International Journal of Innovations in Engineering and Technology (IJIET)
http://dx.doi.org/10.21172/ijiet.131.03

Proficient recovery over records using encryption in cloud computing

D.Kanchana[1], Dhandapani Samiaappan[2]
[1]*Assistant Professsor(S.G), Department of Computer Applications,*
SRM Institute of Science and Technology, Ramapuram Campus, Chennai
[2]*Department of Electronics and Communication Engineering, Saveetha Engineering College, chennai*

Abstract- In many searchable cryptography schemes are planned, few of them support economical retrieval over the documents that are encrypted supported their attributes. A ranked attribute-based cryptography theme is initially designed for a document assortment. A collection of documents will be encrypted together if they share associate integrated access structure. Compared with the cipher text-policy attribute-based cryptography (CP-ABE) schemes, each the cipher text cupboard space and time prices of encryption/decryption are saved. Then, associate index structure named attribute-based retrieval options (ARF) tree is made for the document assortment supported the TF-IDF model and therefore the documents' attributes. The ARF tree is based on the hierarchical attribute based encryption scheme (HABE). A depth-first search algorithmic program for the ARF tree is intended to boost the search potency that can be additional improved by parallel computing. Aside from the document collections, our theme will be conjointly applied to different datasets by modifying the ARF tree slightly. The modification scheme is called as HABE. A radical analysis and a series of experiments are performed as an example the security and potency of the planned theme.
Keywords – Cloud Computing, Encryption, ARF, CP-ABE, HABE

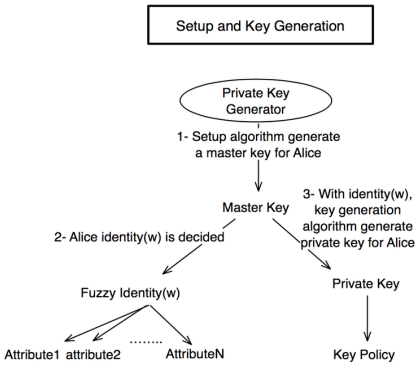
I. INTRODUCTION

A sensible hierarchical attribute-based document assortment encryption scheme is projected during which the documents are organized and controlled supported attributes. The projected theme will greatly decrease the storage and computing burdens. We have a tendency to map the documents to vectors during which both the keywords and′ associated attributes are considered. A depth-first search algorithm for the ARF tree is designed to guarantee both the search efficiency and accuracy. A TF/IDF model is used for compute similarities among documents, this overcome the time-efficient retrieval over the documents. The performance of the approach is thoroughly evaluated by both theoretical analysis and experiments.

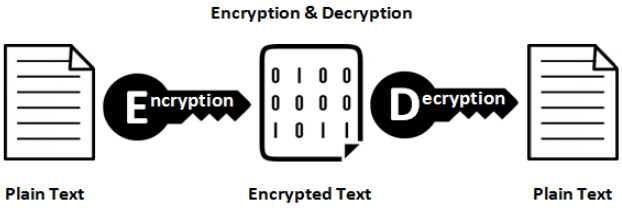
II. PROPOSED ALGORITHM

2.1 Attribute based encryption –

Attribute-based encryption (ABE) is a relatively recent approach that reconsiders the concept of public-key cryptography. In traditional public-key cryptography, a message is encrypted for a specific receiver using the receiver's public-key. Identity-based cryptography and in particular identity-based encryption (IBE) changed the traditional understanding of public-key cryptography by allowing the public-key to be an arbitrary string, e.g., the email address of the receiver. ABE goes one step further and defines the identity not atomic but as a set of attributes, e.g., roles, and messages can be encrypted with respect to subsets of attributes (key-policy ABE - KP-ABE) or policies defined over a set of attributes (ciphertext-policy ABE - CP-ABE). The key issue is, that someone should only be able to decrypt a ciphertext if the person holds a key for "matching attributes" (more below) where user keys are always issued by some trusted party.



Key generation of ABE



File encrypt & decrypt

2.2. TF/IDF algorithm –
The TF of a word is the frequency of a word (i.e. number of times it appears) in a document. When you know it, you're able to see if you're using a term too much or too little. The IDF of a word is the measure of how significant that term is in the whole corpus. If a word appears frequently in a document, then it should be important and we should give that word a high score. But if a word appears in too many other documents, it's probably not a unique identifier, therefore we should assign a lower score to that word. The math formula for this measure :
tfidf(t,d,D)=tf(t,d)×idf(t,D)
Where t denotes the terms; d denotes each document; D denotes the collection of documents.

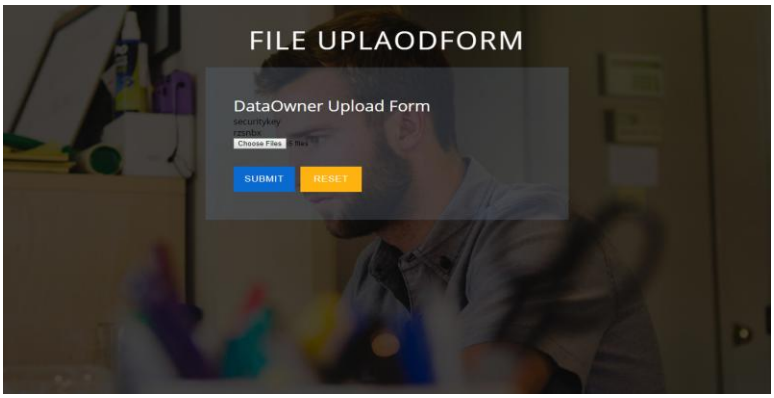
2.3 Hierarchical Attribute-Based Encryption–
Here, encryption scheme has a master node which will be the root master node that correlates with third party trust, multiple domain authority master nodes which correlate with multiple consortium users. The property of hierarchical key generation is used in hierarchical identity based encryption mainly for generating keys. This specific feature empowers cipher text policy hierarchical attribute based encryption system to include large number of users from various organizations by delegating keys, e.g., Validating efficient data sharing between hierarchically arranged groups. For this technique Cipher text policy hierarchical attribute based encryption scheme is constructed with short cipher texts.

fid	securitykey	photourl	file
12	wpjmrh	0x433A5C66696C65735C61646D6974636172642E646F6...	admitcard
13	wpjmrh	0x433A5C66696C65735C616E64726F696420767320696...	android vs ios.ppt
14	wpjmrh	0x433A5C66696C65735C666F726D61742E646F6378	format
15	wpjmrh	0x433A5C66696C65735C6A6F686E61646D6974636172...	johnadmitcard
16	tiznnl	0x433A5C66696C65735C446174616261736520446573736...	Database Design-Cloud
17	tiznnl	0x433A5C66696C65735C456666696369656E742052657...	Efficient Retrieval-Cloud Computing
18	tiznnl	0x433A5C66696C65735C464F524D2044455349474E2D...	FORM DESIGN-Cloud
19	tiznnl	0x433A5C66696C65735C46756C6C20646F63756D656E...	Full documentation

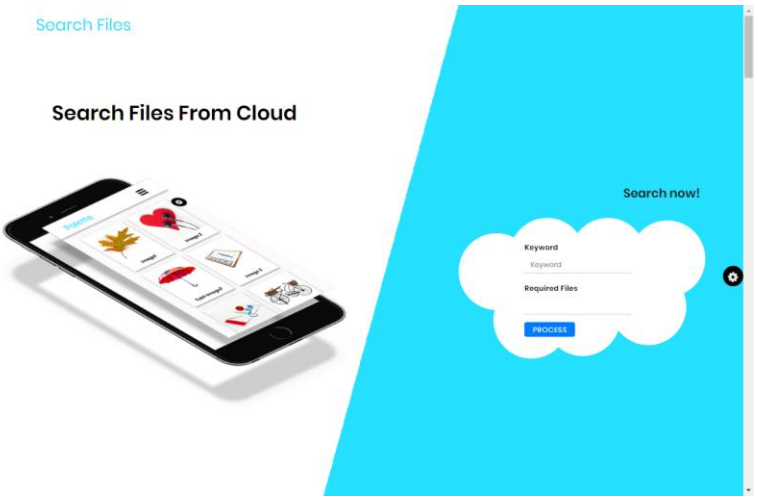
Multiple files generated using hierarchical structure

III. EXPERIMENT AND RESULT

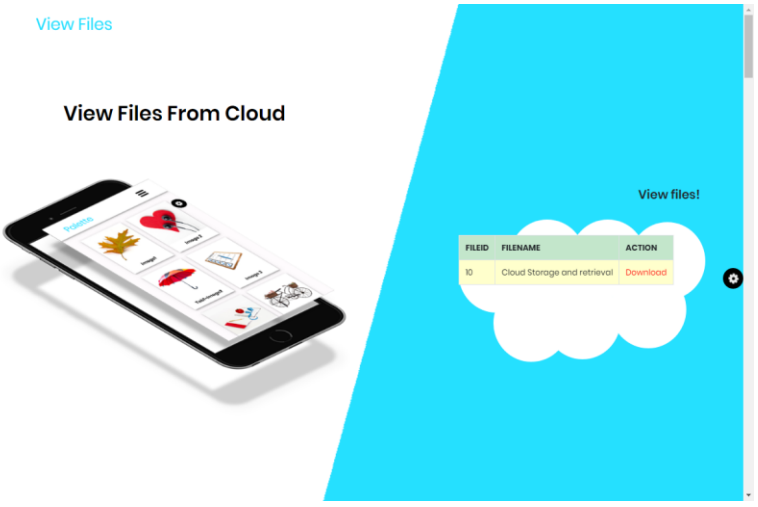
The test set for this evaluation experiment to select the file which you have to upload . Eclipse, Apache Tomcat server 8.0 and HeidiSQL software platform is use to perform the experiment. The PC for experiment is equipped with an Intel P4 2.4GHz Personal laptop and 2GB memory.



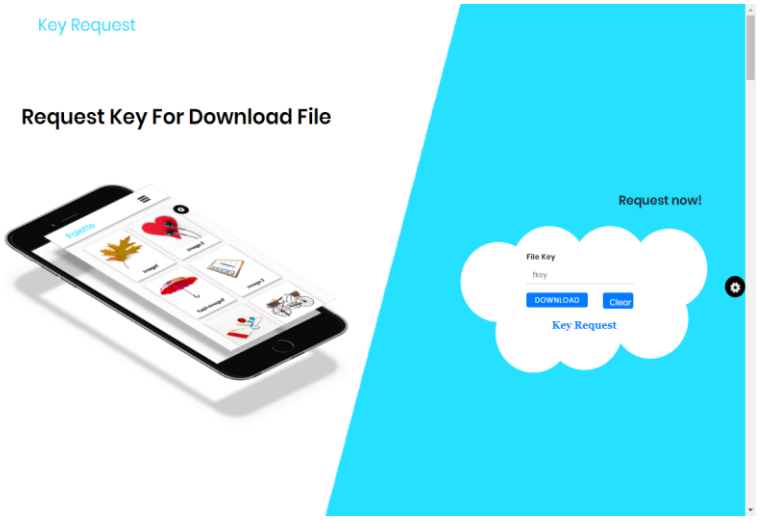
File upload by data owner



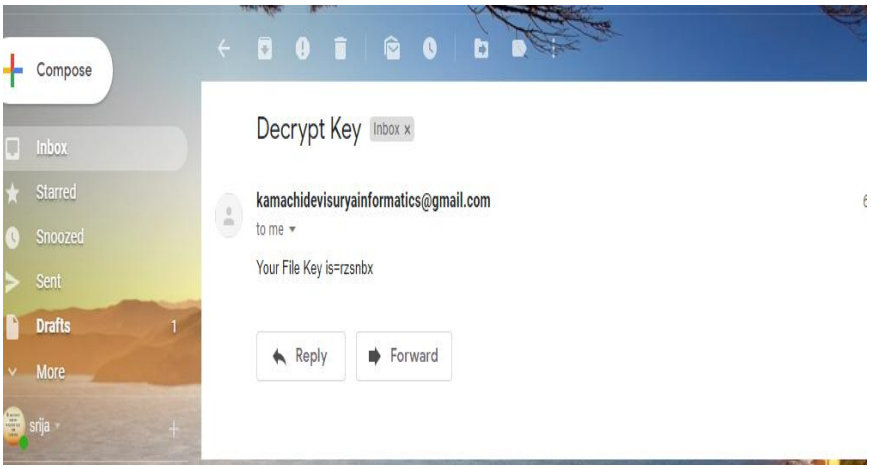
Search files by data user



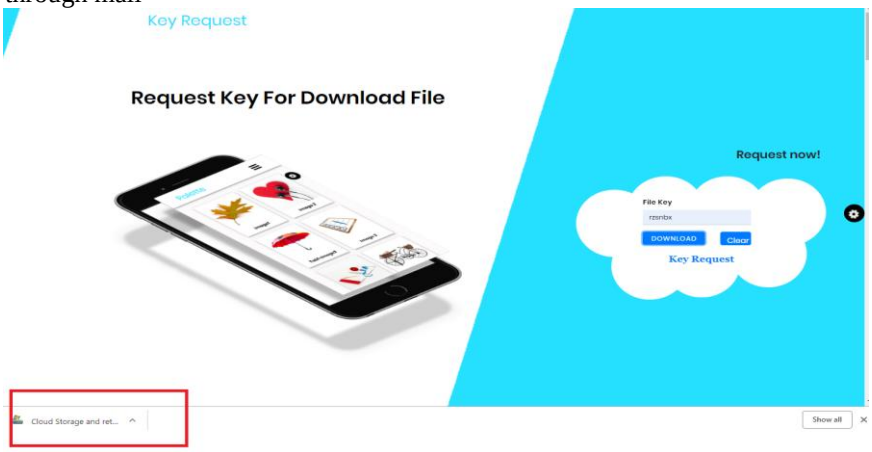
View files by data user



Key request for file download by data user



Decrypt key send through mail



Request key for download file

IV.CONCLUSION

This proposed system we tend to take into account a brand new encrypted document retrieval situation during which the data owner desires to regulate the documents in fine-grained level. To support this service, we initially design a completely unique hierarchical attribute-based document encryption scheme to encrypt a collection of documents along that share an integrated access structure. Further, the ARF tree is planned to prepare the document vectors supported their similarities. Based on CP-ABE and hierarchical attribute based encryption scheme, we uniquely combine them to support the same document with different privileges for different users. A data owner can outsource an encrypted document to cloud servers, sharing the document among the users with a same or higher security class. Our proposed scheme can achieve the merits of original CP-HABE, such as data confidentiality and scalability. At last, a depth-first search formula is intended to improve the search potency for the data users that is very vital for big document collections

V. REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, pp. 69–73, Jan. 2012.
[2] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. SandP 2000. Proceedings. 2000 IEEE Symposium on, pp. 0–44, 2002.
[3] E. J. Goh, "Secure indexes," Cryptology ePrint Archive, http:// eprint.iacr.org/2003/216., 2003.
[4] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in ACM Conference on Computer and Communications Security, pp. 79– 88, 2006.
[5] J. Li, Y. Shi, and Y. Zhang, "Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage," International Journal of Communication Systems, vol. 30, no. 1, 2017.
[6] Y. Miao, J. Ma, X. Liu, X. Li, Q. Jiang, and J. Zhang, "Attributebased keyword search over hierarchical data in cloud computing," IEEE Transactions on Services Computing, vol. PP, no. 99, pp. 1–1, 2017.
[7] A. Swaminathan, Y. Mao, G. M. Su, H. Gou, A. L. Varna, S. He, M. Wu, and D. W. Oard, "Confidentiality-preserving rank-ordered search," in ACM Workshop on Storage Security and Survivability, Storagess 2007, Alexandria, Va, Usa, October, pp. 7–12, 2007.