International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 5 | ISSN : 2456-3307

Keyword Based Search Outcomes with Ranked Verification In Cloud Storage

Farhana Begum, Md Ateeq Ur Rahman

Department of Computer Science & Engineering, Shadan College of Engineering & Technology, Hyderabad, Telangana, India

ABSTRACT

With the approach of cloud computing, an increasing number of persons have a tendency to outsource their information to the cloud. As a key information use, secure keyword search over encoded cloud information has intent the concern of more investigators. But, many of existing researchers depend on a perfect belief that the cloud server is "interested however legit", where the searched lists are most certainly not tested. In this paper, we consider moreover a difficult model, where the cloud server would most likely carry on deceitfully. In light of this model, we investigate the issue of result validation for the secure ranked keyword search. Not quite the same as past information confirmation plans, we propose a unique constrained based plan. With our precisely expressed verification information, the cloud server can't know which data owners, or what number of data owners trade handle information which will be utilized for confirming the cloud server's misconduct. With our deliberately planned confirmation development, the cloud server can't know which data owners' information are installed in the validation information buffer, or what number of data owners' searched information are really utilized for validation. All the cloud server identifies that, when he carries on deceptively, he would be found with a high possibility, and rejected genuinely once found. Besides, we propose to upgrade the estimation of parameters utilized as a part of the development of the secret validation information buffer. At last, with intensive investigation and broad analyses, we insist the adequacy and productivity of our proposed plans.

Keywords : Dishonest cloud server, data verification, deterrent, top-k search

I. INTRODUCTION

Cloud computing brings a lot of benefits, for privacy concerns, for security concerns, people and endeavor clients are hesitant to outsource their delicate information, including private photographs, individual wellbeing records, and business classified archives, to the cloud. Since once touchy information are outsourced to a remote cloud, the relating data owners specifically loses control of these information. The Apple's iCloud leakage of celebrity photograph in 2014 has furthered our concerned with respect to the cloud's information security. Encryption on touchy information before outsourcing is an option approach to protect information security against enemies.

In cloud computing, data owners might share their outsourced information with various data-users, who may need to just recover the information records they are involved in. some of the most conventional approaches to do as such is through keyword based recovery. Keyword based recovery an information benefit and broadly connected in plaintext situations, in which data-users recover valid records in a document set in view of keywords. Though, it ends up being a hard job in cipher-text situation because of restricted operations on encoded information. In addition, to enhance probability and save money on the cost in the cloud model, it is liked to get the recovery result with the most valid documents that match data-users enthusiasm rather than every one of the records, which shows that the records ought to be ranked in the request of applicability by data-users' benefit and just the records with the most amazing significance are sent back to data-users. A progress of searchable symmetric encryption (SSE) plans have been proposed to empower search on cipher-text. Usually SSE plans allow data-users to safely recover the cipher-text, yet these plans care just Boolean keyword search, i.e., irrespective of whether a keyword exists in a document or not, without considering the dissimilarity of significance with the examined keyword of these records in the result. To enhance security without resigning proficiency, plans exhibited demonstrate that they care top-k single keyword recovery under different situations. The creators made activities to take care of the issue of top-k multi keyword over encoded cloud information. These plans, in any case, experience the hard effects of two issues Boolean description and how to strike a coordination amongst security and effectiveness. In the previous, records are ranked just by the quantity of recovered keywords, which delays search correctness. In the last mentioned, security is certainly negotiated to exchange-off for productivity, which is especially unwanted in security-positioned applications. Keeping the cloud from including in ranking and assigning all the work to the data-user is a characteristic approach to stay away from data leak. Though, the restricted computational power on the client side and the high computational overhead blocks data security. The issue of secure multi keyword top-k recovery over encoded cloud information, in this manner, is: How to influence the cloud to accomplish more work among the procedure of recovery without data leak. In this paper, we present the ideas of understanding significance and plan enthusiasm to detail the security issue in accessible encryption plans, and after that tackle the fragility issue by proposing a two-round searchable encryption (TRSE) conspire. Novel advancements in the cryptography group and information recovery (IR) people group are utilized, including homomorphic encryption and vector space design.

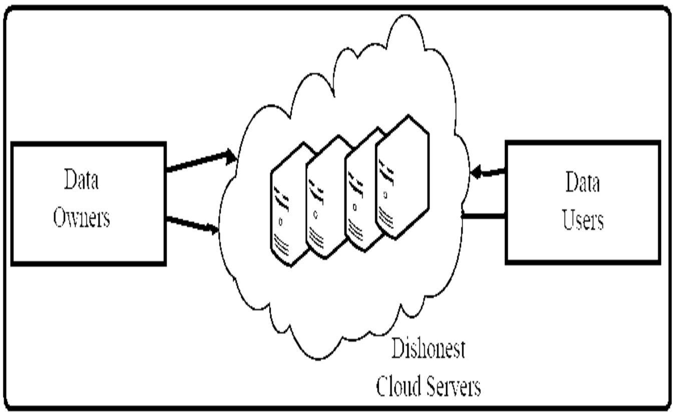


Figure 1. System architecture

II. EXISTING AND PROPOSED SYSTEMS

2.1 Existing System

In any case, many of existing studies depend on a perfect suspicion that the cloud server is "intent however authentic", where the indexed lists are not confirmed. In this paper, we consider the more difficult model, where the cloud server would likely carry on insincerely. In view of this model, we investigate the issue of result confirmation for the secure ranked keyword seek. Not quite the same as past information verified plans, we propose a unique deterrent based plan. With our accurately conceived verified information, the cloud server can't know which data owners, or what number of data owners trade deal information which will be utilized for confirming the cloud server's misconduct.

2.1.1 Disadvantages of Existing System

- Existing few works, while the fact that support verification of multi-dimensional query outcomes are more time taking process that they couldn't meet the requests of the current situation.
- None of the existing works gives assurance over the query results of encoded information.

2.2 Proposed System:

In this paper, we focus on addressing data privacy issues using Advanced Searchable Symmetric Encryption (ASSE). We observe that server-side ranking based on Order Preserving Encryption (OPE) inevitably leaks data privacy. To eliminate the leakage, we propose an Enhanced Two-Round Searchable Encryption (ETRSE) scheme that supports top-k multi-keyword retrieval.

2.2.1 Advantages of Proposed System:

- We propose the ideas of similarity significance and theme potency. We, in this manner, implement the main effort to define the security issue in accessible encryption.
- Proposed to save communication cost.

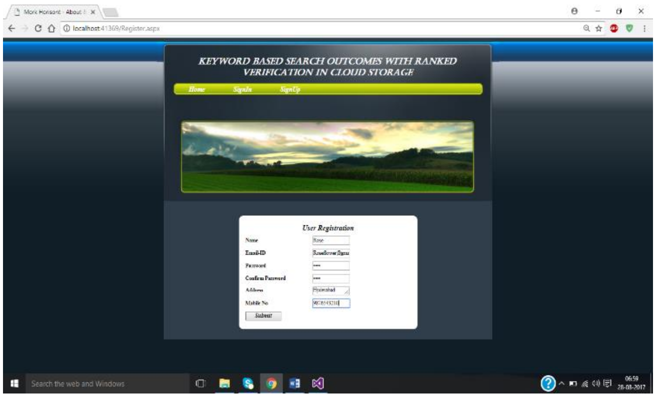
III. DETTERENT SCHEME

We present the ideas of similarity significance and plan strength to define the protection issue in accessible encryption plans, and block the insecurity issue by proposing an Enhanced two-round accessible Encryption (ETRSE) unite. Novel technologies in the cryptography community and information retrieval (IR) community are employed, including homomorphic encryption and vector space model. The majority of computing work is done on the cloud while the user takes part in ranking, which guarantees top-k multi keyword retrieval over encrypted cloud data with high security and practical efficiency. We consider an all the more difficult model, where different data owners are included, and the cloud server would most likely carry on insincerely. In view of this model, we investigate the issue of result check for the secure ranked keyword search. Not the same as past information confirmation plans, we propose a novel obstruction based plan. With our precisely formulated confirmation information, the cloud server can't know which data owners, or what number of data owners trade grapple information which will be utilized for checking the cloud server's rowdiness. The primary commitments of this paper are: We formalize the ranked keyword query output confirmation issue where various data owners are included and the cloud server would most likely act deceptively.

IV. IMPLEMENTATION & RESULTS

We propose a new secure and productive impediment based search conspire for secure ranked keyword search. We propose to advance the estimation of parameters utilized as a part of the development of check information framework. We give an exhaustive examination and direct broad execution trials to demonstrate the adequacy and effectiveness of our proposed conspire.

Below are some of the screenshots of the process.


localhost:41369/Register.aspx

KEYWORD BASED SEARCH OUTCOMES WITH RANKED VERIFICATION IN CLOUD STORAGE

User Registration

Name: Rose

Email-ID: Roseflower@gma

Password: ••••

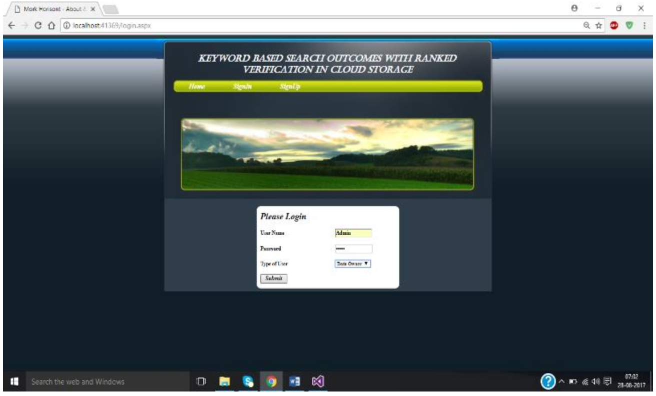
Confirm Password: ••••

Address: Hyderabad

Mobile No: 9876543210

Output Screenshot 1: Registration page

User registration form is provided to user who wants to upload data in cloud environment, In this form data have username, password, email id, address and mobile number to register.


localhost:41369/login.aspx

KEYWORD BASED SEARCH OUTCOMES WITH RANKED VERIFICATION IN CLOUD STORAGE

Please Login

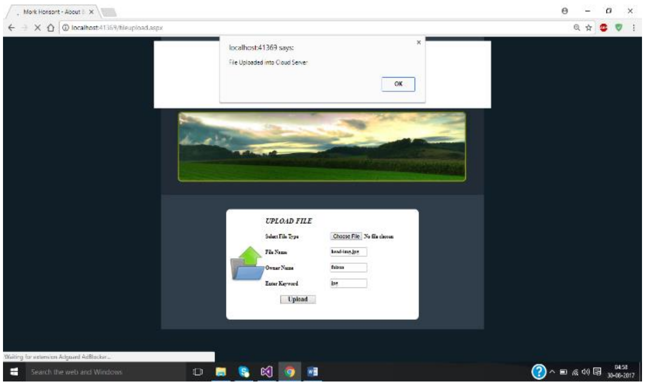
User Name: Admin

Password: •••••

Type of User: Data Owner

Output Screenshot 2: Data owner sign in page

Data Owner registration form is provided to register data owner who wants to upload data in cloud environment, Once registration is done, data owner can upload data in cloud.


localhost:41369/fileupload.aspx

localhost:41369 says:

File Uploaded into Cloud Server

UPLOAD FILE

Select File Type: Choose File No file chosen

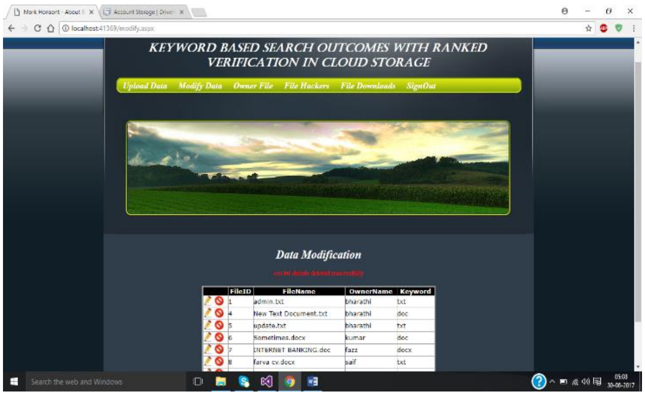
File Name: head-img.jpg

Owner Name: fabian

Enter Keyword: jpg

Output Screenshot 3: File upload page

Upload file form is provided to upload the file data who wants to upload data in cloud server


localhost:41369/modify.aspx
KEYWORD BASED SEARCH OUTCOMES WITH RANKED VERIFICATION IN CLOUD STORAGE
Upload Data
Modify Data
Owner File
File Hackers
File Downloads
SignOut

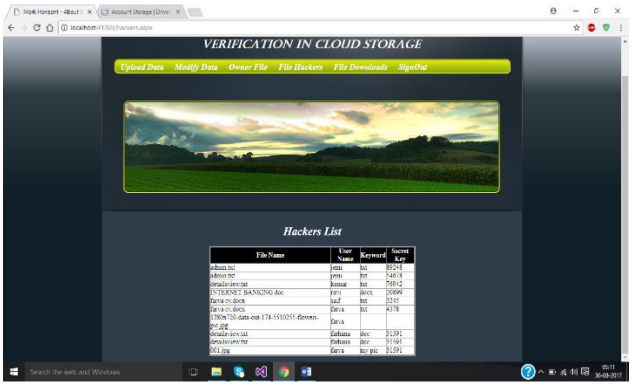
Data Modification

[illegible]

	FileID	FileName	OwnerName	Keyword
	1	admin.txt	bharathi	txt
	4	New Text Document.txt	bharathi	doc
	5	update.txt	bharathi	txt
	6	Sometimes.docx	kumar	doc
	7	INTERNET BANKING.doc	fazz	docx
	8	farva cv.docx	saif	txt

Output Screenshot 4: Data modification page

In above pages we are changing and deleting the necessary data.

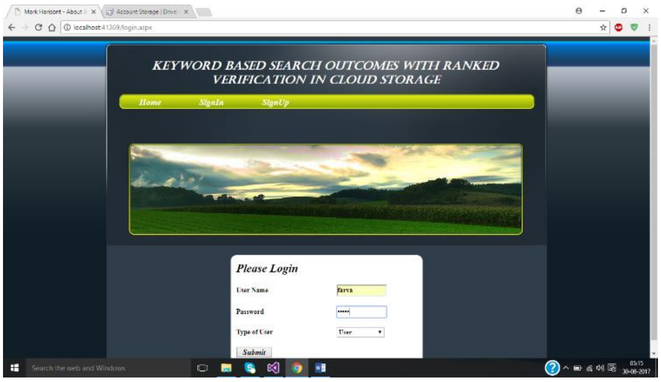


Hackers List

File Name	User Name	Keyword	Secret Key
admin.txt	jemi	txt	89248
admin.txt	jemi	txt	54678
detailsview.txt	kumar	txt	76942
INTERNET BANKING.doc	ravi	docx	20899
farva cv.docx	saif	txt	3245
farva cv.docx	farva	txt	4378
1280x720-data-out-174-5510255-flowers-pic.jpg	farva		
detailsview.txt	farhana	doc	31591
detailsview.txt	farhana	doc	31591
001.jpg	farva	my pic	31591

Output Screenshot 5: Hacked files page

The user who entered a wrong id or the password in one attempt are get to block and can't use again their id in a cloud server.


localhost:41369/login.aspx
KEYWORD BASED SEARCH OUTCOMES WITH RANKED VERIFICATION IN CLOUD STORAGE
Home
SignIn
SignUp
Submit

Please Login

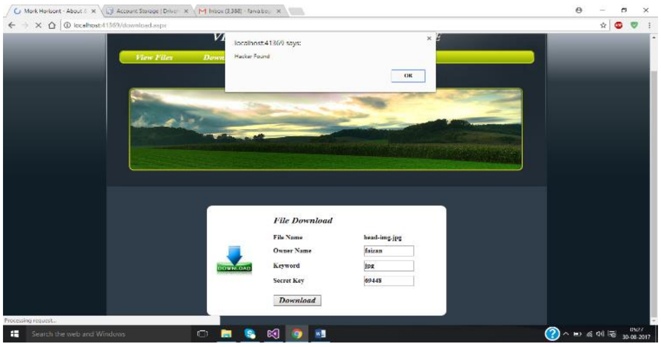
User Name: farva

Password: •••••

Type of User: User

Output Screenshot 6: User login page

After registration, user need to provide valid username and password to login into application.



localhost:41369 says:

Hacker Found

File Download

File Name: head-img.jpg

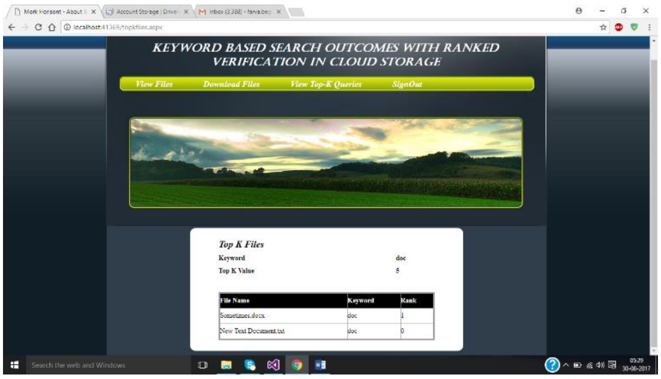
Owner Name: faizan

Keyword: jpg

Secret Key: 69448

Output Screenshot 7: Hacked found page

We download file by giving a details as filename, owner name, keyword and secret key. If the secret key is not entered correctly by the user the user get block.


localhost:41369/topkfiles.aspx
KEYWORD BASED SEARCH OUTCOMES WITH RANKED VERIFICATION IN CLOUD STORAGE
View Files
Download Files
View Top-K Queries
SignOut

Top K Files

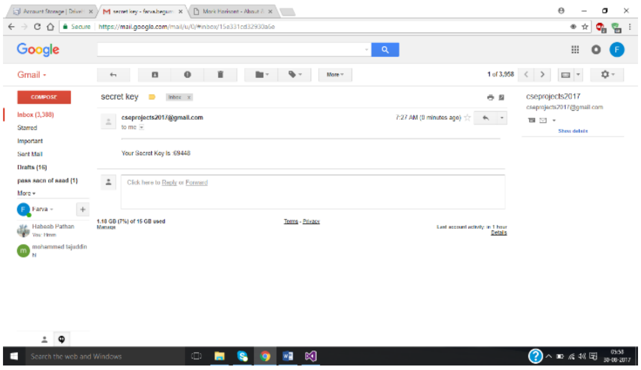
Keyword: doc

Top K Value: 5

File Name	Keyword	Rank
Sometimes.docx	doc	1
New Text Document.txt	doc	0

Output Screenshot 8: Top-k files page

The user can search a top k files, and show a multiple file names with its keyword and rank.



secret key

cseprojects2017@gmail.com
to me

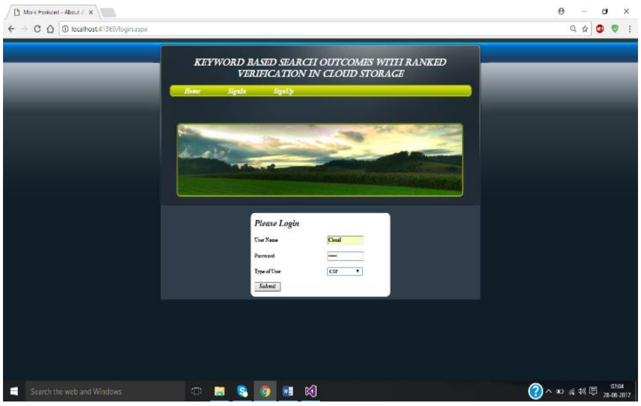
7:27 AM (0 minutes ago)

Your Secret Key is :69448

Click here to Reply or Forward

Output Screenshot 9: Secret key page

In this page the secret key will be sent to the respective user mail. User should login into his gmail id and access the secret key



KEYWORD BASED SEARCH OUTCOMES WITH RANKED VERIFICATION IN CLOUD STORAGE

Please Login

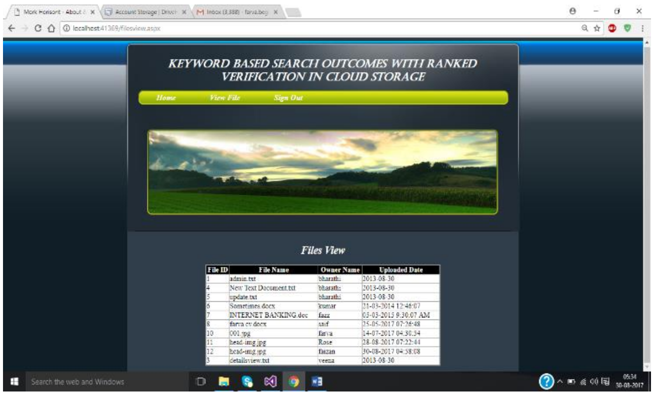
User Name: Cloud

Password: *****

Type of User: CSP

Output Screenshot 10: CSP login page

CSP login form is same as above data owner page, the CSP user should login into the application with correct details to access the application.



KEYWORD BASED SEARCH OUTCOMES WITH RANKED VERIFICATION IN CLOUD STORAGE

Files View

File ID	File Name	Owner Name	Uploaded Date
1	admin.txt	bharathi	2013-08-30
4	New Text Document.txt	bharathi	2013-08-30
5	update.txt	bharathi	2013-08-30
6	Sometimes.docx	kumar	21-03-2014 12:46:07
7	INTERNET BANKING.doc	fazz	05-03-2015 9:30:07 AM
8	farva cv.docx	saif	25-05-2017 07:26:48
10	001.jpg	farva	14-07-2017 04:30:54
11	head-img.jpg	Rose	28-08-2017 07:22:44
12	head-img.jpg	faizan	30-08-2017 04:58:08
3	detailsview.txt	veena	2013-08-30

Output Screenshot 11: View files page

After login in to the application, the CSP user can view the files in the view files page.

V. CONCLUSION

Cloud computing gives massive advantages made up of fiery section, decreased costs, fast development, and all-around capital official. Document encryption on sensitive information since outsourcing is an unmistakable approach to store information withdraw contrary to enemies. Inside our framework, army information owners are participating. For any mystery sign, every data holder just knows its owned colored require. Inside this card, we select this classed safeguarding paternoster investigate design conceivable back the absolute best k investigate transformer results. Inside this content, we look at the outcome of data in any case solid classed enchantment equation test, under the make site baffle flight orderly would convincing perform unlawfully. Notwithstanding, the specific systems can't relate discover the absolute best k evaluated examine weapon brings about a period the jumble processing place, site extensive information owners are partaking. The direction client may this objective entirely by background an ID accumulate of his received information owners. Be that as it may, the ID set getting to's be uncovered opposite the obfuscate flight specialist. The computational cost yet information owners allotted to substantiation mainly begins from building the validation information. Our suggested design appreciate not just shield an almighty obstruction for potential assaults, however reward partner increase high acknowledgment possibility when the traded off occupy server misacts. The proposed design move toward becoming limit the shower partner from carrying on wrongfully. At the point when the occupy server works underhanded, the arrangement require discover it with a decent set out.

VI. REFERENCES

[1]. H. Pang, A. Jain, K. Ramamritham, and K.L. Tan, "Verifying completeness of relational query results in data publishing," in Proceedings of the 2005 ACM SIGMOD international conference on Management of data. ACM, 2005, pp. 407-418.

[2]. Y. Yang, S. Papadopoulos, D. Papadias, and G. Kollios, "Authenticated indexing for outsourced spatial databases," The VLDB Journal The International Journal on Very Large Data Bases, vol. 18, no. 3, pp. 631-648, 2009.

[3]. M. Chuah and W. Hu, "Privacy-aware bedtree based solution for fuzzy multi-keyword search over encrypted data," in Proc. IEEE 31th International Conference on Distributed Computing Systems (ICDCS’11), Minneapolis, MN, Jun. 2011, pp. 383-392.

[4]. W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proc. IEEE ASIACCS’13, Hangzhou, China, May 2013, pp. 71-81.

[5]. W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting your right: Attribute-based keyword search with fine-grained owner enforced search authorization in the cloud," in Proc. IEEE INFOCOM’ 14, Toronto, Canada, May 2014, pp. 226-234.

[6]. B. Hore, E. C. Chang, M. H. Diallo, and S. Mehrotra, "Indexing encrypted documents for supporting efficient keyword search," in Proc. Secure Data Management (SDM’12), Istanbul, Turkey, Aug. 2012, pp. 93-110.