IJDCST @Feb-Mar, 2104, Issue- V-2, I-2, SW-16
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Cryptographic Cloud Storage with data sharing and security for Multi access network

[1]M. GeethaYadav [2]Dr.N. Chandra Sekhar Reddy[3]G.Praveen Babu[4]Ms.I.Surya Prabha
[1]M.tech(CSE)Institute of Aeronautical Engineering, HYD-500043,AP,India.
[2]Professor,CSEDeptInstituteofAeronauticalEngineering,HYD-500043,AP,India.
[3]Associate Professor,Dept., of Computer Science & Engineering,School of Information Technology,JNT University Hyderabad, Andhra Pradesh,India.
[4]Assoc.,Professor,CSE Dept.,Institute of Aeronautical Engineering,HYD-500043,AP,India.

ABSTRACT: The major aims of this technique a secure multi-owner information sharing theme. It implies that any user within the cluster will firmly share information with others by the world organization trustworthy cloud. This theme is ready to support dynamic teams. expeditiously, specifically, new granted users will directly rewrite information files uploaded before their participation while not contacting with information house owners. User revocation will be simply achieved through a completely unique revocation list while not change the key. Keys of the remaining users the scale and computation overhead of coding are constant and independent with the amount of revoked users. We have a tendency to gift a secure and privacy-preserving access management to users, that guarantee any member during a cluster to anonymously utilize the cloud resource. Moreover, the real identities of knowledge house owners will be disclosed by the cluster manager once disputes occur. We offer rigorous security analysis, and perform intensive simulations to demonstrate the potency of our theme in terms of storage and computation overhead. Cloud computing provides a cost-effective and economical resolution for sharing cluster resource among cloud users sharing information AN exceedingly in a very multi-owner manner whereas conserving information and identity privacy from an untrusted cloud continues to be a difficult issue, because of the frequent modification of the membership.

Keywords: Privacy, tendency, multi owner, resource, cluster manager, revocation.

INTRODUCTION:

CLOUD computing is recognized as another to traditional data technology attributable to its resource -sharing and low-maintenance characteristics. In cloud computing, the cloud service suppliers (CSPs), like Amazon, area unit ready to deliver numerous services to cloud users with the assistance of powerful datacenters. By migrating the native knowledge management systems into cloud servers, users will fancy high-quality services and save significant investments on their native infrastructures. One of the foremost basic services offered by cloud providers is knowledge storage. Allow us to think about a sensible knowledge application. An organization permits its staffs within the same cluster or department to store and share files within the cloud. By utilizing the cloud, the staffs are often fully discharged from the difficult native knowledge storage and maintenance. However, it additionally poses a major risk to the confidentiality of those hold on files. Specifically, the cloud servers managed by cloud suppliers aren't totally trustworthy by users while the information files hold on within the cloud could also be sensitive and confidential, like business plans. To preserve knowledge privacy, a basic resolution is to write in code knowledge files, and then upload the encrypted knowledge into the cloud [2].Sadly, designing associate degree economical and secure knowledge sharing theme for groups within the cloud isn't a simple task attributable to the subsequent problems. However, the complexities of user participation and revocation in these schemes

are linearly increasing with the number of knowledge house owners and therefore the range of revoked users, respectively. By setting a bunch with one attribute level projected a secure origin theme supported the cipher text-policy attribute-based encoding technique , which permits any member during a cluster to share knowledge with others. However, the problem of user revocation isn't addressed in their theme bestowed a ascendible and fine-grained knowledge access management theme in cloud computing supported the key policy attribute-based encoding (KP-ABE) technique .Sadly, the single owner manner hinders the adoption of their theme into the case, wherever any user is granted to store and share knowledge.Our contributions. To resolve the challenges bestowed above, we have a tendency to propose Anglesey, a secure multi-owner knowledge sharing theme for dynamic teams within the cloud. The main contributions of this paper include:

1. We have a tendency to propose a secure multi-owner knowledge sharing scheme. It implies that any user within the cluster will securely share knowledge with others by the un trusted cloud.

2. Our projected theme is in a position to support dynamic groups with efficiency. Specifically, new granted users can directly rewrite knowledge files uploaded before their participation while not contacting with knowledge house owners. User revocation may be simply achieved through a novel revocation list while not change the key keys of the remaining users. The dimensions and computation overhead of encoding are constant and independent with the amount of revoked users.

3. We offer secure and privacy-preserving access control to users, that guarantees any member during a group to anonymously utilize the cloud resource. Moreover, the important identities of knowledge house owners may be revealed by the cluster manager once disputes occur.

4. We offer rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our theme in terms of storage and computation overhead. The remainder of this paper is organized as follows:

Section two overviews the connected work. In Section three, some preliminaries and scientific discipline primitives are reviewed. In Section 4, we have a tendency to describe the system model and our style goals. In Section five, the projected theme is bestowed in detail, followed by the protection analysis and therefore the performance analysis in Sections six and seven. Finally, we have a tendency to conclude the paper in Section eight.

LITERATURE SURVEY:

Achieving Secure, Scalable, and Fine-grained DataAccess Control in Cloud Computing

This paper addresses this challenging openissue by, on one hand, defining and enforcing access policies basedon data attributes, and, on the other hand, allowing the dataowner to delegate most of the computation tasks involved in finegraineddata access control to untrusted cloud servers withoutdisclosing the underlying data contents. We achieve this goal byexploiting and uniquely combining techniques of attribute-basedencryption (ABE), proxy re-encryption, and lazy re-encryption.Our proposed scheme also has salient properties of user accessprivilege confidentiality and user secret key accountability.

Plutus: Scalable secure file sharing on untrusted storage

This paper has introduced novel uses of cryptographicprimitives applied to the problem of secure storage inthe presence of untrusted servers and a desire for ownermanagedkey distribution.

Eliminating almost all requirementsfor server trust (we still require servers not to destroydata – although we can detect if they do) and keepingkey distribution (and therefore access control) in thehands of individual data owners provides a basis for a securestorage system that can protect and share data at verylarge scales and across trust boundaries.

3) SiRiUS: Securing Remote Untrusted Storage

This paper presents SiRiUS, a secure file system designed to be layered over insecure networkand P2P file systems such as NFS, CIFS, OceanStore, and Yahoo! Briefcase. SiRiUS assumesthe network storage is untrusted and provides its own read-write cryptographic access controlfor file level sharing. Key management and revocation is simple with minimal out-of-bandcommunication. File system freshness guarantees are supported by SiRiUS using hash tree constructions.SiRiUS contains a novel method of performing file random access in a cryptographicfile system without the use of a block server.

4) **Secure Provenance: The Essential of Bread and Butter ofData Forensics in Cloud Computing**

In this paper proposed scheme is characterized by providingthe information confidentiality on sensitive documentsstored in cloud, anonymous authentication on user access,
and provenance tracking on disputed documents. With theprovable security techniques, we formally demonstrate theproposed scheme is secure in the standard model.

Ciphertext-Policy Attribute-Based Encryption:An Expressive, E_cient, and Provably Secure Realization

This Paper present a new methodology for realizing Ciphertext-Policy Attribute Encryption (CP-ABE) under concrete and noninteractive cryptographic assumptions in the standard model.Our solutions allow any encryptor to specify access control in terms of any access formula overthe attributes in the system. In our most client system, ciphertext size, encryption, anddecryption time scales linearly with the complexity of the access formula. The only previouswork to achieve these parameters was limited to a proof in the generic group model.

Attribute-Based Encryption forFine-Grained Access Control of Encrypted Data

This Paper presents more sensitive data is shared and stored by third-party sites on the Internet, therewill be a need to encrypt data stored at these sites. One drawback of encrypting data,is that it can be selectively shared only at a coarse-grained level (i.e., giving anotherparty your private key). We develop a new cryptosystem for ¯ne-grained sharing ofencrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). Inour cryptosystem, ciphertexts are labeled with sets of attributes and private keys areassociated with access structures that control which ciphertexts a user is able to decrypt.We demonstrate the applicability of our construction to sharing of audit-log informationand broadcast encryption.

Revocation and Tracing Schemes for StatelessReceivers ?

This paper provides a general traitor tracing mechanism that can be integrated withany Subset-Cover revocation scheme that satisfies a \bifurcation property". This mechanism does not need an a priori bound on the numberof traitors and does not expand the message length by much comparedto the revocation of the same set of traitors.

EXISTING SYSTEM:

Several security schemes for data sharing on untrusted servers have been proposed. In these approaches, data owners store the encrypted data

files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively. By setting a group with a single attribute, Lu et al. proposed a secure provenance scheme based on the cipher text-policy attribute-based encryption technique, which allows any member in a group to share data with others. However, the issue of user revocation is notaddressed in their scheme presented a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique. Unfortunately, the single owner manner hinders the adoption of their scheme into the case where any user is granted to store and share data.

DISADVANTAGES OF EXISTING SYSTEM

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 system 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.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 is more flexible in practical applications.

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.

PROPOSED SYSTEM:

This paper, we propose a secure multi owner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.

ADVANTAGES

We propose a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud.

We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource.

CONCLUSION:

In this paper, we design a secure data sharing scheme, Mona, for dynamic groups in an untrusted cloud. In Mona, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, Mona 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. Proposed a cryptographic storage system that enables secure file sharing on un trusted servers,

named Plutus. By dividing files into file groups and encrypting each file group with a unique file-block key, the data owner can share the file groups with others through delivering the corresponding lockbox key, where the lockbox key is used to encrypt the file-block keys. However, it brings about a heavy key distribution overhead for large-scale file sharing. Additionally, the file-block key needs to be updated and distributed again for a user revocation.

REFERENCES:

[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 ofCloudComputing," 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 Untrusted Storage," 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: AnExpressive, Efficient, and Provably Secure Realization," Proc. Int'lConf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted
Data," Proc. ACM Conf. Computer and Comm. Security (CCS),pp. 89-98, 2006.

[10] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and TracingSchemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf.Advances in Cryptology (CRYPTO), pp. 41-62, 2001.