Avoiding Collusion Problem and Provide Secure Data Transfer for Dynamic Group

K. Saravanan[1] Dr. K. Thangadurai[2]
[1]Assistant Professor [2]Head
[2]Department of Computer Science
[1]Thiruvalluvar University College of Arts and science, Tirupattur-635901, Tamil Nadu, India
[2]Government Arts College, Karur-639005. Tamil Nadu, India

Abstract— A cloud computing is one of the upgrading technology, it provide the data access mechanism through cloud provider. User can accomplish a useful and economical advance for information sharing between group members in the cloud with the benefits of low maintenance cost. In the meantime, we must offer security assurance for the sharing information files because they are outsourced. Regrettably, because of the regular change of the membership, sharing information while offering privacy-preserving is still a difficult issue, particularly for an un-trusted cloud due to the collusion harass. Moreover, many schemes were proposed, the security of key allocation is based on the protected communication conduit, however, to have such conduit is a strong assumption and is tricky for practice. In this paper we provide various approaches for the dynamic transfer of data in the cloud.

Key words: Cloud Computing, Data Transfer, Dynamic Groups and Security

I. Introduction

Cloud computing has become increasingly popular because it offers users the illusion of having infinite computing resources, of which they can use as much as they need, without having to worry about how those resources are provided. It also provides greater scalability, availability, and reliability than users could achieve with their own resources. Cloud Computing, with the characteristics of natural information sharing and low support, gives a superior usage of resources. In Cloud Computing, cloud administration suppliers offer a reflection of boundless storage room for customers to host information. It can offer customers some support with reducing their money related overhead of information administrations by moving the nearby administrations framework into cloud servers. However, security concerns turn into the principle control as we now outsource the capacity of information, which is perhaps delicate, to cloud suppliers. To safeguard information security, a typical methodology is to encode information records before the customers transfer the scrambled information into the cloud [1, 2]. Unfortunately, it is hard to outline a protected and productive information sharing plan, particularly for element groups in the cloud.

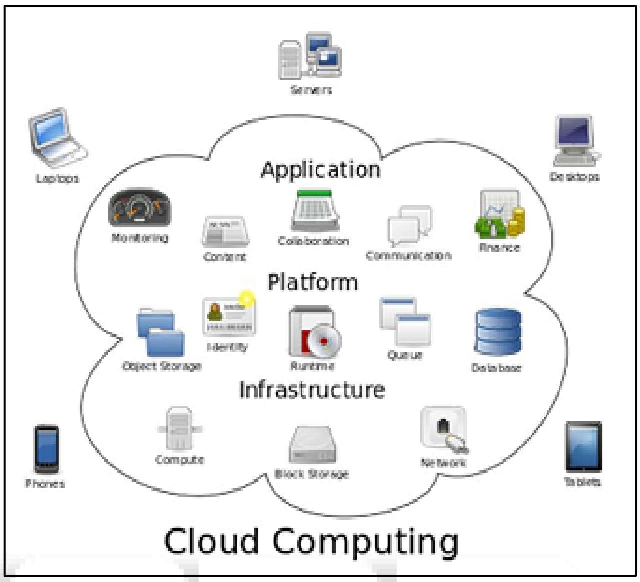

Fig. 1: Cloud architecture

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. The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them [3]. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing. In cloud providing security, guarantees for the sharing data file. Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Unfortunately, because of the frequent change of the membership, sharing data while providing privacy-preserving is still a challenging issue, especially for an untrusted cloud due to the collusion attack. The techniques of key policy attribute-based encryption, proxy re-encryption and lazy re-encryption to achieve fine-grained data access control without disclosing data contents. However, the single-owner manner may hinder the implementation of applications, where any member in the group can use the cloud service to store and share data files with others [4]. However, the scheme will easily suffer from the collusion attack by the revoked user and the cloud. The revoked user can use his private key to decrypt the encrypted data file and get the secret data after his revocation by conspiring with the cloud. As one of the primitive services, cloud storage allows data owners to outsource their data to cloud for its appealing benefits. However, the fact that owners no longer have physical possession of the outsourced data raises big security concerns on the storage correctness. Hence, enabling secure storage auditing in the cloud environment with new approaches becomes imperative and challenging [5]. Several mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. However, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential information-identity privacy-to public verifiers.

II. Literature review

A. Ryan K L Ko et.al [6]

Studied the problems and challenges of the trusted cloud, where the unauthorized user can access the entire data without disturbing the actual user. An unauthorized person may do the two things which is accessing the data and putting duplicate data because cloud storage provides a geographical database. It is not a trusted one to store the data of the users. For this problem Ryan K L Ko et al proposed a TrustCloud framework, to achieve a trusted cloud to the user, to provide a service by making use of detective controls in cloud environment. Detecting process has the accountability access with the cloud. Here user is a responsible person for their data, hence user must tell the accountability with the technical and policy based services. By providing the accountability through user it may solve the problem from the untrusted one. Hence this approach provides privacy, security, accountability and auditability.

B. Muhammad Rizwan Asghar et.al [7]

Discusses the problems of enforcing security policies in cloud environment. With the high growth of data in cloud they were problem arises due untrused person access of the data. To ensure the security is immature, they didn't ensure for the safe data in cloud environments. Security problem is a great issue; here we enforce the security for the owner's data. Providing high security they may high expensive for the users. For the above mentioned problem Muhammad Rizwan Asghar et.al proposed an ESPOON policy which is Encrypted Security Policies for OutsOurced eNvironments. This policy is used to address the above problem and give better confidentiality to the users. It provides a better security by separating the security policy and the enforcement mechanism. Here M R Asghar uses an encrypted scheme to protect the user's data. This is used to protect confidentiality policies based on user's policy. This method has two main scheme, which is policy deployment and policy evaluation scheme. Policy deployment is used to exploit the user's guidelines and the policy evaluation is used to estimate the user guidelines. By using this method user can safe their data.

C. L Ferretti et al [8]

Studied the problem of data leakage of the legitimate user in cloud environment by the cloud provider; they didn't give better security to the user for their personal data or internal data. Main problem arise because of no encrypted data were found, and also it provide the security for the frond-end database only and not controlled the backend database, so the malicious attackers may gain the data access to the outsourced data.

D. S. Kent and R. Atkinson [9]

We believe the security issues related to the proposed MoRaRo can be resolved with the security mechanisms available for the MIPv6 protocol and its derivatives such as the NEMO basic support protocol and Hierarchical MIPv6 (HMIPv6) protocol. As both the MR and it's HA belong to the same administrative domain, they use their pre-established security association (SA). The MNN and MR exchange their mutually trusted identities to establish the SA. A trusted identity can be an IP address or a certificate signed by a Certificate Authority (CA) that both the MR and MNN trust. Similarly, the MNN and CN are mutually trusted through the return routability test. Furthermore, as in MIPv6, all signaling messages exchanged among the MNN, MR, HA and CN are authenticated by IPSec. Performing route optimization reveals the location of the MNN to the CN. The location information is considered as personal information, the revealing of which may create a privacy exposure problem. However, the MNN can use privacy rules to protect its location information against possible misuse. The privacy rules regulate the CN's activities regarding the collection, use, disclosure, and retention of location information of the MNN. In our MoRaRo scheme, the MNN can perform privacy negotiation with the CN by using the privacy protection frameworks being developed.

E. Ankita Ajay Jadhav [10]

Data sharing among cluster members within the cloud with the characters of low maintenance and tiny management price. Meanwhile, we tend to offer security guarantees for the sharing information files since they're outsourced. To owing the frequent amendment of the membership, sharing information whereas providing privacypreserving continues to be a difficult issue, particularly for an untrusted cloud owing to the collusion attack. Moreover, for existing schemes, the safety of key distribution is predicated on the secure channel, however, to own such channel may be a sturdy assumption and is troublesome for apply. We tend to propose a secure information sharing theme for dynamic members. First, we tend to propose a secure manner for key distribution with none secure communication channels, and therefore the users will firmly obtain their non-public keys from cluster manager. Secondly, we can do fine-grained access management; any user within the group of members will use the supply within the cloud and revoked users not able to access the cloud once more once they're revoked. Third, we are able to shield the theme from collusion attack, which suggests that revoked users cannot get the initial record though they conspire with the untrusted cloud. In our approach, by investing polynomial perform; we are able to attain a secure user revocation theme. Finally, we can provide the non-public key for security where the user needn't update, hence no need for a replacement of user joins within the cluster or a user is revoked from the cluster.

F. G. Mercy Vimala [11]

The Benefited from Cloud Computing, clients can achieve a flourishing and moderate methodology for information sharing among gathering individuals in the cloud with the characters of low upkeep and little administration cost. Then, security certifications to the sharing information records will be given since they are outsourced. Horribly, due to the never-ending change of the enrolment, sharing information while giving protection saving is still a testing issue, particularly for an untrusted cloud because of the agreement attack. In addition, for existing plans, the security of key dispersion depends on the safe communication channel, then again, to have such channel is a solid feeling and is difficult for practice. In this paper, we propose a safe information sharing plan for element individuals. Firstly, we propose a safe route for key dispersion with no safe correspondence channels, and the clients can safely acquire their private keys from gathering administrator. Besides, the plan can accomplish fine-grained access control, any client in the gathering can utilize the source in the cloud and refused clients can't get to the cloud again after they are rejected. Thirdly, we can protect the plan from trickery attack, which implies that rejected clients can't get the first information record regardless of the possibility that they scheme with the untrusted cloud. In this methodology, by utilizing polynomial capacity, we can achieve a protected client denial plan. At long last, our plan can bring about fine productivity, which implies past clients need not to overhaul their private keys for the circumstance either another client joins in the gathering or a client is given up from the gathering.

III. PRIVACY PRESERVING FOR SECURE DATA TRANSFER

A. Privacy-Preserving Public Auditing For Shared Data in the Cloud

With cloud data services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. Unfortunately, the integrity of cloud data is subject to scepticism due to the existence of hardware/software failures and human errors. Several mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. However, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential information-identity privacy-to public verifiers. In this paper, we propose a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. In particular, we exploit ring signatures to compute verification metadata needed to audit the correctness of shared data [12]. With our mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. In addition, our mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one. Our experimental results demonstrate the effectiveness and efficiency of our mechanism when auditing shared data integrity.

B. Security Challenges for the Public Cloud

In this talk, I will first discuss a number of pressing security challenges in Cloud Computing, including data service outsourcing security and secure computation outsourcing. Then, I will focus on data storage security in Cloud Computing. As one of the primitive services, cloud storage allows data owners to outsource their data to cloud for its appealing benefits [13]. However, the fact that owners no longer have physical possession of the outsourced data raises big security concerns on the storage correctness. Hence, enabling secure storage auditing in the cloud environment with new approaches becomes imperative and challenging.

C. Privacy-Preserving Public Auditing For Data Storage Security in Cloud Computing

Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public audit ability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we utilize and uniquely combine the public key based homomorphism authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements [14]. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

D. Computing Encrypted Cloud Data Efficiently Under Multiple Keys

The emergence of cloud computing brings users abundant opportunities to utilize the power of cloud to perform computation on data contributed by multiple users. These cloud data should be encrypted under multiple keys due to privacy concerns. However, existing secure computation techniques are either limited to single key or still far from practical. In this paper, we design two efficient schemes for secure outsourced computation over cloud data encrypted under multiple keys [15]. Our schemes employ two non-colluding cloud servers to jointly compute polynomial functions over multiple users' encrypted cloud data without learning the inputs, intermediate or final results, and require only minimal interactions between the two cloud servers but not the users. We demonstrate our schemes' efficiency experimentally via applications in machine learning. Our schemes are also applicable to privacy-preserving data aggregation such as in smart metering.

1) Key Distribution

The prerequisite of key transportation is that clients can safely get their private keys from the gathering director with no Certificate Authorities. In other existing plans, this purpose is skilful by expecting that the communication channel is secure, on the other hand, in our plan, we can accomplish it without this solid thought.

2) Access control

First, collect individuals can make use of the cloud asset for information stockpiling and information sharing. Second, unapproved clients can't get to the cloud asset whenever, and disavowed clients will be unfitted for utilizing the cloud asset again once they are renounced.

3) Information classification

Data secrecy requires that unapproved clients including the cloud are unequipped for taking in the substance of the put away information. To keep up the accessibility of information secrecy for element gatherings is still an essential and testing issue. In particular, renounced clients can't unscramble the put away information document after the denial.

4) Effectiveness

Any gathering part can store and impart information records to others in the gathering by the cloud. Client repudiation can be accomplished without including the others, which implies that the remaining clients don't have to overhaul their private keys.

E. Secure Multi-Owner Data Sharing For Dynamic Groups in the Cloud

With the character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. In 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 [16]. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiment

F. Scalable Secure File Sharing On Un-Trusted Storage

Which uses a lockbox to protect only the keys. Mechanisms that use to provide basic file system security features-(1) To detect and prevent unauthorized data modifications, (2) To differentiate between read and write access to files, and (3) To change user's access privileges. In encrypt-on-disk file systems, the clients encrypt all directories and their contents. When used a single key to encrypt an entire directory of files. Scalable secure file sharing on un-trusted storage introduces a new secure file system which strives to provide strong security even with an un-trusted server. The main feature is that all data is stored encrypted and all key distribution is handled in a decentralized manner. All cryptographic and key management operations are performed by the clients, and the server incurs very little cryptographic overhead.

IV. Cloud Computing Benefits

A. Achieve Economies of Scale

Increase volume output or productivity with fewer people. Your cost per unit, project or product plummets.

B. Reduce Spending On Technology Infrastructure

Maintain easy access to your information with minimal upfront spending. Pay as you go (weekly, quarterly or yearly), based on demand.

C. Globalize Your Workforce on the Cheap

People worldwide can access the cloud, provided they have an Internet connection.

D. Streamline Processes

Get more work done in less time with less people.

E. Reduce Capital Costs

There's no need to spend big money on hardware, software or licensing fees.

F. Improve Accessibility

You have access anytime, anywhere, making your life so much easier!

G. Efficiency

Any group member can store and share data files with others in the group by the cloud. User revocation can be achieved without involving the others, which means that the remaining users do not need to update their private keys.

V. Conclusion

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared business infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing. In cloud providing security, guarantees for the sharing data file. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. This paper provides the various approaches and their uses. It will provide a better idea to make a different task to the users

REFERENCES

[1] Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg , Qianhui Liang , Bu Sung Lee, "TrustCloud: A Framework for Accountability and Trust in Cloud Computing" 2011 IEEE World Congress on Services.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. "A View of Cloud omputing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr.2010.

[3] 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.

[4] LAN Zhou, Vijay Varadharajan, and Michael Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage," IEEE Transactions on Information Forensics and Security.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.

[6] Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg , Qianhui Liang , Bu Sung Lee, "TrustCloud: A Framework for Accountability and Trust in Cloud Computing" 2011 IEEE World Congress on Services.

[7] Muhammad Rizwan Asghar, Mihaela Ion, Bruno Crispo, "ESPOON Enforcing Encrypted Security Policies in Outsourced Environment", 2011 Sixth International Conference on Availability, Reliability and Security.

[8] Luca Ferretti, Michele Colajanni, and Mirco Marchetti, "Access control enforcement on query-aware encrypted cloud databases" IEEE 2013.

[9] S. Kent and R. Atkinson, "Security architecture for the Internet protocol," IETF RFC 2401, November 1998.

[10] Ankita Ajay Jadhav, "Anti Collusion Data Sharing Schema for Centralized Group in Cloud"

[11] G.Mercy Vimala, "A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud"

[12] B. Sheng and Q. Li, "Verifiable Privacy-Preserving Range Query in Two-Tiered Sensor Networks," Proc. IEEE INFOCOM, pp. 4650, 2008.

[13] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: The essential of bread and butter of data forensics in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.

[14] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. Netw. Distrib. Syst. Security Symp., 2005, pp. 29–43.

[15] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ci-phertexts or Decryption Keys," Proc. First Int'l Conf. Pairing-Based Cryptography, pp. 39-59,2007

[16] Zhongma Zhu, Zemin Jiang, Rui Jiang, "The Attack on Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," Proceedings of 2013 International Conference on Information Science and Cloud Computing (ISCC 2013), Guangzhou, Dec.7, 2013, pp. 185-189.