# EVALUATION OF A SAFE AND EFFICIENT ENERGY EFFORT SEARCHING TECHNIQUE ON MOBILE CLOUD

**[1]Susmitha Valli. Gogula, [2]P. Gopal Krishna**

[1]Assistant Professor, Department of Computer science engineering, GITAM University.

[2]Associate Professor, Department of Information Technology, Gokaraju Rangaraju Institute of Engineering and Technology

**ABSTRACT**

Customers are hesitant to trust the cloud with their information due to concerns about data protection even if cloud storage offers inexpensive, convenient, enormous, and scalable storage. One method to increase privacy from the standpoint of the data owner is to encrypt the files before outsourcing them to the cloud and decode the information after downloading them. Data encryption, however, imposes a significant burden on mobile devices, and data retrieval requires complex communication between the data user and cloud. Because of the frequently constrained bandwidth capacity and battery life, which add significant overhead to compute and communication as well as a higher power consumption for mobile device users, encrypted search over mobile cloud is quite challenging. TEES (Traffic and Energy saving Encrypted Search), a mobile cloud encrypted search architecture that consumes less bandwidth and energy, is presented in this paper. By further enhancing communication between the mobile clients and the cloud, the proposed architecture offloads computing from mobile devices to the cloud. It has been shown that using performance improvement techniques does not compromise data privacy. Our testing show that TEES significantly reduces network traffic while cutting computation time by 24% to 46% and energy consumption by 36% to 56% per file retrieval.

**Keywords:** Mobile cloud, storage, private and public cloud

## 1. INTRODUCTION

Cloud computing is a huge benefit to data providers who want to outsource their data to the cloud without disclosing their sensitive information to third parties and who want users with specific permissions to be able to access the data. Data must be kept in encrypted formats with access control policies that forbid people without the required attributes (or credentials) from decrypting the data. This is important to achieve this goal.

This criterion is addressed by an encryption technique known as "attribute-based encryption" (ABE). A message is encrypted using an access policy (or access structure) over a set of attributes in this method, and a user can decrypt a ciphertext using their private key if their set of attributes complies with the access policy linked to the ciphertext.

However, secure deduplication, a technique for minimising redundant copies of encrypted data stored in the cloud to free up storage space and network bandwidth, cannot be implemented by the standard ABE system. To the best of our knowledge, none of the current secure deduplication systems are built on attribute-based encryption, though.

Building a cloud storage system with both ABE and safe deduplication would be advantageous, though, considering how frequently cloud computing uses both.

Later, Alice, a different data provider, uploads a ciphertext for the same underlying file M that has access policy A0 applied to it. The cloud will keep M twice since it cannot determine whether the plaintext corresponding to Alice's and Bob's ciphertexts is the same because the file was uploaded in an encrypted manner. It goes without saying that such redundant storage uses up both storage space and transmission bandwidth. Hosting over the internet is used to store, manage, and process data instead of using a local server or a personal computer. The necessary storage space is provided by the cloud, enabling customers to save their data there.

There are various cloud platforms available for storing data.

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 organizations 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 servers, hardware, and storage necessary to support operations. These items are all available across a network. Cloud computing security has always been a significant risk, despite the fact that it offers businesses and customers a lot of ease.

Data encryption, however, imposes a significant burden on mobile devices, and data retrieval requires complex communication between the data user and cloud. The encrypted search over mobile cloud is highly difficult because of the often restricted bandwidth capacity and battery life, which bring considerable overhead to compute and communication as well as higher power consumption for mobile device users.

Mobile cloud storage (MCS) refers to a group of online services that are becoming more and more well-liked. It even serves as the main file storage for mobile devices.Through wireless connection, MCS enables users of mobile devices to save and retrieve files or other data from the cloud, improving data accessibility and facilitating file sharing without using up internal resources on the mobile device.

Since cloud storage systems have a privacy problem, owners encrypt sensitive data before sending it to the cloud, and users utilise encrypted search techniques to find the data they're looking for. Modern mobile devices are subject to many of the same security risks as personal computers in MCS, and numerous conventional data encryption techniques are imported.The restricted computing and battery capacity of mobile devices, as well as data sharing and accessing ways over wireless communication, present new problems for mobile cloud storage systems compared to the conventional encrypted search schemes. As a result, MCS requires a suitable and effective encrypted search scheme.

Due to the short battery life and associated traffic charges, mobile cloud storage often has a high need for bandwidth and energy efficiency for data encryption search schemes.As a result, we concentrate on creating a mobile cloud architecture that minimises network traffic and energy consumption while maintaining data security standards through wireless communication channels. Customers can access scalable and dynamic storage through public cloud-based storage services like Microsoft's Azure and Amazon's S3. Customers can save money by transferring their data to the cloud, which eliminates the need to construct and maintain a proprietary storage system.

For the majority of consumers, this offers multiple advantages at a reasonable price, including availability (being able to access data from anywhere) and reliability (without having to worry about backups). Cloud storage has benefits in terms of pay-per-use and elastic scalability. However, the data security risk ruins the relationship of trust between the consumer and cloud service provider. Encrypting data before it is saved in the cloud is a

straightforward solution to this issue. Therefore, the leaked data cannot be decoded without the decryption key. Despite being a fantastic technology, encryption is not necessarily suited for mobile users. Performance should be taken into account while utilizing a mobile device, such as a Smartphone, to access data that is stored in a cloud storage system because the encryption strategy involves a lot of workload.

Retrieving Files from Cloud Storage

Standard encrypted search over cloud data

Traditional cloud data encryption techniques include Fie/Index encryption.

After authentication, data retrieval and search are possible. File/Index encryption:

The preparation and indexing tasks are first carried out by the data owner.

A data user can only access a file after being verified by the data owner. Data Search and Retrieval after Authentication.

The data user provides his identification to the data owner during the authentication process.

If the user is a legitimate user, the data owner provides the encrypted keys back. The cloud server assists users in finding the top k relevant files for a particular keyword without having to decrypt them. Searches involve the following steps:

The query keyword is stemmed by the authenticated user, encrypted with the keys, then hashed to obtain its entry in the index. The cloud server receives the encrypted keyword at that point.

The cloud server first looks for the encrypted keyword in the index after receiving it. The data users are then supplied the index associated with this keyword.

The data user determines the top-k relevant files using the chosen index and relevance scores before sending a follow-up request to the cloud server to obtain the files.

There are three ways to access cloud storage services: through a co-located cloud computing service, a web service Application Programming Interface (API), or users of programmes that make use of the API, including cloud desktop storage gateways or web-based content management systems.

Cloud storage, which is based on infrastructure that is substantially virtualized, is comparable to bigger cloud computing in terms of an accessible interface, almost immediate elasticity and scalability, multitenancy, and metered resources.

Amazon S3 and VION capacity offerings are examples of off-premises cloud storage solutions that can be used. Although the phrase "cloud storage" originally referred to a hosted object storage service, it has since expanded to cover other forms of data storage that are also offered as services, such as block storage.

Services for object storage like Amazon S3 and Microsoft Azure storage programmes like open stack swift are available.

Storage that may be hosted and deployed with cloud storage features includes distributed storage research projects like Ocean Store and VISION Cloud as well as object storage solutions like EMC Atmos, EMC ECS, and Hitachi Content Platform.

Either in a federated or a cooperative storage cloud architecture, made up of numerous distributed resources but nevertheless acting as one.

Highly fault resilient thanks to data dissemination and redundancy.

Incredibly long-lasting thanks to the generation of versioned copies.

Typically, with respect to data replicas, eventually consistent.

## SYSTEM ANALYSIS

The statistic TF-IDF (term frequency-inverse document frequency), used in information retrieval, measures how significant a word is to a document in a collection. In text mining and keyword-based retrieval, it is frequently employed as a weighing factor. Among other systems, the TF-IDF algorithm, which Salton and McGill's book proposed, is one of the most well-liked.

Boolean keyword search and ranked keyword search are currently part of encrypted search. The server only returns files in a Boolean keyword search based on the presence or absence of the keywords.

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

We use one-to-one mapping OPE in this study, which will result in the control of statistics information leaks. Wang and associates. Proposed an OPE with a one-to-many mapping They used a complex algorithm to protect against security breaches. Due to their algorithm's complexity and high resource requirements, they would have performance and energy consumption issues. Proposed a rank-ordered search that protects secrecy. As the relevance ratings are calculated on the client side, adding to its workload, this technique performs poorly. proposed a single-round-trip search algorithm that could look through encrypted data. It's important to keep in mind that search results for many keywords could be more serious.

**IMPLIMENTATION**

The Placement Cell Authority generates the content key and the secret key that the end user has requested. Officer is another name for the officer in the placement cell. Authority can review all files using the content key and master secret key that were generated with the matching data owner details of the specific file.

The data student in this programme must first sign up for a cloud server accounts and obtain authorization. The term "student" here also means "data owner" or "end user." After receiving cloud server authorization, a student will encrypt and add a file, after which the student requests the content key and the master secret key from the placement cell for the file they added and looks for redundancy. Only after the keys have been generated is the file uploaded to the cloud server. The student must grant download and search permission for each file after uploading it in order for people to download and search for it.

The user needs sign up and log in in order to access files that are saved in the cloud. The user is permitted by the cloud to validate the registration. The user must request the MSK master secret key and content key in order to download the file. Users can only download and search for files if the file's owner has given them permission to do so.

**CLOUD SERVER**

To provide services for data storage, a cloud is run by a cloud server. Data owners encrypt and store their data files in the cloud in order to share them with cloud End users. Access to the shared data files requires both the MSK master secret key and the content key, which users must request. Additionally, the cloud will provide the authorization. Additionally, it monitors all attackers and file-related activity.

## EXPERIMENTAL RESULTS

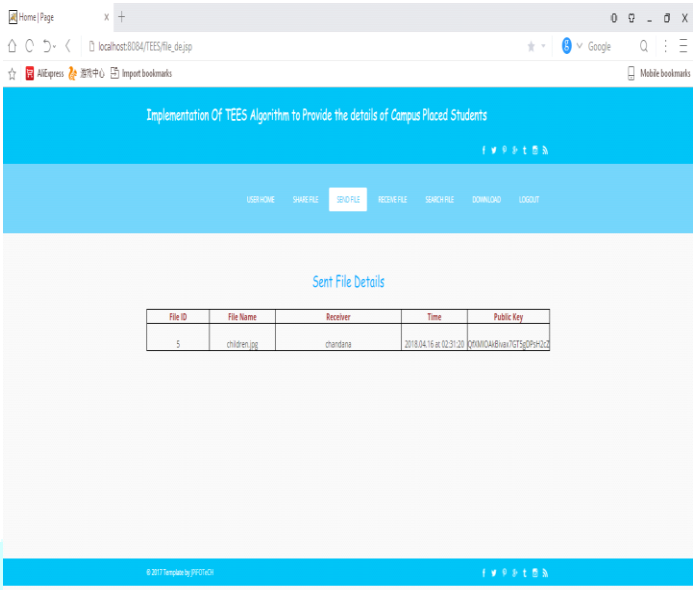


Fig 1. Seet file details

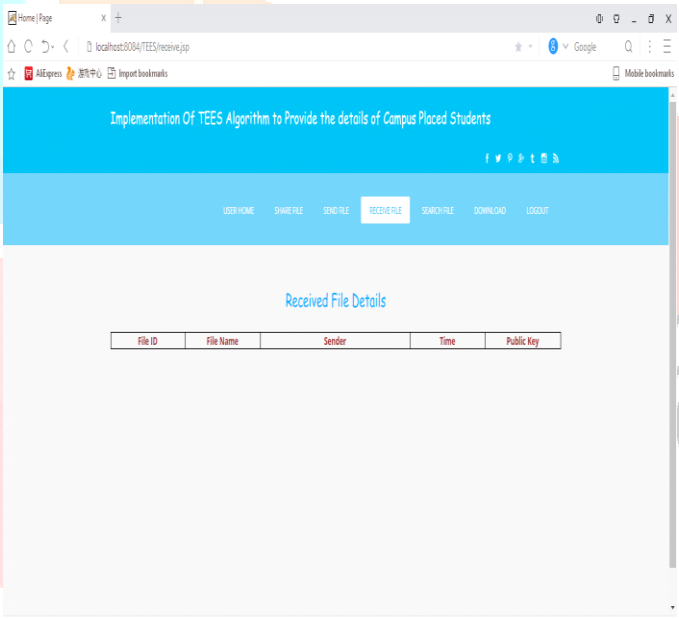


Fig 2 received file details

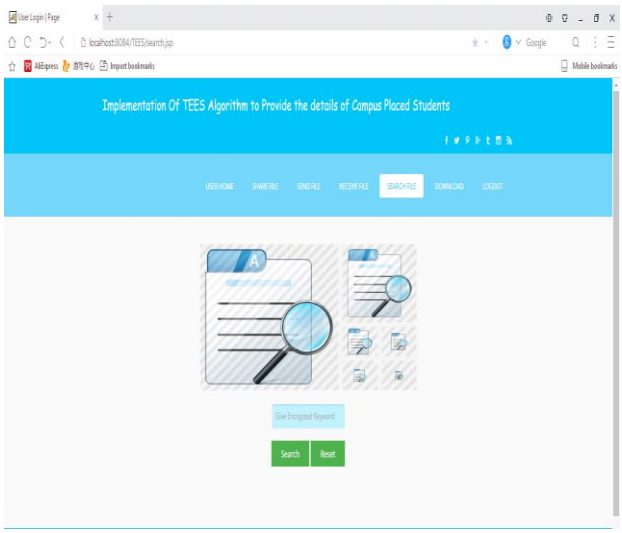


Fig 3 output result

## CONCLUSION

Attribute-based encryption (ABE), which enables data providers to transport encrypted data to the cloud and share it with users who have the necessary credentials, has been widely used in cloud computing. On the other hand, reduplication, which eliminates duplicate copies of the same data, is a critical method to reduce network traffic and storage space. However, standard ABE systems do not offer safe reduplication, making them more expensive to adopt in some commercial storage services. In this work, we presented a novel approach for building an attribute-based storage system that supports secure reduplication. In the hybrid cloud architecture of our storage solution, compute is managed by a private cloud, while storage is managed by a public cloud.

## 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.