VERIFIABLE ASSOCIATE DEGREED MULTI-KEYWORD SEARCHABLE ATTRIBUTE-BASED CRYPTOGRAPHY THEME FOR CLOUD STORAGE

Mr.U.Satyanarayana
Asst. Professor ,Department of Computer Science Engineering, Narayana Engineering College Gudur

Manaswini Chunduru
B.Tech, Department of Computer Science Engineering, Narayana Engineering College Gudur

Kalyani Doddaka
B.Tech, Department of Computer Science Engineering, Narayana Engineering College Gudur

Priyanka Modem
B.Tech, Department of Computer Science Engineering, Narayana Engineering College Gudur

ABSTRACT

In an Attribute-Based Searchable Encryption (ABSE) scheme, knowledge homeowners will cipher their data with access policy for security thought, and cipher keywords to get keyword index for privacy keyword search, and knowledge users will search attention-grabbing keyword on keyword indexes by keyword search trapdoor. But many existing searchable cryptography schemes entirely supports single keyword search and most of existing attribute-based encryption (ABE) schemes have high process prices at user consumer. These issues considerably limit the appliance of attribute-based searchable cryptography schemes in apply. In this paper, we have a tendency to propose a verifiable and multi-keyword searchable attribute-based cryptography (VMKS-ABE) theme for cloud storage, in our new theme multi-keyword are often searched and therefore the search privacy is also protected. That is, the cloud sever will search the multi-keyword with keyword search trapdoor however it doesn't understand any info of the keywords searched .

Keywords: attribute-based encryption, verifiable outsourcing, multi-keyword search, adaptive security

1.INTRODUCTION

With the event of cloud computing, several of data are often shared through pc networks. The cloud server (CS) will offer users with a spread of services, like outsourcing commission calculations and knowledge storage. Users will store their massive amounts of knowledge to the caesium and share data with alternative users. For the aim of the protection of storage knowledge and user's privacy, knowledge is typically hold on in encrypted kind in caesium .The SE technology primarily solves the matter of the way to use the server to complete the rummage around for attention-grabbing keywords once the info is encrypted and hold on in caesium, however caesium isn't fully trustworthy. The way to improve the potency of keyword search whereas reducing native computing load remains a retardant to be resolved. Most of existing schemes support single-keyword search. Single-keyword search waste network information measure and computing resources, as this search methodology returns an outsized variety of results, this implies that the search result's not correct.

2.LITERATURE SURVEY

The concept of searchable encryption(SE) was first proposed by Song et al [1],which provides a basic method for searching on encrypted data in the cloud.

To implement a SE scheme in a multiuser environment Dong et al [2] used RSA public key encryption algorithm and proxy encryption technology.

ABSE scheme based on the attribute encryption algorithm was proposed by Li et al [3] and proved that it can achieve indistinguishable safety against chosen keyword plaintext attacks under the selective model of attribute set. And also many scholars experts published their solutions about the problem of how to conduct secure keyword search in encrypted data.

ABSE with constant-size was constructed by Ye et al. [4] in which the scheme realizes that the cipher text size remains unchanged and a constant calculation cost. Because of improper operation and data destruction, cloud server may return wrong search answers. Consequently, in semi-trusted cloud environment, it is very significant to ensure the correctness of returned answers .

Sun et al. [5], and Dong et al. [6] constructed ABSE schemes to implement fine-grained access control and search for encrypted data. Attribute-based keyword search has been used extensively because it can implement flexible access policy. Notably, the communication cost and computational cost in the existing ABSE schemes are arranged with the number of required attributes.

Zhang et al. [7] proposed a fully outsourced ciphertextpolicy ABE scheme that for the first time achieves outsourced key generation, encryption and decryption simultaneously. However, although CS has strong computing power, it is not completely trustworthy. Usually cloud server is considered as honest but curious.

The concept of ABE was proposed by Sahai and Waters [8]. ABE can be classified into two types: one is the key-policy attribute-based encryption (KP-ABE) [9]; the other is the ciphertextpolicy attribute-based encryption (CP-ABE) [10]. In the CPABE schemes, the ciphertext is related to an access policy, and private key of each user is related to the attribute set of the user. Users can decrypt a ciphertext only if their attribute set satisfies the access policy of the ciphertext. In the KP-ABE schemes, the attribute set and access policy are opposite to those described in the CP-ABE scheme. Only if the user’s attributes set satisfies the access policy,then only the user can do decryption correctly in the decryption process.

3.EXISTING SYSTEM

Most of existing attribute-based cryptography (ABE) schemes have high process prices at user consumer. These issues greatly limit the applications of ABE schemes in apply. The idea of searchable cryptography , that provides a basic methodology for looking out on encrypted cloud knowledge used RSA public key cryptography rule and proxy encryption technology to implement a SE theme in an exceedingly multiuser surroundings. The disadvantages present in this system are though caesium has study computing power, it's not fully trust worthy. And also have high computational costs at user client in many of the existing attribute-based encryption (ABE) schemes.

4.PROPOSED SYSTEM

To unravel the issues of network information measure waste and high process value, we have a tendency to propose a Verifiable and Multi-Keyword Searchable Attribute-Based Cryptography (VMKS-ABE) theme for cloud storage as shown in fig 1, within which several computing tasks are outsourced to cloud proxy server to scale back native computing burden, the theme additionally supports the verification of the correctness of outsourced personal keys. Lai et al. Projected a verifiable outsourced ABE theme which will verify the correctness of decipherment. In this system search privacy is protected and the keyword search accuracy is improved. And decreases the communication value of the answer .

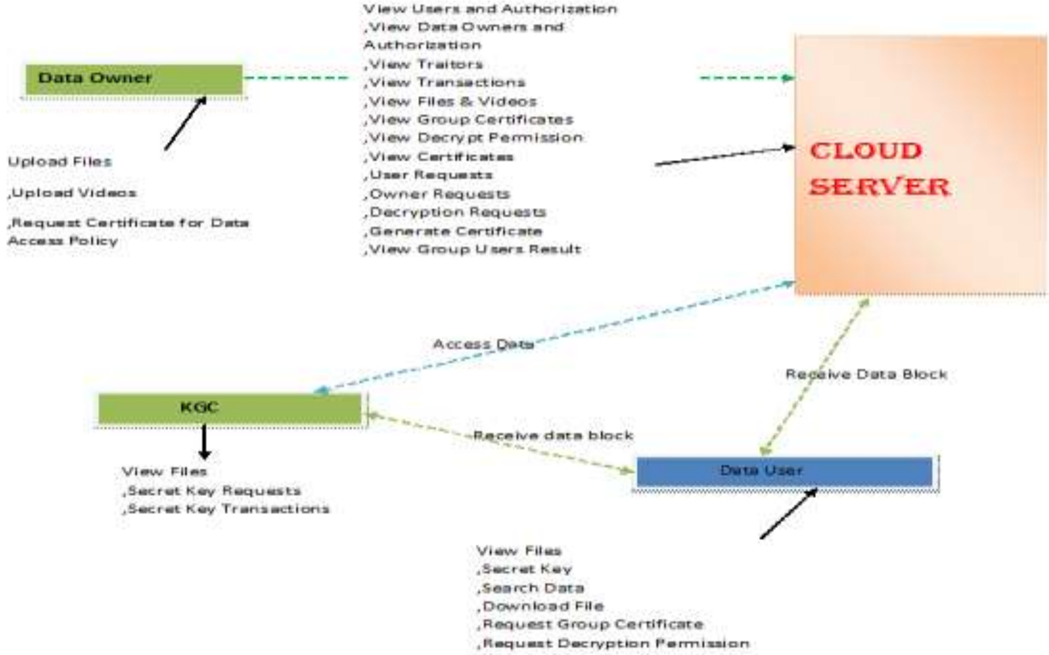
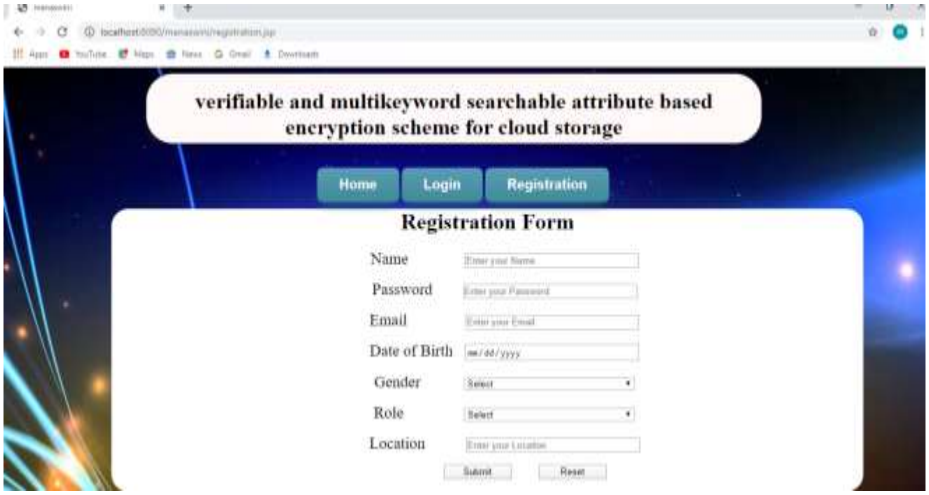


Fig. 1 cloud storage

Data Owner

During this module, he/she can logs in by using his/her user name and password. Once login the owner Uploads knowledge, read files blocks as shown in Fig. 2 and Fig. 3



verifiable and multikeyword searchable attribute based encryption scheme for cloud storage

Registration Form

Name	Enter your Name
Password	Enter your Password
Email	Enter your Email
Date of Birth	mm/dd/yyyy
Gender	Select
Role	Select
Location	Enter your Location

Fig. 2 Log in

User

During this module, he/she logs in by using his/her user name and password. Once login is successful user will do some operations like searching files to download,download files etc.

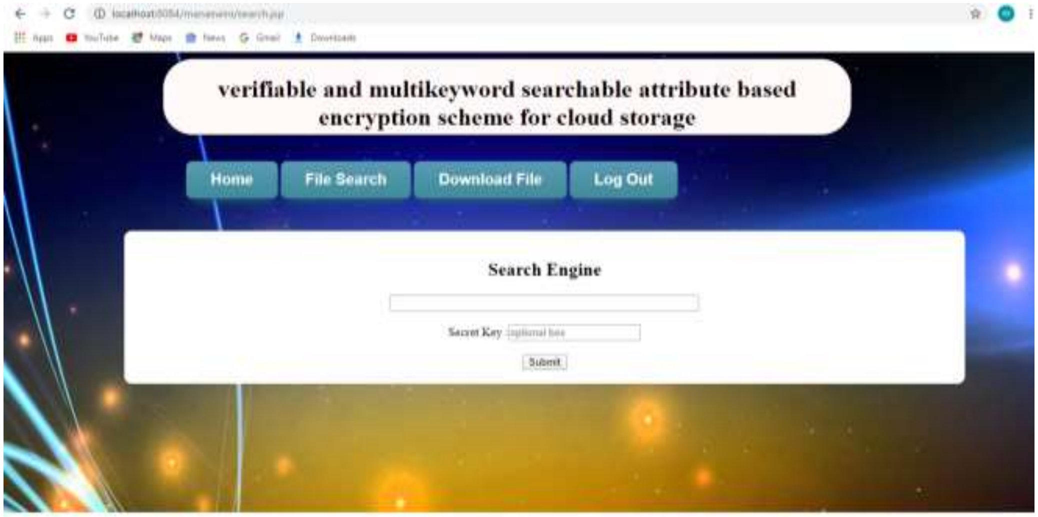
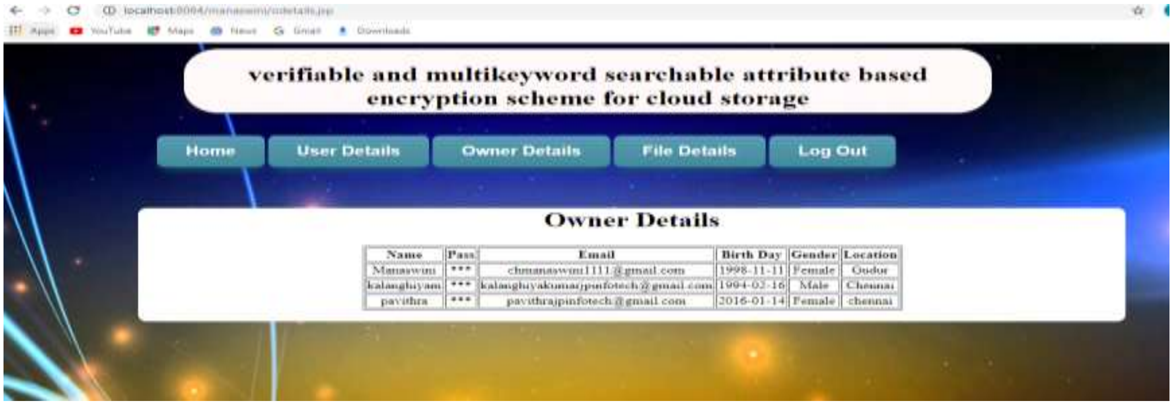

verifiable and multikeyword searchable attribute based encryption scheme for cloud storage
Home
File Search
Download File
Log Out
Search Engine
Secret Key
optional box
Submit

Fig. 3

Cloud Server

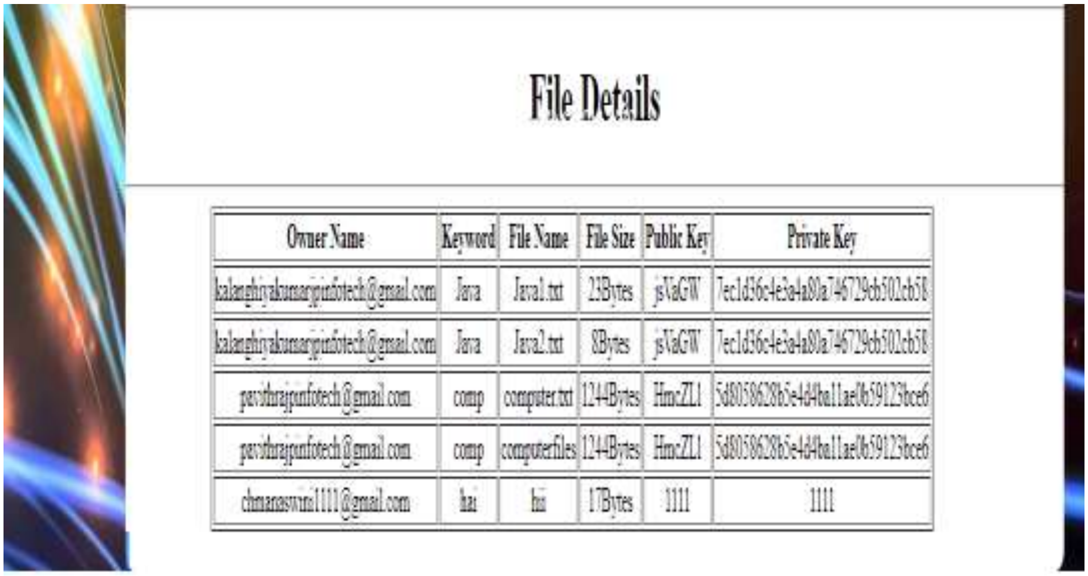
The Cloud server as a server to produce knowledge storage service and may additionally do the subsequent operations like read finish Users and Authorize ,View knowledge homeowners and Authorize, read All hold on knowledge, read Transactions,View Attackers, read Search Request, read Download_Request,View Files Rank In Chart, read Time Delay In Chart, read output In Chart.In this module, we develop the Key Distribution Center (KDC) which provides the accessibility of files to users.Initially to the selected file,the user will request for a secret key pair.The respective public and private key credentials will be sent to the Email ID of users by key distribution centre. All end user details, owner details and file details are shown in Fig 4. In this the owner can view all end users,owners and their details as shown in Fig 5,6 and 7


verifiable and multikeyword searchable attribute based encryption scheme for cloud storage
Home
User Details
Owner Details
File Details
Log Out

Owner Details

Name	Pass	Email	Birth Day	Gender	Location
Manaswini	***	chmanaswini1111@gmail.com	1998-11-11	Female	Gudur
kalanghiyam	***	kalanghiyakumarjpinfotech@gmail.com	1994-02-16	Male	Chennai
pavithra	***	pavithrajpinfotech@gmail.com	2016-01-14	Female	chennai

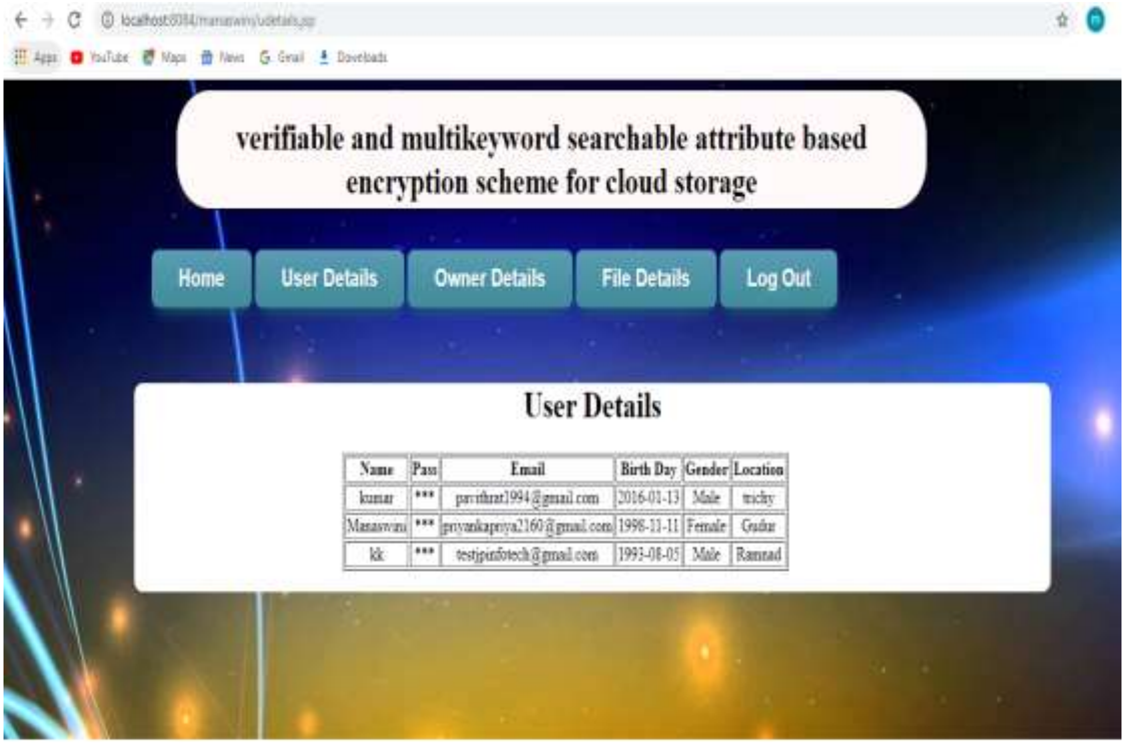
Fig. 4 Key distribution center



File Details

Owner Name	Keyword	File Name	File Size	Public Key	Private Key
kalanghiyakumarjpinfotech@gmail.com	Java	Java1.txt	23Bytes	jsVaGW	7ec1d36c4e3a4a80a746729cb502cb58
kalanghiyakumarjpinfotech@gmail.com	Java	Java2.txt	8Bytes	jsVaGW	7ec1d36c4e3a4a80a746729cb502cb58
pavithrajpinfotech@gmail.com	comp	computer.txt	1244Bytes	HmcZL1	5d8058628b5e4d4ba11ae0b59123bce6
pavithrajpinfotech@gmail.com	comp	computerfiles	1244Bytes	HmcZL1	5d8058628b5e4d4ba11ae0b59123bce6
chmanaswini1111@gmail.com	hai	hii	17Bytes	1111	1111

Fig. 5



verifiable and multikeyword searchable attribute based encryption scheme for cloud storage

User Details

Name	Pass	Email	Birth Day	Gender	Location
kumar	***	pavithrat1994@gmail.com	2016-01-13	Male	trichy
Manaswini	***	priyankapriya2160@gmail.com	1998-11-11	Female	Gudur
kk	***	testjpinfotech@gmail.com	1993-08-05	Male	Ramnad

Fig. 6

5.CONCLUSION

During this article we have a tendency to projected VMKS-ABE theme. In our theme, we have a tendency to mix the verifiable of the correctness of outsourced personal key with multi-keyword search supported attribute cryptography. Within the general cluster model, the protection of keyword index is tested. Underneath the random oracle model, the ciphertext is tested to be by selection secure. Since the protection within the general cluster model is way weak than in the commonplace model, it's price constructing verifiable and multi-keyword searchable theme within the commonplace model.

6.REFERENCES

[1] D.X. Song, D. Wanger, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," IEEE Symposium on Security & Privacy, Washington, DC, USA: IEEE Computer Society, May 2000, pp. 44-55.

[2] C. Dong, G. Russello, N. Dulay, "Shared and Searchable Encrypted Data for Untrusted Servers," Lecture Notes in Computer Science, Berlin, Germany: Springer, Jul. 2008, pp.127-143

[3] M.Xu and S.Li, "A keyword searchable attribute-based public encryption scheme," Chinese Journal of Computers, vol. 37, no. 5, 1018-1024, Jun. 2014, doi: 10.3724/SP.J.1016.2014.01017.

[4] Y. Ye, J. Han, W. Susilo, T. H. Yuen, and J. Li, " Attribute-Based Keyword Search with Constant-Size Ciphertexts(ABKS-CSC)," Security & Communication Networks, vol. 9, no. 18, pp. 5003-5015, Oct. 2016, doi: org/10.1002/sec.1671.

[5] W. Sun, S. Yu, W. Lou, Y. Hou, and H. Li, "Verifiable Attribute-Based Keyword Search with Fine-Grained OwnerEnforced Search Authorization in the Cloud by Protecting Your Right," IEEE INFOCOM, vol. 27, no. 4, pp. 226-234, Jul. 2014,doi:10.1109/INFOCOM.2014.6847943.

[6] Q. Dong, Z. Guan, and Z. Chen, "Attribute-Based Keyword Search Efficiency Enhancement through an Online/Offline Approach," the 21th IEEE International Conference on Parallel and Distributed Systems, Dec. 2015, pp. 298-305.

[7] Z. Rui, M. Hui, and L. Yao, "Fine-grained access control system based on fully outsourced attribute-based encryption," Journal of Systems and Software, vol. 125, pp. 344-353, Mar. 2017, doi: 10.1016/j.jss.2016.12.018.

[8] B.Waters and A. Sahai, "Fuzzy identity-based encryption," In Advances in Cryptology – EUROCRYPT, Cramer R. Eds. Berlin, Germany: Springer, 2005, pp. 457-473.

[9] O. Pandey ,V. Goyal, B. Waters and A. Sahai" For fine-grained access control of encrypted data by using attribute-based encryption," in Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA: ACM, 2006, pp. 89-98.

[10] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy AttributeBased Encryption," in proc. IEEE Symposium on Security and Privacy, Washington, DC, USA: IEEE Computer Society, May 2007, pp.3213