A SECURE AGGREGATE KEY CLOUD STORAGE SYSTEM WITH PRIORITY QUEUE BASED SEGMENTATION

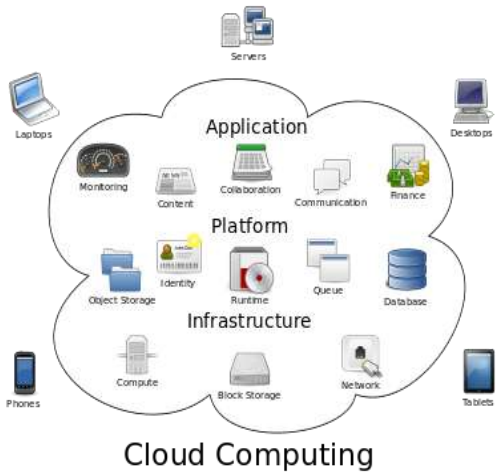
[1]R. Rasheeda Begum, [2]M.O.Ramkumar,
[1,2]Department of CSE, IFET College of Engineering,
[1]rasheeda011996@gmail.com, [2]ramkumar.mo86@gmail.com
Villupuram, India

Abstract— **As Cloud Computing becomes popular, personal and sensitive information are being increasingly centralized into the cloud. By utilizing the cloud, the user can be completely released from the troublesome local data storage and maintenance. For the protection of data privacy, sensitive data has to be encrypted before outsourcing. Even though which make the effective data utilization it perform encryption and decryption process were used to protect the data but the intruders are increasing in cloud to hack the group of data. In this paper, priority queue based segmentation is utilized after the data encrypted and then upload the encrypted data into the cloud. In results of this the intruders cannot rely on whole data which they prefer, but they receive minuscule data with this few data hackers cannot do anything .Therefore it provides a security for the stored data files in cloud.**

Index Terms— Cloud computing, Encryption, Priority queue based segmentation, storage

I. INTRODUCTION

Nowadays cloud computing is a recently evolved computing terminology based on the consumption of computing resources. Cloud computing involves deploying groups of remote servers and software networks that allow centralized data storage and online access to computer services. Clouds can be classified into public and private.



Cloud computing relies on sharing of resources to achieve the economies of scale, similar to a utility (likes electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services.

The goal of cloud computing is to apply traditional supercomputing, ubiquitous or high-performance computing power, normally used by military and other research facilities, it perform tens of trillions of computations per second, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The data leaks, caused by a malicious adversary cloud operator, can usually lead to serious breaches of personal privacy or business secrets (e.g., the recent high profile incident of celebrity photos being leaked in Cloud). To avoid the leakage in cloud storage, a common approach is for the data owner to encrypt all the data before uploading them to the cloud, after sometime encrypted data are retrieved and decrypted by those who have the authority of decryption keys. Such a cloud storage is often called the cryptographic cloud storage. However, the encryption of data makes a challenging for the users to search and then selectively retrieve only the data containing given keywords. A common solution is to employ a searchable symmetric encryption (SSE) scheme. To support searchable group data sharing the main re-quirements for efficient key management is a data owner only needs to distribute a single aggregate key (instead of a group of keys) to a user for sharing any number of files and then the user only needs to submit a trapdoor to the cloud for performing keyword search over any number of shared files. In this paper we address to enhance the data security because nowadays hackers (or) intruders are increasing in cloud to hack the group of data.so the main aim of the paper is to provide an advanced data security which can be achieved through priority queue based segmentation is utilized. Due to this segmentation the hackers cannot obtain the whole data and only pinch of data is disclosed with this few data they cannot do anything and one of the advantage is delay less data uploading in G-mail and it give more security, flexibility to share a data to the accurate user.

II.LITERATURE SURVEY

A. A Study on the Different Image Segmentation Technique

The segmentation process converts a given image into different object and region. Image Segmentation[7] has become prevalent due to its many vision applications. It is defined as the process of dividing the image into parts based on homogeneity. The main purpose of image segmentation is to make the representation of an image simpler into something that is more meaningful and easier to understand. The process in which a data set or say pixels are replaced by cluster, pixels may belong together because of the same color, texture etc is known as Clustering based method.

B. Server-Aided Public Key Encryption with Keyword Search"

In this work, we provided a practical and applicable treatment on (inside) off-line KGA(keyword guessing attack) by formalizing a new PEKS system, namely Server-Aided Public Key Encryption with Keyword Search (SA-PEKS)[8]. We introduced a universal transformation from any PEKS scheme to a secure SAPEKS scheme, also with the first instantiation of SA-PEKS scheme and showed how to securely implement the client-KS protocol with a rate-limiting mechanism against on-line KGA. It achieves much better efficiency while providing resistance against both off-line and on-line KGAs.

C. Image Segmentation by Cascaded Region Agglomeration

It proposes a hierarchical segmentation algorithm that starts with a very fine over segmentation and gradually merges regions using a cascade of boundary classifiers. This approach allows the weights of region and boundary features are adapted to the segmentation scale at which they are applied. The stages of the cascade are trained sequentially, with asymmetric loss to maximize boundary recall. On six segmentation data sets, the hierarchical segmentation algorithm achieves best performance under most region-quality measures. Hierarchical segmentation[6] algorithm is also highly competitive in dense over segmentation (super pixel) regime under boundary-based measures.

D. Secure ranked keyword search over encrypted cloud data

In this paper solve the problem of supporting efficient ranked keyword search for achieving effective utilization of remotely stored encrypted data in Cloud Computing and it weaken the security guarantee, so it resort to the newly developed crypto primitive OPSE(order preserving symmetric encryption), and derive an efficient one-to-many order-preserving mapping function, which allows the effective RSSE to be designed. It enjoys "as-strong-as-possible" security guarantee compared to previous SSE schemes[4], while correctly realizing the goal of ranked keyword search.

E. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing

A secure cloud storage system supporting privacy-preserving public auditing to avoid the burden of user. It extend the result to enable the TPA (Third Party Auditor)[3]to perform audits for multiple users simultaneously and efficiently to avoid the knowledge about the data content stored in the cloud server. It avoid the user fear when they are outsourcing the sensitive data and it provide extensive security and performance analysis show that it provably secure and highly efficient.

III. SYSTEM DESIGN

A. Existing System

To kept the data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task.

The data owner encrypted the multiple data and need to distribute a single aggregate key(instead of a group of keys) to a user forsharing a large number of documents and need to submit a single trapdoor to the cloud for querying the shared documents.

B. Disadvantages of Existing System

- Unexpected privilege escalation will expose all and is not efficient
- Shared data will not be secure because intruders are increasing
- The costs and complexities involved generally increase with the number of the decryption keys to be shared and convert into trapdoor

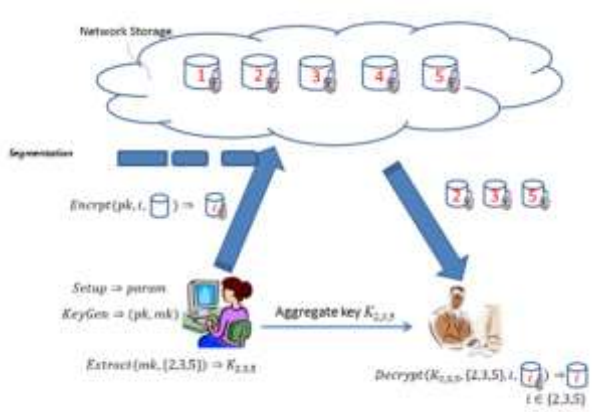
C. Proposed System

In our proposed system we are going to overcoming the delay related issues we are applying segmentation process after the encryption for increasing delay efficiency. In segmentation phase, apply priority queue based segmentation process in cloud while storing a data. It will convert the complete data into small segments. By using this segmentation process, the intruders cannot rely on whole data's which they prefer, but they receive chunked data, with this data the hackers cannot do anything. It provides a security and privacy among the hackers. The cloud storage system highlights on a process when a file is crashed while uploading in G-mail, it doesn't start loading again from the beginning but from crashed part because nowadays intruders are increasing in cloud to hack the group of data to avoid this segmentation process are held.

D. Advantage of Proposed System

- Any user in the group can store and shared data files with others by the cloud in a secure manner
- Usually the segmentation scheme will ensure the additional delay less communication
- Decryption key is sent via a secure channel and kept secret because to avoid the intruder during the transfer
- It is an efficient public-key encryption scheme which supports flexible delegation
- The extracted key are an aggregate key which is as compact as a secret key for a single class and this avoid the large number of keys
- The delegation of decryption can be efficiently implemented with the aggregate key send by the sender who have the authority to store the data in cloud

IV. ARCHITECTURE



V. MODULES DESCRIPTION

A. Setup and KeyGen Phase

- In setup phase, the data owner have the authority to executes the setup phase for an account on server and takes implicit security parameter
- In Keygen phase, the data owner is executed by data user to generate public key or the master key pair (pk, msk)

B. Encrypt Phase

- This phase is executed by user who wants to send the encrypted data
- Encrypt (pk, m), the encryption algorithm takes input as public keypk, a message m, The algorithm encrypts message m using public key and produces a cipher text C such that only a user that has a set of attributes that satisfies the access structure is able to decrypt the message
- The format of encryption is
  - Input= public key pk, and message m
  - Output = cipher text

C. Segmentation Phase

- In segmentation phase applying the segmentation process in cloud while storing a data.
- It will convert the complete data into small segments after calculating the size of the data.
- After chunk the data is stored in queue cloud buffer.
- Then the data are stored in cloud in different database with the help of drop tail mechanism.
- This will lead to reduce the hacking data and provide flexibility, security, privacy among the hackers.

D. Extract

- In the Extract phase, the data owner for delegating the decrypting power for a certain set of ciphertext classes to a delegate
- The format of Extract is
  - Input = master-secret key mk and a group of single set S corresponding to different classes
  - Outputs = aggregate key for single set S denoted by Ks

E. Decryption

- In the Decryption phase, is used by the user who has the decryption authorities. Decrypt (kS, S, I, C), the decryption algorithm takes input as public parameters pk, a cipher text C, i denoting cipher text classes for a set S of attributes
- The format of Decryption is
  - Input = kS and the set S, where C = cipher text class
  - Outputs = original plaintext are displayed

VI. CONCLUSION

Considering the practical problem of privacy preserving data sharing system increasing in public cloud storage. In this paper we proposed a schemes priority queue based segmentation for data storage security in cloud computing and it ensure the delay less communication. It avoids the privacy risk during the data transfer and provides a security among the Hackers.

VII. REFERENCES:

[1]. Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in *Proc. of ACNS'05*, 2005.

[2]. R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky. "Searchable symmetric encryption: improved definitions and efficient constructions", In Proceedings of the 13th ACM conference on Computer and Communications Security, ACM Press, pp. 79-88, 2006.

[3]. C. Wang, Q. Wang, K. Ren, and W. Lou, ―Privacy-Preserving Public Auditing for Data Storage Security in Cloud Comput-ing‖,Proc. IEEE INFOCOM, pp. 525-533, 2010.

[4]. C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. IEEE Distributed Computing Systems (ICDCS'10), Genoa, Italy, Jun.2010, pp. 253–262.

[5] X. Liu, Y. Zhang, B. Wang, and J. Yan. "Mona: secure multiowner data sharing for dynamic groups in the cloud", IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6): 1182-1191.

[6].ZhileRen, Gregory Shakhnarovich, "Image Segmentation by Cascaded Region Agglomeration", CVPR,2013

[7].RozyKumari, Narinder Sharma, "A Study on the Different Image Segmentation Technique" ,International Journal of Engineering and Innovative Technology (IJEIT**),** Volume 4, Issue 1, July 2014.

[8]. Rongmao Chen, Yi Mu, Guomin Yang Fuchun Guo, Xinyi Huang, Xiaofen Wang* and Yongjun Wang "Server-Aided Public Key Encryption with Keyword Search", IEEE Transactions on Information Forensics and Security, 1556-6013 (c) 2016