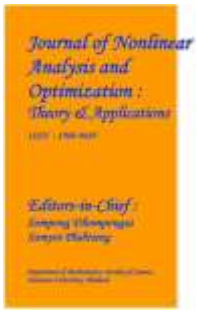
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 14, Issue. 2 : 2023
ISSN : **1906-9685**



SECURED AND RELIABLE ENERGY EFFICIENT SEARCH SCHEME ON MOBILE CLOUD

[1]Dr.V.Venu Gopal, [2] Miriyala.Prasanthi, [3] M.Arjun, [4]Adigoppala Sravanthi
[1]Professor, [2,3]Assistant Professor, [4]Student, Dept. of Computer Science Engineering, Newton's Institute of Engineering, Macherla, Andhra Pradesh, India.

ABSTRACT
Cloud storage provides a convenient, massive, and scalable storage at low cost, but data privacy is a major concern that prevents users from storing files on the cloud trustingly. One way of enhancing privacy from data owner point of view is to encrypt the files before outsourcing them onto the cloud and decrypt the files after downloading them. However, data encryption is a heavy overhead for the mobile devices, and data retrieval process incurs a complicated communication between the data user and cloud. Normally with limited bandwidth capacity and limited battery life, these issues introduce heavy overhead to computing and communication as well as a higher power consumption for mobile device users, which makes the encrypted search over mobile cloud very challenging. In this paper, we propose TEES (Traffic and Energy saving Encrypted Search), a bandwidth and energy efficient encrypted search architecture over mobile cloud. The proposed architecture offloads the computation from mobile devices to the cloud, and we further optimize the communication between the mobile clients and the cloud. It is demonstrated that the data privacy does not degrade when the performance enhancement methods are applied. Our experiments show that TEES reduces the computation time by 23% to 46%and save the energy consumption by 35% to 55% per file retrieval, meanwhile the network traffics during the file retrievals are also significantly reduced.

Key Words: Public cloud, Private cloud, Hybrid cloud, Scalable storage

1. INTRODUCTION

Cloud computing greatly facilitates data providers who want to outsource their data to the cloud without disclosing their sensitive data to external parties and would like users with certain credentials to be able to access the data. This requires data to be stored in encrypted forms with access control policies such that no one except users with attributes (or credentials) of specific forms can decrypt the encrypted data.

An encryption technique that meets this requirement is called attribute-based encryption(ABE) , where a user's private key is associated with an attribute set, a message is encrypted under an access policy(or access structure) over a set of attributes, and a user can decrypt a ciphertext with his/her private key if his/her set of attributes satisfies the access policy associated with this ciphertext.

However, the standard ABE system fails to achieve secure deduplication , which is a technique to save storage space and network bandwidth by eliminating redundant copies of the encrypted data stored in the cloud. On the other hand, to the best of our knowledge, existing constructions for secure deduplication are not built on attribute-based encryption.

Nevertheless, since ABE and secure deduplication have been widely applied in cloud computing, it would be desirable to design a cloud storage system possessing both properties.

http://doi.org/10.36893/JNAO.2023.V14I2.305-311

We consider the following scenario in the design of an attribute-based storage system supporting secure deduplication of encrypted data in the cloud, in which the cloud will not store a file more than once even though it may receive multiple copies of the same file encrypted under different access policies.A data provider, Bob, intends to upload a file M to the cloud, and share M with users having certain credentials. In order to do so, Bob encrypts M under an access policy A over a set of attributes, and uploads the corresponding ciphertext to the cloud, such that only users whose sets of attributes satisfying the access policy can decrypt the ciphertext. Later, another data provider, Alice, uploads a ciphertext for the same underlying file M but ascribed to a different access policy A0. Since the file is uploaded in an encrypted form, the cloud is not able to discern that the plaintext corresponding to Alice's ciphertext is the same as that corresponding to Bob's, and will store M twice. Obviously, such duplicated storage wastes storage space and communication bandwidth. hosted on the internet to store, manage and process data rather than a local server or a personal computer. Cloud provides the space to store the data i.e. the user can store his data in the cloud service.

There are different types of clouds where the data can be store.

Public cloud: The data in the public cloud can be accessible by any person.

Private cloud: The data in a private cloud be accessible by a group of people.

Hybrid cloud: It is the combination of both public and the private cloud**.**

Community cloud: A group of similar organisations can access the data in this type of cloud.

Services Models

Cloud Computing comprises three different service models.Those are

Software As a service: SAAS is a software distribution model in which applications are hosted by vendor or service provider and made available to customers over a network, typically the internet.

Platform as a service: PAAS refers to the delivery of operating system and associate services over the internet without downloads or the installation.

Infrastructure as a service: IAAS involved outsourcing the equipment used to support operations, including storage, hardware, servers all of which are made accessible over a network.

Although cloud computing brings great convenience to enterprises and users, the cloud computing security has always been a major hazard.

Cloud Storage

Cloud storage provides

Convenient

Massive and

Scalable storage at low cost

The major concern is privacy that prevents users from storing files on the cloud trustingly. one way to enhance the privacy from data owner point of view is to encrypt the files before outsourcing them on to the cloud and decrypt the files other downloading them. Cloud storage system is a service model in which data are maintained, managed and backup remotely on the cloud side and mean while data keeps available to the users over a network.

However, data encryption is a heavy overhead for the mobile devices and data retrieval process incurs a complicated communication between the data user and cloud. Normally with limited bandwidth capacity and limited battery life, these issues introduce heavy overhead to computing and communication as well as higher power consumption for mobile device users, which makes the encrypted search over mobile cloud very challenging.

Mobile cloud storage(MCS), denotes a family of increasingly popular on-line services and even acts as the primary file storage for the mobile devices.MCS enables the mobile device users to store and retrieve files or data on the cloud through wireless communication, which improves the data availability and facilities the file sharing process without draining the local mobile device resource.

The data privacy issue is in cloud storage system, so the sensitive data is encrypted by the owner before outsourcing onto the cloud and data users retrieve the interested data by encrypted search scheme. In MCS, the modern mobile devices are conformed with many of the same security threats as pc's and various traditional data encryption methods are imported in MCS.However, mobile cloud storage system incurs new challenges over the traditional encrypted search schemes, in consideration of the limited computing and battery capacities of mobile device, as well as data sharing and accessing approaches through wireless communication. Therefore, a suitable and efficient encrypted search scheme is necessary for MCS.

Generally speaking, the mobile cloud storage is in great need of the bandwidth and energy efficiency for data encrypted search scheme, due to the limited battery life and payable Traffic fee.Therefore,we focus on the design of a mobile cloud scheme that is efficient in terms of both energy consumption and the network traffic, while keep meeting the data security requirements through wireless communication channels. Storage services based on public clouds such as Microsoft's Azure storage service and Amazon's S3 provide customers with scalable a dynamic storage. By moving their data to the cloud customers can avoid the costs of building and maintaining a private storage infrastructure.

For most customers, this provides several benefits including availability(i.e., being able to access data from anywhere) and reliability(i.e., not having to worry about backups)at a relatively low cost. The cloud storage own advantages in pay for use and elastic scalability. However, the data security risk destroys the trust relation between the cloud service provider and user. A direct method to avoid this problem is to encrypt data before data stored in the cloud.

Thus, without the decryption key, the leakage data cannot be decrypted. While the encryption technology is good, it is not always suitable for the mobile user. When using the mobile device, such as smart phone, to access the data that stored in cloud storage system, the performance issue should be considered, because the encryption scheme involves high workload.

File Retrieval in Cloud Storage

Traditional encrypted search over cloud data

Traditional encrypted search over cloud data include

Fie/Index encryption

Data search and Retrieval after authentication

File/Index encryption:

The data owner first executes the preprocessing and indexing work.

Data Search and Retrieval after Authentication:

A data user can only access a file after being authenticated by the data owner.

In the process of authentication, the data user sends his identity to the data owner.

The data owner sends the encrypted keys back if the user is a legal user.

http://doi.org/10.36893/JNAO.2023.V14I2.305-311

In the process of search and retrieval the cloud server helps the users to find the top-k relevant files for a given keyword without decrypting it, searches incur following steps:

The authenticated user stems the keyword to be queried, encrypts it with the keys and hashes it to get its entry in the index. Then the encrypted keyword is sent to the cloud server.

On receiving the encrypted keyword, the cloud server first searches for it in the index. Then the index related to this keyword is sent back to the data users.

The data user calculates the relevance scores with the selected index to find the top-k relevant files and sends a follow-up request to the cloud server in order to retrieve the files.

The position of these files is selected and they are sent back to the data users from the cloud server.

The data user decrypts the files and recovers the original data.

Cloud storage services may be accessed through a co-located cloud computer service, a web service Application Programming Interface(API)or by applicants that utilize the API, such as cloud desktop storage gateway or web-based content management systems.

Cloud storage is based on highly virtualized infrastructure and is like broader cloud computing in terms of accessible interface, near-instant elasticity and scalability, multitenancy and metered resources.

Cloud storage services can be utilized from an off-premises service (Amazon S3) or deployed on premises (VION capacity services)

Cloud storage typically returns to a hosted object storage service, but the term has broadened to include other types of data storage that are now available as a service, like block storage.

Object storage services like Amazon S3 and Microsoft Azure storage software like open stack swift.

Object storage systems like EMC Atmos, EMC ECS and Hitachi content platform and distributed storage research projects like Ocean store and VISION Cloud are all examples of storage that can be hosted and deployed with cloud storage characteristics.

Cloud storage is:

Made up of many distributed resources, but still acts as one, either in a federated or a cooperative storage cloud architecture.

Highly fault tolerant through redundancy and distribution of data.

Highly durable through the creation of versioned copies.

Typically, eventually consistent with regard to data replicas.

II. SYSTEM ANALYSIS

In Information Retrieval, TF-IDF (term frequency-inverse document frequency) is a statistic which reflects how important a word is to a document in a collection. It is often used as a weighting factor in keyword-based retrieval and text mining. The TF-IDF algorithm was proposed by Salton and McGill's book is one of the most popular schemes, among other schemes as.

Up to now, encrypted search includes Boolean keyword search and ranked keyword search. In Boolean keyword search the server sends back files only based on the existence or absence of the keywords.

It's not compatible with existing file encryption schemes.

It cannot deal with compressing data and After that many methods of keyword search showed up.

http://doi.org/10.36893/JNAO.2023.V14I2.305-311

In this project, we implement one-to-one mapping OPE which will lead to Statistics Information Leak Control Wang et al. Proposed a one-to-many mapping OPE They implemented a complicate algorithm for security protection.

However, their performance and energy consumption would a problem since their algorithm was complicate and need much computing resource. Proposed a confidentiality preserving rank ordered search. This scheme displays low performances as the relevance scores are computed on the client side, increasing its workload. Proposed a one round trip search scheme which could search the encrypted data. It worth noticing that multi keyword ranked search may incur more serious.

The advantages of the TEES design in terms of relevance score calculation offloading.

Thus, leads to reduction of file search and retrieval process.

III.MPLIMENTATION

PLACEMENT CELL OFFICER

Placement Cell Authority generates the content key and the secret key requested by the end user.Placement Cell Officer is also called Authority.

Authority can view all files with the content key and master secret key generated with the corresponding data owner details of the particular file.

STUDENT

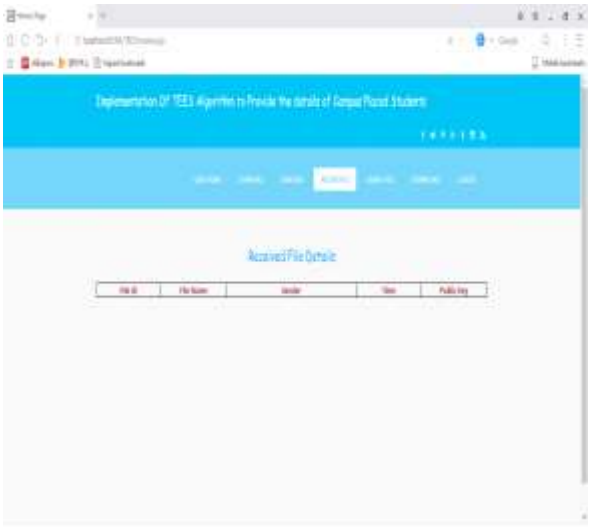
In this module, initially the data student has to register to the cloud server and get authorized . Here student is also called data owner or end user After the authorization from cloud student will encrypt and add file to the cloud server where in after the addition of file student requests the content key and the master secret key to the placementcell for the file they uploaded and finds Find deduplication ,only after the keys generated the file is uploaded to the cloud server. After the uploading of the file the student will have to provide download and the search permission for individual file for the users to perform search and download.User has to register and login for accessing the files in the cloud. User is authorized by the cloud to verify the registration. User has to request for the MSK master secret key and content key to download the file. User can only download and serach the file if the data owner of the particular file has provided the permissions.

CLOUD SERVER

The cloud server manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with cloud End users. To access the shared data files users will request the permission of content key and the MSK master secret key. And the cloud will provide the permission .and also views all the transactions and attackers related to the files.

IV.EXPERIMENTAL RESULTS

http://doi.org/10.36893/JNAO.2023.V14I2.305-311



CONCLUSION

Attribute-based encryption (ABE) has been widely used in cloud computing where data providers outsource their encrypted data to the cloud and can share the data with users possessing specified c redentials. On the other hand, deduplication is an important technique to save the storage space and network bandwidth, which eliminates duplicate copies of identical data.

However, the standard ABE systems do not support secure deduplication, which makes them costly to be applied in some commercial storage services. In this paper, we presented a novel approach to realize an attribute-based storage system supporting secure deduplication. Our storage system is built under a hybrid cloud architecture, where a private cloud manipulates the computation and a public cloud manages the storage.

The private cloud is provided with a trapdoor key associated with the corresponding ciphertext, with which it can transfer the ciphertext over one access policy into ciphertexts of the same plaintext under any other access policies without being aware of the underlying plaintext. After receiving a storage request, the private cloud first checks the validity of the uploaded item through the attached proof. If the proof is valid, the private cloud runs a tag matching algorithm to see whether the same data underlying the ciphertext has been stored. If so, whenever it

is necessary, it regenerates the ciphertext into a ciphertext of the same plaintext over an access policy which is the union set of both access policies.

The proposed storage system enjoys two major advantages. Firstly, it can be used to confidentially share data with other users by specifying an access policy rather than sharing the decryption key. Secondly, it achieves the standard notion of semantic security while existing deduplication schemes only achieve it under a weaker security notion.

REFERENCES

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

2. K. R. Choo, J. Domingo-Ferrer, and L. Zhang, "Cloud cryptography: Theory, practice and future research directions," Future Generation Comp. Syst., vol. 62, pp. 51–53, 2016.

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

4. Y. Yang, H. Zhu, H. Lu, J.Weng, Y. Zhang, and K. R. Choo, "Cloud based data sharing with fine-grained proxy re-encryption," Pervasive and Mobile Computing, vol. 28, pp. 122–134, 2016.

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

6. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings, ser. Lecture Notes in Computer Science, vol. 3494. Springer, 2005, pp. 457–473.