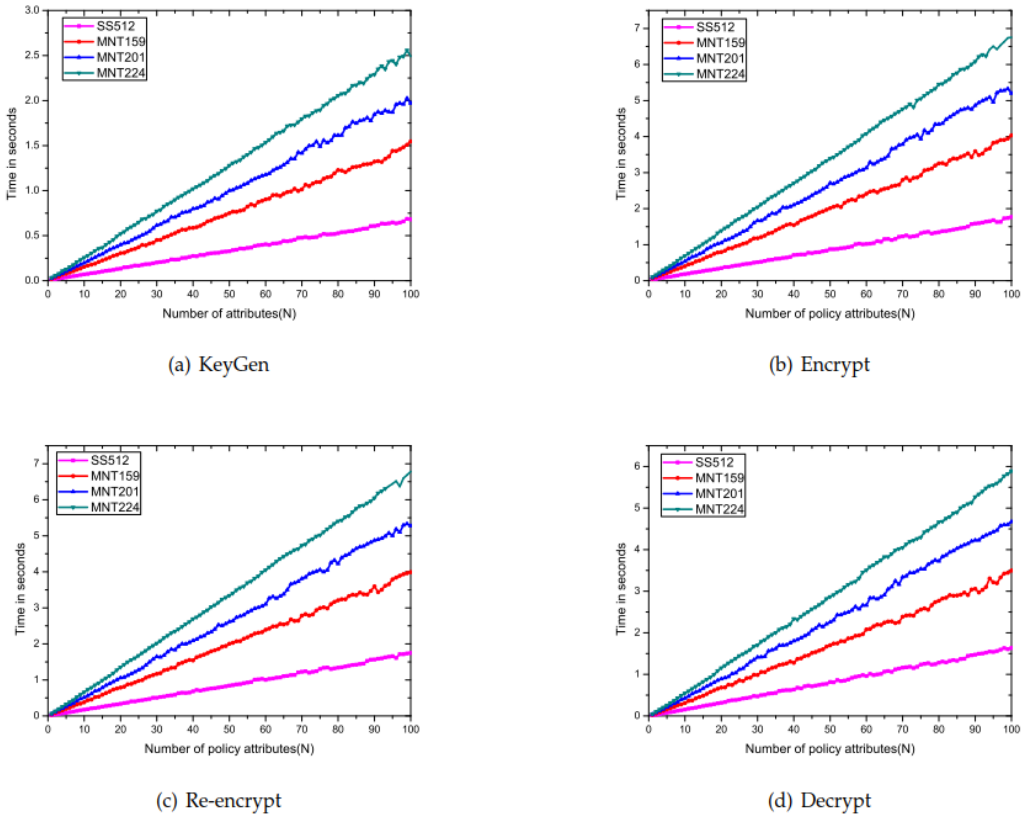
Attribute-based encryption (ABE) allows each cipher text to be associated with an attribute, and the master-secret key holder can extract a secret key for a policy of these attributes so that a cipher text can be decrypted by this key if its associated attribute conforms to the policy. In a multiauthority ABE scheme, multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to users and encryptions can require that a user obtain keys for appropriate attributes from each authority before decrypting a message. However, the major concern in ABE is collusion-resistance but not the compactness of secret keys

Future work includes efficient data ownership verification, scheme optimization with hardware acceleration at IoT devices for practical deployment, and development of a flexible solution to support deduplication and data access controlled by either the data owner or its representative agent.

RESULT AND DISCUSSION

A cryptographic primitive called adaptable CP-ABE, where a semi-trusted proxy is introduced into the setting of CP-ABE. The proxy, given a system wide trapdoor key, is able to transform any ciphertext under one access policy into ciphertexts of the same plaintext under any other access policies without learning any information about the plaintext during the process of transformation. However, this method of using a single trapdoor key for all ciphertexts is quite risky, since if the single key is compromised, the security for the system will be totally bro-ken. An adversarial user using the compromised trapdoor key can regenerate a ciphertext into an access structure that user attributes satisfy, and thus he/she can obtain theplaintext not intended for user. Besides, the trapdoor key in [4] is generated by the AA who already controls the decryption keys in the system, so it is desirable to reduce its power in manipulating the encryption. Unlike that in [13], our technique is one-to-one such that each trapdoor keycan only be used to transform its corresponding ciphertext. Therefore, even at some point, a trapdoor key is comprised,the damage is limited to

one message. At a high level, ourtechnique brings another way to build adaptive CP-ABEsystems from a different point of view.



(a) KeyGen (b) Encrypt

(c) Re-encrypt (d) Decrypt

Fig. 5: Performance of our attribute-based storage system supporting secure deduplication.

CONCLUSION

Nowadays, cloud storage, which can offer on-demand outsourcing data services for both organizations and individuals, has been attracting more and more attention. However, one of the most serious obstacles to its development is that users may not fully trust the CSPs in that it is difficult to determine whether the CSPs meet their legal expectations for data security. Therefore, it is critical and significant to develop efficient auditing techniques to strengthen data owners' trust and confidence in cloud storage. Differing from the existing works, our scheme migrates the auditing metadata-ta excerpt the block tags from the CSP to the TPA, and thereby significantly reduces the computational cost and communication overhead. Meanwhile, exploiting the structural advantages of the DHT, our scheme can also achieve better performance than the state-of-the-art schemes in the updating phase. In addition, for privacy preservation, our scheme introduces a

random masking provided by the TPA into the process of generating proof to blind the data information. The results demonstrate that our scheme can effectively achieve secure auditing in clouds, and induce significantly fewer costs of storage, communication and computation than the previous schemes.

REFERENCES

[1] R. Choo, J. Domingo-Ferrer, and L. Zhang, "Cloud cryptog- raphy: Theory, practice and future research directions," Future Generation Comp. Syst., vol. 62, pp. 51–53, 2016.

[2] K. R. Choo, M. Herman, M. Iorga, and B. Martini, "Cloud foren-sics: State-of-the-art and future directions," Digital Investigation,vol. 18, pp.77–78, 2016.

[3] D. Quick, B. Martini, and K. R. Choo, Cloud Storage Forensics. Syngress Publishing / Elsevier, 2014. [On-line]. Available: http://www.elsevier.com/books/cloud-storage-forensics/quick/978-0-12-419970-5

[4] D. Quick and K. R. Choo, "Google drive: Forensic analysis of data remnants," J. Network and Computer Applications, vol. 40, pp. 179–193, 2014.

[5] B. Zhu, K. Li, and R. H. Patterson, "Avoiding the disk bottleneck in the data domain deduplication file system," in 6th USENIX Conference on File and Storage Technologies, FAST 2008, February 26-29, 2008, San Jose, CA, USA. USENIX, 2008, pp. 269–282

[6] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Message-locked encryption and secure deduplication," in Advances in Cryptology EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings, ser. Lecture Notes in Computer Science, vol. 7881. Springer, 2013, pp. 296–312.

[7] M. Abadi, D. Boneh, I. Mironov, A. Raghunathan, and G. Segev,"Message-locked encryption for lock-dependent messages," in Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings,Part I, ser. Lecture Notes in Computer Science, vol. 8042. Springer,2013, pp. 374–391

[8] S. Keelveedhi, M. Bellare, and T. Ristenpart, "Dupless: Server-aided encryption for deduplicated storage," in Proceedings of the22th USENIX Security Symposium, Washington, DC, USA, August 14-16, 2013. USENIX Association, 2013, pp. 179–194.

[9] M. Bellare and S. Keelveedhi, "Interactive message-locked encryption and secure deduplication," in Public-Key Cryptography – PKC 2015 - 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD, USA, March 30 – April 1, 2015, Proceedings, ser. Lecture Notes in Computer Science, vol. 9020. Springer, 2015, pp. 516–538.

[10] "Thunderclouds: Managing SOA-Cloud Risk", Philip Wik. 2011-10, Service Technology Magazine.

[11] Chunye Gong, "the Characteristics of cloud computing", 2010, 39th international conference on parallel processing workshops.

[12] B.R. Kandukuri, R.P.V. and A.Rakshit "Cloud Security Issues" In IEEE international conference on services computing (SCC).

[13] M.R. Abbasy and B. Shanmugam, on, 2011, "Enabling Data Hiding for Resource Sharing in Cloud Computing Environments Based on DNA Sequences," in Services

[14] J. Feng, Y. Chen, D. Summerville, W. Ku, and Z. Su, "Enhancingcloud storage security against roll-back attacks with a new fair multi-party non-repudiation protocol," on 2011 in Consumer Communications and Networking Conference (CCNC).

[15] Lori M. Kaufman, "Data security in the world of cloud computing", July. Aug. 2009. IEEE Security and Privacy Journal, Vol. 7