International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 5 Issue 3, March-2016

Multi Owner Data Sharing With Security and Load Balancing in Cloud

P. Shyamala[1], Mr. C. Nandhakumar[2]

[1]PG Scholar, Department of Computer Science, PPG Institute of Technology, Coimbatore, India,
[2]Assistant Professor (CSE), Department of Computer Science, PPG Institute of Technology, Coimbatore, India

ABSTRACT

Cloud computing, also known as on-demand computing is a kind of internet-based computing, where shared resources and information are provided to computers and other devices on-demand. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their sensitive data in third-party data centers. To keep the shared data confidential in an un-trusted cloud service provider a natural way is to store the encrypted data. The key problems of this approach include establishing access control for the encrypted data, and revoking the access rights from users when they are no longer authorized to access the encrypted data. Problem of sharing data in a multi-owner cloud group is a challenging issue, due to the frequent change of the membership. A secure multi-owner data sharing scheme is proposed that any user in the group can securely share data with others by the un-trusted cloud. To support dynamic group's efficiently new granted users can directly use data files uploaded without contacting data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users and its guarantees any member in a group to utilize the cloud resource from a load balanced server.

Keywords: Cloud computing, Data owners, Security, Authentication, Overloaded partition, Priority queue.

I. INTRODUCTION

Cloud computing, also on-demand computing, is a kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers. Users are at the mercy of their cloud service providers (CSP) for the availability and integrity of their data. Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Though the benefits are clear, such a service is also relinquishing users' physical possession of their outsourced data, which inevitably poses new security risks toward the correctness of the data in cloud.

1.1 Cloud Storage

Cloud storage is a model of networked enterprise storage where data is stored in virtualized pools of storage which are generally hosted by third parties. Hosting companies operate large data centres, and people who require their data to be hosted buy or lease storage capacity from them. The data centre operators, in the background, virtualized the resources according to the requirements of the customers and expose them as storage pools, which the customers can themselves use to store files or data objects. Physically, the resource may span across multiple servers and multiple servers and multiple locations. The safety of the files depends upon the hosting companies, and on the applications that leverage the cloud storage. Cloud storage services may be accessed through a web service application programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a cloud storage gateway or Web-based content management systems.

1.2 Attribute Authority

That is, the enterprise can revoke data access rights from users once they are no longer its employees. A user whose permission is revoked will still retain the keys issued earlier, and thus can still decrypt data in the cloud. The traditional

revocation scheme usually requires the AAs to periodically re-encrypt data, and re-generate new secret keys to remaining authorized users. s. A more scalable approach is to take advantage of the abundant resources in a cloud by allowing the AAs to delegate the CSP to re-encrypt data and re-generate keys to users, under the environment that the CSP knows nothing about the data and keys.

II. RELATED WORK

Identity privacy is one of the most significant obstacles for the wide deployment of cloud computing [1]. 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. 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 [8]. The single-owner manner where only the group manager can store and modify data in the cloud, the multiple-owner manner is more flexible in practical applications groups are normally dynamic in practice [6].

The changes of membership make secure data sharing extremely difficult. Several security schemes for data sharing on un trusted servers have been proposed in these approaches, data owners store the encrypted data files in un trusted storage and distribute the corresponding decryption keys only to authorized users [13]. 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. A scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique. Unluckily, the single owner manner hinders the adoption of their scheme into the case, where any user is granted to store and share data [15].

III. PROBLEM DEFINITION

A secure multi-owner data sharing scheme for dynamic groups in the cloud it implies that any user in the group can securely share data with others by the untrusted cloud. The 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.

Secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource.. In every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. In practice, attributes belong to different authorities can be identified by encoding the attributes with different prefix. In this approach Every AA has full control over the structures and semantics of its attributes, and maintains a state and a revocation list for each attribute in its domain. Each AA is responsible for issuing secret keys to users when they are entitled attributes in its domain and publishing update keys for each attribute in its domain at each time slot to reflect the users' possessions of the attribute at the time slot.

Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the "software as a service" (SaaS) computing architecture, are transforming data centres into pools of computing service on a huge scale. Meanwhile, the increasing network bandwidth and reliable yet flexible network connections make it even possible that clients can now subscribe high-quality services from data and software that reside solely on remote data centres.

Although envisioned as a promising service platform for the Internet, this new data storage paradigm in "Cloud" brings about many challenging design issues which have profound influence on the security and performance of the overall system. One of the biggest concerns with cloud data storage is that of data integrity verification at untrusted servers. For example, the storage service provider, which experiences Byzantine failures occasionally, may decide to hide the data errors from the clients for the benefit of their own. What is more serious is that for saving money and storage space the service provider might neglect to keep or deliberately delete rarely accessed data files which belong to an ordinary client. Consider the large size of the outsourced electronic data and the client's constrained resource capability, the core of the problem can be generalized as how can the client find an efficient way to perform periodical integrity verifications without the local copy of data files.

In order to solve the problem of data integrity checking, many schemes are proposed under different systems and security models. In all these works, great efforts are made to design solutions that meet various requirements: high scheme efficiency, stateless verification, unbounded use of queries and irretrievability of data, etc. Considering the role of the

verifier in the model, all the schemes presented before fall into two categories: private audit ability and public audit ability. Although schemes with private audit ability can achieve higher scheme efficiency, public audit ability allows any one, not just the client (data owner), to challenge the cloud server for correctness of data storage while keeping no private information. Then, clients are able to delegate the evaluation of the service performance to an independent third party auditor (TPA), without devotion of their computation resources. In the cloud, the clients themselves are unreliable or may not be able to afford the overhead of performing frequent integrity checks. Thus, for practical use, it seems more rational to equip the verification protocol with public audit ability, which is expected to play a more important role in achieving economies of scale for Cloud Computing. Moreover, for efficiency consideration, the outsourced data themselves should not be required by the verifier for the verification purpose.

IV. ULTI OWNER ARCHITECTURE

A secure multi-owner data sharing scheme for dynamic groups in the cloud it implies that any user in the group can securely share data with others by the un trusted cloud. The 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.

Secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource.. In every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. In practice, attributes belong to different authorities can be identified by encoding the attributes with different prefix. In this approach Every AA has full control over the structures and semantics of its attributes, and maintains a state and a revocation list for each attribute in its domain. Each AA is responsible for issuing secret keys to users when they are entitled attributes in its domain and publishing update keys for each attribute in its domain at each time slot to reflect the users' possessions of the attribute at the time slot.

Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the "software as a service" (SaaS) computing architecture, are transforming data centres into pools of computing service on a huge scale. Meanwhile, the increasing network bandwidth and reliable yet flexible network connections make it even possible that clients can now subscribe high-quality services from data and software that reside solely on remote data centres.

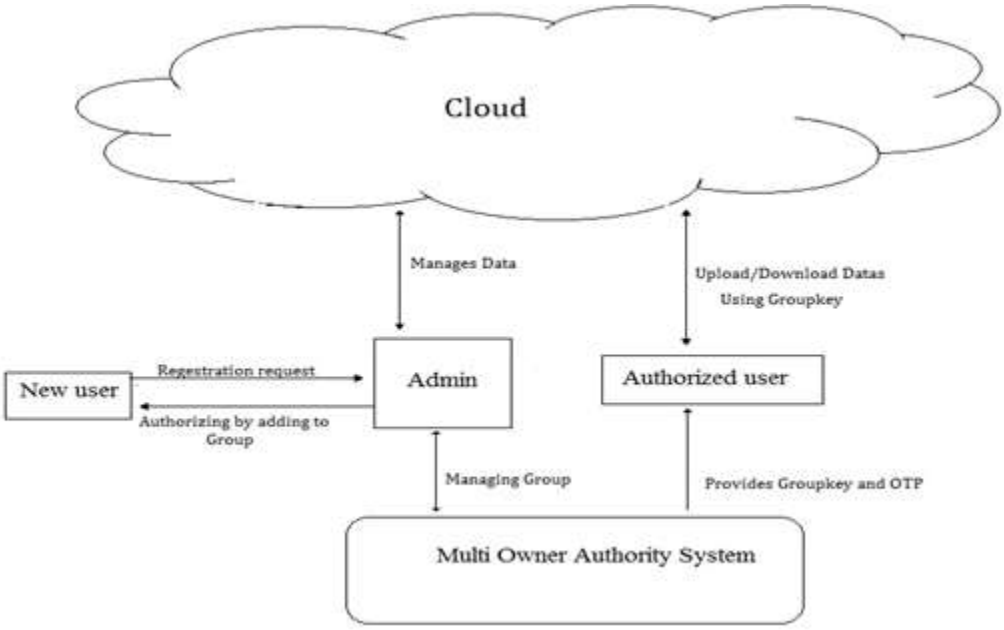

Fig 1 Block Diagram of Multi Owner Authority

Although envisioned as a promising service platform for the Internet, this new data storage paradigm in "Cloud" brings about many challenging design issues which have profound influence on the security and performance of the overall system. One of the biggest concerns with cloud data storage is that of data integrity verification at untrusted servers. For

example, the storage service provider, which experiences Byzantine failures occasionally, may decide to hide the data errors from the clients for the benefit of their own. What is more serious is that for saving money and storage space the service provider might neglect to keep or deliberately delete rarely accessed data files which belong to an ordinary client. Consider the large size of the outsourced electronic data and the client's constrained resource capability, the core of the problem can be generalized as how can the client find an efficient way to perform periodical integrity verifications without the local copy of data files.

In order to solve the problem of data integrity checking, many schemes are proposed under different systems and security models. In all these works, great efforts are made to design solutions that meet various requirements: high scheme efficiency, stateless verification, unbounded use of queries and irretrievability of data, etc. Considering the role of the verifier in the model, all the schemes presented before fall into two categories: private audit ability and public audit ability. Although schemes with private audit ability can achieve higher scheme efficiency, public audit ability allows any one, not just the client (data owner), to challenge the cloud server for correctness of data storage while keeping no private information. Then, clients are able to delegate the evaluation of the service performance to an independent third party auditor (TPA), without devotion of their computation resources.

In the cloud, the clients themselves are unreliable or may not be able to afford the overhead of performing frequent integrity checks. Thus, for practical use, it seems more rational to equip the verification protocol with public audit ability, which is expected to play a more important role in achieving economies of scale for Cloud Computing. Moreover, for efficiency consideration, the outsourced data themselves should not be required by the verifier for the verification purpose.

V. CLOUD LOAD BALANCING

Cloud load balancing is the process of distributing workloads across multiple computing resources. Cloud load balancing reduces costs associated with document management systems and maximizes availability of resources.

Load Balancing with priority queue

According to this design each node maintains two queues, Priority queue and Non priority queue. Priority queue is used when the cloud partition status is idle or normal and Non priority queue is used when partition status is overloaded. When user submit job request job allocation is performed either by load balancing approach or by scheduling algorithm. When a new job arrives, if cloud partition status is idle or normal then load balancing approach is used to select a best node for executing the job. The load balancing approach uses priority queue for all arriving jobs. The jobs assigned to the nodes have the same priority and total CPU power is shared by all the jobs in the queue. When the cloud partition status is overloaded then queue is splitted into two. Then the jobs in idle and normal partition status are moved to Priority queue and the jobs after overloaded status are moved to non-priority queue. A separate scheduling algorithm is used for this allocation to Non priority queue.

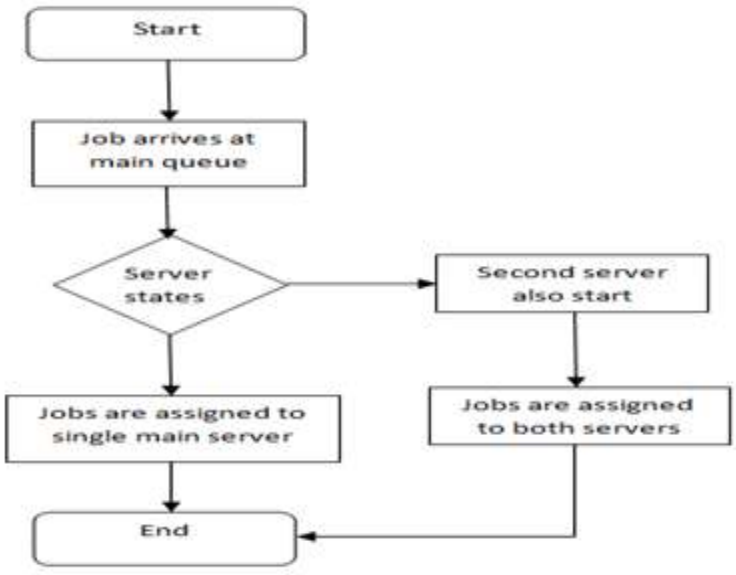

Fig 2 Job assignment strategy for overloaded status

CONCLUSION

In this work a secure multi-owner data sharing scheme is proposed that any user in the group can securely share data with others by the un trusted cloud. To support dynamic group's efficiently new granted users can directly use data files uploaded without contacting the data owners. User revocation can be easily achieved through a novel revocation list with updating the secret keys of the remaining users and its guarantees any member in a group to anonymously utilize the cloud resource. Proposed approach the efficiency of our scheme in terms of storage and computation overhead.

REFERENCES

[1]. Armbrust, Michael, et al. "A view of cloud computing." Communications of the ACM 53.4 (2010): 50-58.
[2]. Kamara, Seny, and Kristin Lauter. "Cryptographic cloud storage." Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2010. 136-149..
[3]. Yu, Shucheng, et al. "Achieving secure, scalable, and fine-grained data access control in cloud computing." INFOCOM, 2010 Proceedings IEEE. IEEE, 2010.
[4]. Kallahalla, Mahesh, et al. "Plutus: Scalable Secure File Sharing on Untrusted Storage." Fast. Vol. 3. 2003.
[5]. Goh, Eu-Jin, et al. "SiRiUS: Securing Remote Untrusted Storage." NDSS. Vol. 3. 2003.
[6]. Ateniese, Giuseppe, et al. "Improved proxy re-encryption schemes with applications to secure distributed storage." ACM Transactions on Information and System Security (TISSEC) 9.1 (2006): 1-30.
[7]. Lu, Rongxing, et al. "Secure provenance: the essential of bread and butter of data forensics in cloud computing." Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. ACM, 2010.
[8]. Waters, Brent. "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization." Public Key Cryptography–PKC 2011. Springer Berlin Heidelberg, 2011. 53-70.
[9]. Goyal, Vipul, et al. "Attribute-based encryption for fine-grained access control of encrypted data." Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006.
[10]. Naor, Dalit, Moni Naor, and Jeff Lotspiech. "Revocation and tracing schemes for stateless receivers." Advances in Cryptology—CRYPTO 2001. Springer Berlin Heidelberg, 2001.
[11]. Boneh, Dan, and Matt Franklin. "Identity-based encryption from the Weil pairing." Advances in Cryptology—CRYPTO 2001. Springer Berlin Heidelberg, 2001.
[12]. Boneh, Dan, Xavier Boyen, and Hovav Shacham. "Short group signatures."Advances in Cryptology–CRYPTO 2004. Springer Berlin Heidelberg, 2004.
[13]. Boneh, Dan, Xavier Boyen, and Eu-Jin Goh. "Hierarchical identity based encryption with constant size ciphertext." Advances in Cryptology–EUROCRYPT 2005. Springer Berlin Heidelberg, 2005. 440-456.
[14]. Delerablée, Cécile, Pascal Paillier, and David Pointcheval. "Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys." Pairing-Based Cryptography–Pairing 2007. Springer Berlin Heidelberg, 2007. 39-59.
[15]. Chaum, D., & Van Heyst, E. (1991, January). Group signatures. In Advances in Cryptology—EUROCRYPT'91 (pp. 257-265). Springer Berlin Heidelberg.