ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2 Issue 1 Jan-March 2014
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

Data Sharing in Cloud Using Hybrid Cryptosystem

[I]N. Aravindhu, [II]G. Venkatesan, [III]S. Anandhanayagie
[I]Senior Assistant Professor(CSE), Christ College of Engineering & Technology, Pondicherry University, Pondicherry, India
[II, III]M.Tech final year Students, (CSE), Christ College of Engineering & Technology, Pondicherry University, Pondicherry, India

Abstract
With the character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud user. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an un trusted cloud is still a challenging issue, due to the frequently change of the membership. In this project we present a new efficient Secret sharing revocation scheme which is efficient, secure, and unassisted. In this scheme, the original data are first divided into a number of slices, and then published to the cloud storage. When a revocation occurs, the data owner needs only to retrieve one slice, and re-encrypt and re-publish it. Thus, the revocation process is accelerated by affecting only one slice instead of the whole data. To securely encrypt the data and key generation using Hybrid cryptosystem and also using blind signature technique and All or Nothing Transformation(AONT) , this will allow signer sign without learn the content of the original message and stored in cloud. This Hybrid cryptosystem provides three cryptographic primitives such as integrity, confidentiality and authentication. This can be achieved by the combinatorial effect of Elliptic Curve Cryptography implemented by Elliptic Curve Diffie Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA), Dual RSA and Hash algorithm implemented by Message Digest 5. This new security algorithm has been designed for better security with integrity using a combination of both symmetric and asymmetric cryptographic techniques.

Keywords
AONT, ECDSA, ECDH, Hybrid cryptosystem.

I. Introduction

The term "cloud", as used in this white paper, appears to have its origins in network diagrams that represented the internet, or various parts of it, as schematic clouds. "Cloud computing" was coined for what happens when applications and services are moved into the internet "cloud." Cloud computing is not something that suddenly appeared overnight; in some form it may trace back to a time when computer systems remotely time-shared computing resources and applications. More currently though, cloud computing refers to the many different types of services and applications being delivered in the internet cloud, and the fact that, in many cases, the devices used to access these services and applications do not require any special applications. In the world where the users of the computer of today's internet world do not, install store their application or data on their own computers, today every piece of your information or data would reside on the Cloud .Cloud computing comes into focus only, a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software. It encompasses any pay-per-use service that, in real time over the Internet. Cloud is Internet based development and use of computing technology. The style of computing is scalable and virtualized resources are provided as a service over the Internet. Clouds services are infrastructure are a service, platform as a service and software as a service .cloud infrastructures are much more powerful and reliable than personal computing devices, but they are still susceptible to internal and external threats that can damage data integrity, Next, for the benefits of possession, there exist various motivations for cloud service providers to behave untruth toward the cloud users.

II. EXISTING SYSTEM

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 the cloud. 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. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues. First, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Without the guarantee of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers.

On the other hand, unconditional identity privacy may incur the abuse of privacy. For example, misbehaved staff can deceive others in the company by sharing false files without being traceable. Therefore, traceability, which enables the group manager (e.g., a company manager) to reveal the real identity of a user, is also highly desirable .Second it is highly recommended that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner. Compared with the single-owner manner,

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

where only the group manager can store and modify data in the cloud, the multiple-owner manner is more flexible in practical applications. More concretely, each user in the group is able to not only read data, but also modify his/her part of data in the entire data file shared by the company .Last but not least, groups are normally dynamic in practice, e.g., new staff participation and current employee revocation in a company. The changes of membership make secure data sharing extremely difficult. On one hand, the anonymous system challenges new granted users to learn the content of data files stored before their participation, because it is impossible for new granted users to contact with anonymous data owners, and obtain the corresponding decryption keys. On the other hand, an efficient membership revocation mechanism without updating the secret keys of the remaining users is also desired to minimize the complexity of key management.

To achieve secure data sharing for dynamic groups in the cloud, we expect to combine the group signature and dynamic broadcast encryption techniques. Specially, the group signature scheme enables users to anonymously use the cloud resources, and the dynamic broadcast encryption technique allows data owners to securely share their data files with others including new joining users.

Unfortunately, each user has to compute revocation parameters to protect the confidentiality from the revoked users in the dynamic broadcast encryption scheme, which results in that both the computation overhead of the encryption and the size of the cipher text increase with the number of revoked users. Thus, the heavy overhead and large cipher text size may hinder the adoption of the broadcast encryption scheme to capacity-limited users. To tackle this challenging issue, we let the group manager compute the revocation parameters and make the result public available by migrating them into the cloud. Such a design can significantly reduce the computation overhead of users to encrypt files and the cipher text size. Specially, the computation overhead of users for encryption operations and the cipher text size is constant and independent of the revocation users.

A. Dynamic Broadcast Encryption

Broadcast encryption [1] enables a broadcaster to transmit encrypted data to a set of users so that only a privileged subset of users can decrypt the data. Besides the above characteristics, dynamic broadcast encryption also allows the group manager to dynamically include new members while preserving previously computed information, i.e., user decryption keys need not be recomputed, the morphology and size of cipher texts are unchanged and the group encryption key requires no modification. The first formal definition and construction of dynamic broadcast encryption are introduced based on the bilinear pairing technique in, which will be used as the basis for file sharing in dynamic groups. A company uses a cloud to enable its staffs in the same group or department to share files. The system model consists of three different entities: the cloud, a group manager (i.e., the company manager), and a large number of group members (i.e., the staffs).

Cloud is operated by CSPs and provides price abundant storage services. 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. That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes but will try to learn the content of the stored data and the identities of cloud users.

Group manager takes charge of system parameters generation, user registration, user revocation, and revealing the real identity of a dispute data owner. In the given example, the group manager is acted by the administrator of the company. Therefore, we assume that the group manager is fully trusted by the other parties.

Group members are a set of registered users that will store their private data into the cloud server and share them with others in the group. In our example, the staffs play the role of group members. Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company.

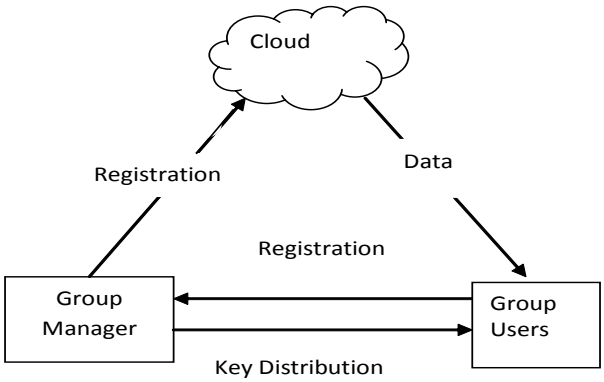

Fig. 1: Existing System model

III. Proposed System

In the proposed system the following techniques are used to overcome the problem of existing system.

A. All-or-Nothing Transforms (AONT)

All-or-Nothing Transforms (AONTs) [7], which have been proposed by Rivest as a mode of operation for block ciphers. An AONT is an unkeyed, invertible, randomi transformation, with the property that it is hard to invert unless all of the output is known. Applications of AONTs include improving the security and speed of encryption. An all-or-nothing package transformation is one in which some text is transformed into message blocks, such that all blocks must be obtained before the reverse transformation can be applied. Thus, if any blocks are corrupted or lost, the original message cannot be reproduced. An all-or-nothing package transformation is not encryption, although a block cipher algorithm is used. The encryption key is randomly generated and is extractable from the message blocks.

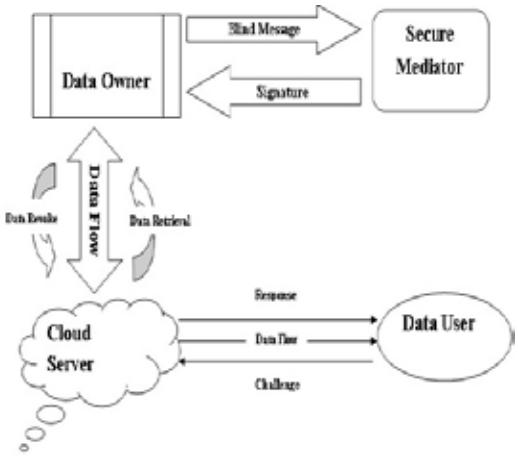

Fig. 2: Proposed System model

1. Cipher-Block Chaining (CBC)

In CBC process, each block of plaintext is XOR with the previous cipher text block before being encrypted. This way, each cipher text block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block. If the first block has index 1, the mathematical formula for CBC encryption is

$$C_i = E_K(P_i \oplus C_{i-1}), C_0 = IV$$

While the mathematical formula for CBC decryption is

$$P_i = D_K(C_i) \oplus C_{i-1}, C_0 = IV.$$

Decrypting with the incorrect IV causes the first block of plaintext to be corrupt but subsequent plaintext blocks will be correct. This is because a plaintext block can be recovered from two adjacent blocks of cipher text. As a consequence, decryption can be parallelized. Note that a one-bit change to the cipher text causes complete corruption of the corresponding block of plaintext, and inverts the corresponding bit in the following block of plaintext, but the rest of the blocks remain intact.

B. Digital Signature

A digital signature [4] is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

1. Blind signature

Blind signature [4] as introduced by David Chaum is a form of digital signature in which the content of a message is disguised (blinded) before it is signed. The resulting blind signature can be publicly verified against the original, unblinded message in the manner of a regular digital signature. Blind signatures are typically employed in privacy-related protocols where the signer and message author are different parties. Examples include cryptographic election systems and digital cash schemes.

An often-used analogy to the cryptographic blind signature is the physical act of enclosing a ballot in a special carbon paper lined envelope. The ballot can be marked through the envelope by the carbon paper. It is then sealed by the voter and handed to an official who signs the envelope. Once signed, the package can be given back to the voter, who transfers the now signed ballot to a new unmarked normal envelope. Thus, the signer does not view the message content, but a third party can later verify the signature and know that the signature is valid within the limitations of the underlying signature scheme.

Blind signatures can also be used to provide unlinkability, which prevents the signer from linking the blinded message it signs to a later un-blinded version that it may be called upon to verify. In this case, the signer's response is first "un-blinded" prior to verification in such a way that the signature remains valid for the un-blinded message. This can be useful in schemes where anonymity is required.

Blind signature schemes can be implemented using a number of common public key instance RSA and DSA. To perform such a signature, the message is first "blinded", typically by combining it in some way with a random "blinding factor". The blinded message is passed to a signer, who then signs it using a standard signing algorithm. The resulting message, along with the blinding factor, can be later verified against the signer's public key. In some blind signature schemes, such as RSA, it is even possible to remove the blinding factor from the signature before it is verified. In these schemes, the final output (message/signature) of the blind signature scheme is identical to that of the normal signing protocol.

IV. Conclusions

A special type revoke scheme, called Secret sharing scheme, this scheme will be efficient, secure, unassisted and also use Hybrid Cryptographic algorithm has been developed for better performance in terms of computation costs and memory storage requirements. We also use Blind signature and AONT technique allow singer to sign without learn the content of the original message.

References

[1] *"Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud" ,Xuefeng Liu and Yuqing Zhang , VOL. 24, NO. 6, JUNE 2013.*

[2] *"Storing Shared Data on the Cloud via Security-Mediator", Boyang Wang and Sherman S.M. Chow, 2013 IEEE 33rd International Conference on Distributed Computing Systems.*

[3] *"Identity-Based Secure Distributed Data Storage Schemes", Jinguang Han.*

[4] *"A Survey of Group Signature Technique, its Applications and Attacks",Aayush Agarwal and Rekha Saraswat, Volume 2, Issue 10, April 2013.*

[5] *"A Survey on Symmetric Key Encryption Algorithms", E. Surya and C.Diviya, Vol 2(4), 475-477.*

[6] *DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems", Kan Yang and Xiaohua Jia.*

[7] *"Efficient revocation in ciphertext-policy attribute-based encryption based cryptographic cloud storage", Zhi-ying WANG and Jun MA, Nov. 6, 2012; Crosschecked Jan. 11, 2013.*

[8] *"Cryptanalysis of Blind Signature Schemes", Nitu Singh and Sumanjit Das, Volume 71– No.19, June 2013.*

[9] *"Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", VOL. 24, NO. 1, JANUARY 2013.*

[10] *"Public Auditing for Shared Data with Efficient User Revocation in the Cloud", Baochun L and Gene Tsudik.*