INTERNATIONAL JOURNAL · ENGINEERING RESEARCH ·

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 17th February 2018. Link :

http://www.ijiemr.org/downloads.php?vol=Volume-7&issue=ISSUE-2

Title: A Greedy Depth-First-Search Scheme on Encrypted Data In Cloud Storage.

Volume 07, Issue 02, Page No: 475 - 481

Paper Authors

*** MR. SHAHANSHA SHAIK , MR. NAGARJUNA REDDY.**

* , Dept of CSE, D.V. R College of Engineering And Techonology.

A GREEDY DEPTH-FIRST-SEARCH SCHEME ON ENCRYPTED DATA IN CLOUD STORAGE

***MR. SHAHANSHA SHAIK , **MR. NAGARJUNA REDDY**

,*PG Scholar, Dept of CSE, D.V. R College of Engineering And Techonology(T.S),India.
.**Assistant Professor, Dept of CSE, D.V. R College Of Engineering And Techonology, (T.S),India.

shahanshabtech@gmail.com anr304@gmail.com

ABSTRACT:

Because of the developing ubiquity of distributed computing, an ever increasing number of information proprietors are encouraged to utilize their information to the server for accommodation and decrease information administration costs. In any case, the information should be encoded before giving a workforce to the security prerequisites that ruin information utilize, for example, secret word recuperation. In this article, we introduce a security look through that is ordered as a watchword for scrambled cloud information, bolsters dynamic updates, for example, erasing and embeddings records. In particular, the generally utilized spatial vector and model TF_IDF are joined to plan and define inquiries. We construct unique tree file structures and give the principal seek calculation to characterize various catchphrase looks. The Protected KNOW calculation is utilized to encode the vector of the list and the question and in the meantime gives a legitimate assessment of the pertinence between the encoded list and the asserted vector. To adapt to the assault, motto insights are added to the file vector to look for indexed lists. Because of the utilization of our extraordinary carpentry record structure, the proposed plot accomplishes seek times under transportation and dealing with, erasure, and archive joining adaptably. Propelled tests are being led to show the adequacy of the proposed venture.

Keywords: Searchable encryption, multi-keyword ranked search, dynamic update, cloud computing.

I INTRODUCTION

Cloud computing is using laptop resources, which are supplied as a provider on the internet (generally the net). This call comes from using the cloud image as a down load for complicated infrastructure loaded in the system chart. Cloud computing a depended on service that carries software and records computing facts. Cloud computing has the h/w and s/w for 0.33 birthday party internet control services. Those operations generally provide excessive-level get entry to high-quit programs and servers on the server.

Fig 1: Computer architecture structure in the cloud

Working in Cloud Computing

The purpose of cloud computing is to carry out supercomputing conventional and powerful laptop overall performance, that is extensively used by army and research, billions of 2nd-term programming calculators, together with economic capital for providing awesome personal statistics garage or laptop video games.

Cloud computing team of workers, big server servers normally use low cost computers with specialised links to again up obligations to get admission to statistics in them. The full it infrastructure includes a device of fairly big organizations. Digital techniques are often used to growth laptop power.

Pattern capabilities and services:

The residences of cloud computing primarily based on the definition furnished with the the nist are as follows:

• Self Carrier on Request:

Unanticipated laptop customers can provide capabilities which includes server and community time loads as wished its very own without requiring human dialogue with every person provider.

• Large network get admission to:

Accessibility available on line and accessed through a preferred mechanism that complements the usage of a platform of thinness or thickness of a client.

II.SYSTEM ARCHITECTURE SYSTEM ARCHITECTURE:

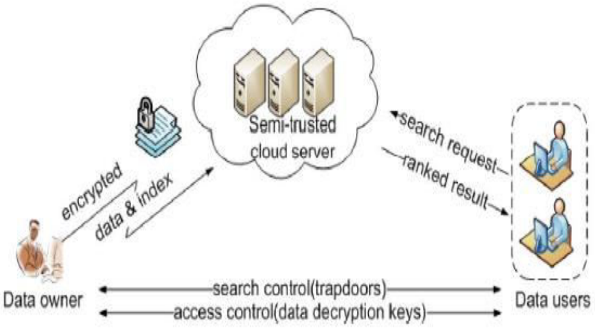

Semi-trusted cloud server
encrypted data & index
search request
ranked result
Data owner
search control(trapdoors)
access control(data decryption keys)
Data users

Fig.2 SYSTEM ARCHITECTURE

Design Goals

To enable secure, efficient, accurate and dynamic multikeyword ranked search over outsourced encrypted cloud data under the above models, our system has the following design goals.

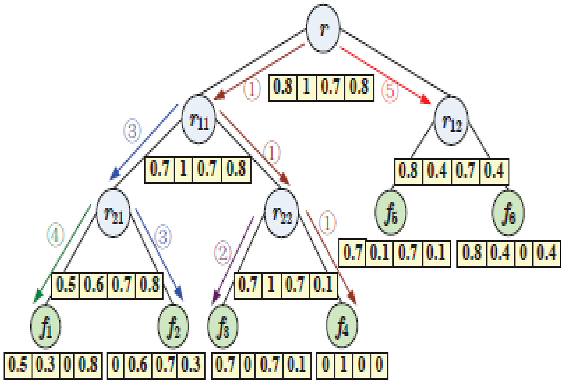


Fig. 3. An example of the tree-based index with the document collection $\mathcal{F} = \{f_i | i = 1, ..., 6\}$ and cardinality of the dictionary $m = 4$. In the construction process of the tree index, we first generate leaf nodes from the documents. Then, the internal tree nodes are generated based on the leaf nodes. This figure also shows an example of search process, in which the query vector Q is equal to $(0, 0.92, 0, 0.38)$. In this example, we set the parameter $k = 3$ with the meaning that three documents will be returned to the user. According to the search algorithm, the search starts with the root node, and reaches the first leaf node f_4 through r_{11} and r_{22}. The relevance score of f_4 to the query is 0.92. After that, the leaf nodes f_3 and f_2 are successively reached with the relevance scores 0.038 and 0.67. Next, the leaf node f_1 is reached with score 0.58 and replace f_3 in $RList$. Finally, the algorithm will try to search subtree rooted by r_{12}, and find that there are no reasonable results in this subtree because the relevance score of r_{12} is 0.52, which is smaller than the smallest relevance score in $RList$.

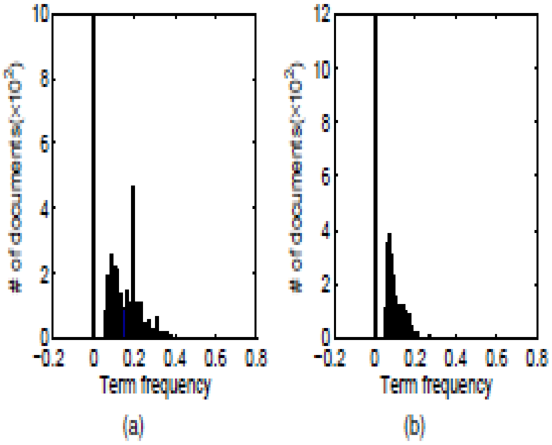
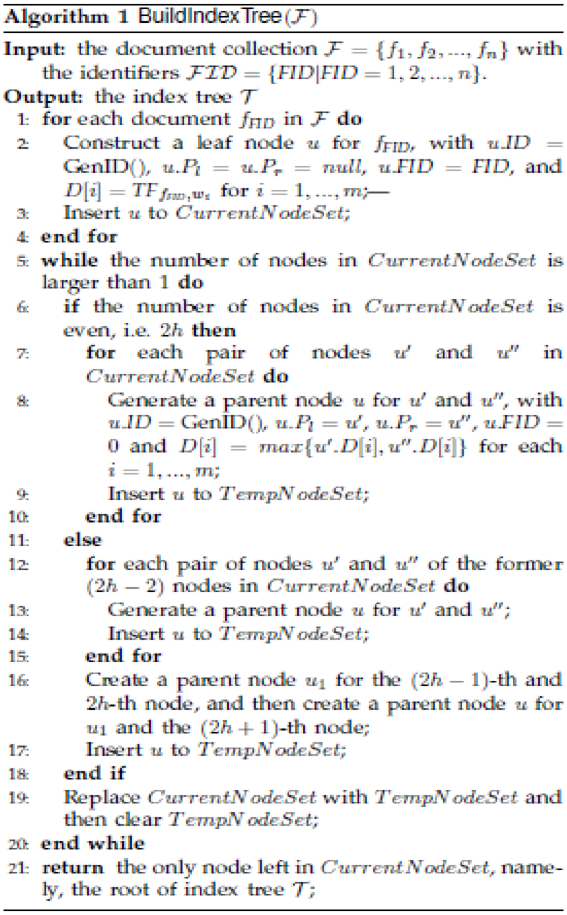
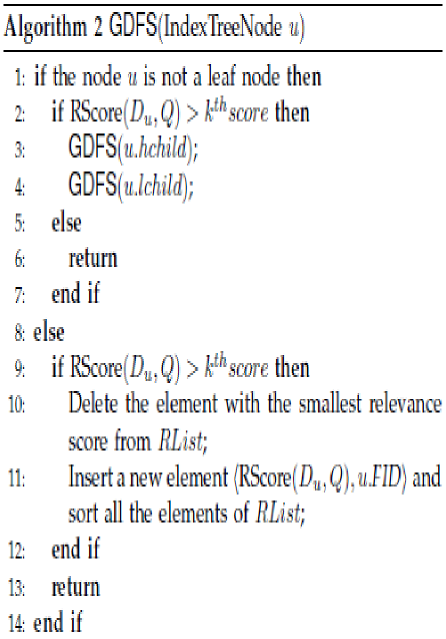


Fig. 4. Distribution of term frequency (TF) for (a) keyword "subnet", and (b) keyword "host".

PROPOSED ALGORITHMS:



```
Algorithm 1 BuildIndexTree($\mathcal{F}$)
Input: the document collection $\mathcal{F} = \{f_1, f_2, ..., f_n\}$ with
    the identifiers $\mathcal{FID} = \{FID|FID = 1, 2, ..., n\}$.
Output: the index tree $\mathcal{T}$
for each document $f_{FID}$ in $\mathcal{F}$ do
    Construct a leaf node $u$ for $f_{FID}$, with $u.ID$ = GenID(), $u.P_l = u.P_r = null$, $u.FID = FID$, and $D[i] = TF_{f_{FID}, w_i}$ for $i = 1, ..., m$;—
    Insert $u$ to $CurrentNodeSet$;
end for
while the number of nodes in $CurrentNodeSet$ is larger than 1 do
    if the number of nodes in $CurrentNodeSet$ is even, i.e. $2h$ then
        for each pair of nodes $u'$ and $u''$ in $CurrentNodeSet$ do
            Generate a parent node $u$ for $u'$ and $u''$, with $u.ID$ = GenID(), $u.P_l = u'$, $u.P_r = u''$, $u.FID = 0$ and $D[i] = max\{u'.D[i], u''.D[i]\}$ for each $i = 1, ..., m$;
            Insert $u$ to $TempNodeSet$;
        end for
    else
        for each pair of nodes $u'$ and $u''$ of the former $(2h - 2)$ nodes in $CurrentNodeSet$ do
            Generate a parent node $u$ for $u'$ and $u''$;
            Insert $u$ to $TempNodeSet$;
        end for
        Create a parent node $u_1$ for the $(2h - 1)$-th and $2h$-th node, and then create a parent node $u$ for $u_1$ and the $(2h + 1)$-th node;
        Insert $u$ to $TempNodeSet$;
    end if
    Replace $CurrentNodeSet$ with $TempNodeSet$ and then clear $TempNodeSet$;
end while
return the only node left in $CurrentNodeSet$, namely, the root of index tree $\mathcal{T}$;
```



```
Algorithm 2 GDFS(IndexTreeNode $u$)
if the node $u$ is not a leaf node then
    if RScore($D_u, Q$) > $k^{th}score$ then
        GDFS($u.hchild$);
        GDFS($u.lchild$);
    else
        return
    end if
else
    if RScore($D_u, Q$) > $k^{th}score$ then
        Delete the element with the smallest relevance score from $RList$;
        Insert a new element (RScore($D_u, Q$), $u.FID$) and sort all the elements of $RList$;
    end if
    return
end if
```

DATA FLOW DIAGRAM:

1. The DFD is moreover called as air pocket graph. it's miles a truthful graphical formalism that speak to a framework as some distance as information records to the framework, extraordinary dealing with finished in this facts, and the yield information is created by means of this framework.

2. The records circulation chart (DFD) is a vital displaying gadgets. It is applied to demonstrate the framework components. Those elements are the framework process, the data utilized by the process, an out of doors substance that cooperates with the framework and the facts streams within the framework.

3. DFD shows how the information travels via the framework and how it's miles changed by a progression of adjustments. It's far a graphical method that delineates statistics movement and the modifications which might be related as statistics movements from contribution to yield.

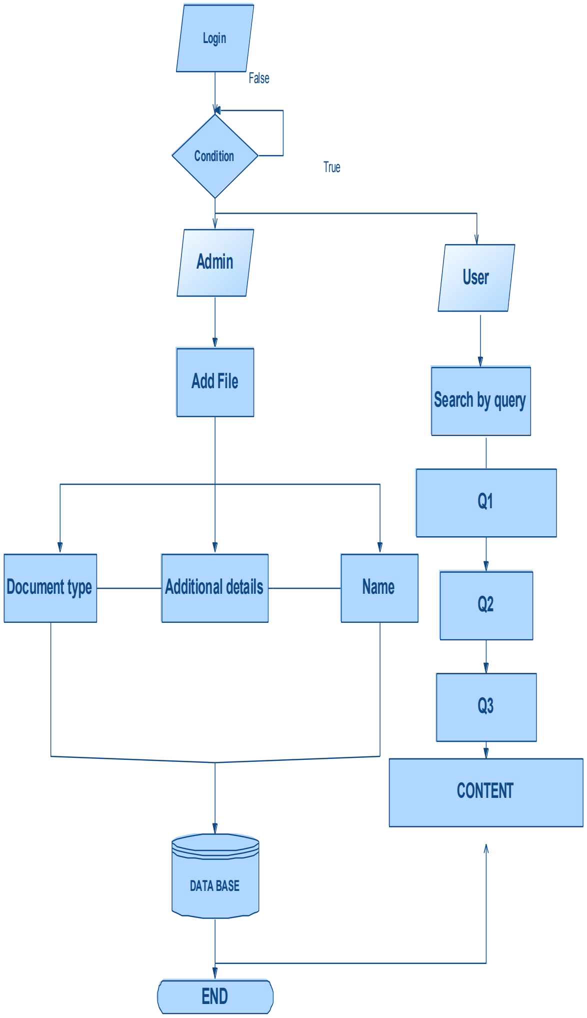


Fig.5: DATA FLOW DIAGRAM

III IMPLEMENTATION

1 MODULES:

1.Cloud

2.Group Manager

3.Group Member

4.File Security

5.Group Signature

6. User

MODULES DESCRIPTION:

1.Cloud :

In this module, we make a neighbourhood cloud and give estimated bottomless capability administrations. The clients can switch their information within the cloud. We build up this module, wherein the allotted garage may be made relaxed. Be that as it could, the cloud is not completely relied on by clients because the CSPS are likely going to be outdoor of the cloud customers' confided in space. This is the cloud server won't vindictively erase or alter patron information due to the insurance of data analyzing plans, yet will try to take inside the substance of the placed away statistics and the characters of cloud clients.

2.Group Manager Module :

Group manager takes charge of followings:
1. System parameters generation,
2. User registration,
3. Consumer revocation, and
4. Revealing the real identity of a dispute facts proprietor.

In the end, we take delivery of that the collection administrator is absolutely depended on with the change gatherings. the organization supervisor is the administrator. the collection supervisor has the logs of every ultimate process in the cloud. the gathering administrator is in fee of consumer enlistment and moreover patron disavowal as nicely.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

3. Group Member Module:

Amassing people are an arrangement of enlisted clients so one can

1. Store their private data into the cloud server and
2. Percentage them with others inside the accumulating.

Word that, the gathering enrolment is regularly changed, due to the body of workers abdication and new worker cooperation within the organization. The gathering component has the responsibility for the information within the accumulating. Whoever within the amassing can see the records which are transferred of their gathering and moreover exchange it?

4. File Security Module:

1. Scrambling the records file.
2. Report put away inside the cloud can be erased by either the collection director or the data owner.

(i.e., the element that transferred the record into the server).

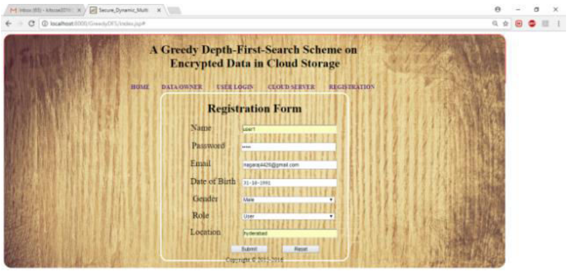
5. Group Signature Module:

A meeting mark conspire allows any individual from the gathering to signal messages even as keeping the person mystery from verifiers. In addition, the assigned amassing administrator can uncover the character of the mark's originator when a question occurs, that's indicated as traceability.

6. User Module:

Patron denial is achieved with the collection manager via an open handy repudiation list (rl), in light of which bunch people can scramble their information files and guarantee the type towards the renounced customers.

IV RESULTS

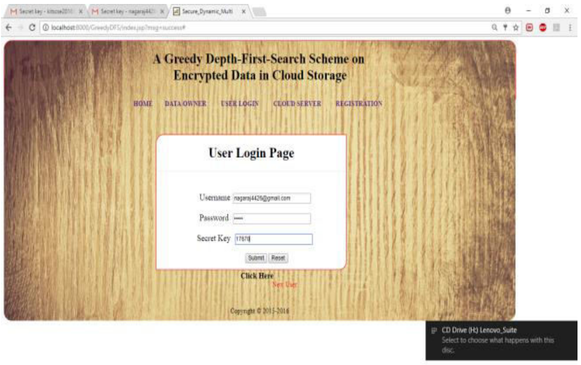


A Greedy Depth-First-Search Scheme on Encrypted Data in Cloud Storage

Registration Form

Name: user1
Password: •••••
Email: nagaraj4426@gmail.com
Date of Birth: 31-10-1991
Gender: Male
Role: User
Location: hyderabad

Copyright © 2015-2016



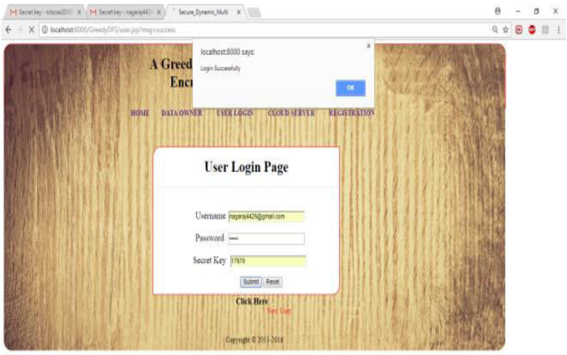
A Greedy Depth-First-Search Scheme on Encrypted Data in Cloud Storage

User Login Page

Username: nagaraj4426@gmail.com
Password: •••••
Secret Key: 17670

Copyright © 2015-2016

CD Drive (H:) Lenovo_Suite
Select to choose what happens with this disc.

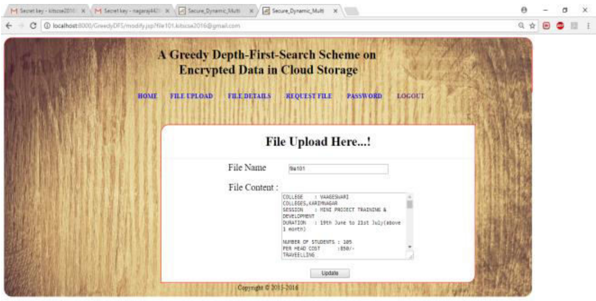


localhost:8000 says:
Login Successfully

User Login Page

Username: nagaraj4426@gmail.com
Password: •••••
Secret Key: 17670

Copyright © 2015-2016



A Greedy Depth-First-Search Scheme on Encrypted Data in Cloud Storage

File Upload Here...!

File Name: file101

File Content :

```
COLLEGE     : VAAGESWARI
COLLEGES,KARIMNAGAR
SESSION     : MINI PROJECT TRAINING &
DEVELOPMENT
DURATION    : 19th June to 21st July(above
1 month)

NUMBER OF STUDENTS : 105
PER HEAD COST      :850/-
TRAVEELLING
```

Copyright © 2015-2016

V CONCLUSION

This text presents a at ease and powerful safe search scheme that not best helps correct seek with many keywords, however additionally deletes dynamics and record insertion. We create binary key-word key phrases particularly listed and offer first-intensity understanding algorithms for higher results than linear seek. Additionally, a concurrent seek system can be carried out less time beyond regulation prices. The security of this scheme is covered towards threat model the usage of a included KNN set of rules. The experimental results display the efficient of the proposed scheme. There are nonetheless many demanding situations in the symmetric se venture. Within the requested scheme, the priority of the data is accountable for producing update data and for sending it to the server. Consequently, the statistics proprietor need to keep the tree of the unencrypted index and the facts had to re-calculate the fee of the IDF. Users of such active facts won't be appropriate for cloud models. It may be a meaningful, but tough-to-locate, future virtual encoding scheme that can be terminated via a cloud server, however continues the potential to preserve track of multiple key-word searches. Similarly, because maximum encryption is sought, our schema focuses on server challenges. in truth, there are some qualities in many user initiatives. First, all customers continually support the identical security key to create a trap in a symbolic ce plot. In this case, user cancellation is a extraordinary undertaking. If you want to revoke a person on this scheme, we want to restore the index and distribute new protection keys to all legal users. 2nd, the symmetric se scheme is commonly everyday that every one records customers can be trusted. This isn't an apparent and irregular user of the records in an effort to result in specific troubles. as an instance, customers with unjustified information can search for files and distribute decrypted documents into unauthorized files. Further, unfair consumer data may also distribute its safety key to unauthorized users. in destiny work, we can try to improve the ce challenge to deal with these challenges.

VI REFERENCES

[1] Ok. wang et al. , "public security demanding situations" ieee internet computing, vol. sixteen, no. page 1 page sixty nine-seventy three, 2012.

[2] s. kamara and ok. lautter, "clone cloud storage", in financial cryptography and statistics security. springer 2010, pp. 136-149.

[3] S. gentry, "homomorphic complete encryption scheme" stanford university, 2009

[4] O. goldreich and r. ostrovsky, "program safety and fraud of rams unknown" acm magazine (jacm), vol. forty three, no. three pages. 431-473, 1996.

[5] D. boneh, g. crescenzo, ostrovsky and persian persian "with public keyword encryption".

[6] D. boneh, e kushilevitz, ostrovsky and w. w. skeith iii "encrypted with a public key, selecting fake questions," in evolution cryptology-crypto 2007, springer, 2007, pp. 50-67.

[7] E. d. and wagner perigot, "unique technology for encrypting information restoration," in the 2000 "s & p 2000" safety and exclusive "manufacturing and protection." ieee convention 2000. ieee 2000, forty four-55.

AUTHORS

Mr. NAGARJUNA REDDY, B.Tech (CSE) M.Tech (CSE) is having 13+ years of relevant work experience in Academics, Teaching, and Controller of Examinations. At present, he is working as an Associate Professor, In-charge of M.Tech CSE Dept, D.V.R college of engineering and techonology(T.S),INDIA,and utilizing his teaching skills, knowledge, experience and talent to achieve the goals and objectives of the Engineering College in the fullest perspective. He has attended seminars and workshops. He has also guided 25 post graduate students. His areas of interest Data Mining, Data Warehousing, Network security, Data Structures through C Language & Cloud Computing.

Mr. SHAHANSHA SHAIK, PG scholar Dept of CSE, D.V.R college of engineering and techonology(T.S),INDIA, **B.Tech** degree in Computer Sciense Engineering at Loyola Institute Of Technology And Management(T.S).