Catching the Misbehavior of the Cloud using Ranked Keyword Search

[1]C. Reddineelima, [2]P. Hemavathi, [3]K. Sadasiva, [4]S.Lavanya, [5]V. Swathi

[1]Assistant Professor, [2,3,4,5]B.Tech Students
Computer Science and Engineering,
Mother Theresa Institute of Engineering and Technology, Palamaner, Chittoor(A.P),India

***Abstract*—With the introduction of cloud computing, more and more people tend to store their data in the cloud. Initially, secure keyword search over encrypted cloud data has attracted many researchers recently. Whereas most of recent researches are based on an assumption that the cloud server is honest, where the search results are not verified. Here, we consider a model, where the cloud server may behave dishonestly. Based on this model, we explore the problem of result verification for the secure ranked keyword search. How many data owners exchange their data that is used for verifying the cloud server's misbehavior or which data owners are involved is not known to the cloud server. And also by our verification the cloud server cannot know which data owners' data are embedded in the verification data, or how many data owners' verification data are actually used for verification. Once cloud server behaves dishonestly, he should be discovered with a high probability, and punished seriously once discovered. Further, we propose to minimize the value of parameters used in the secret verification.**

***Index Terms*—Cloud computing, dishonest cloud server, data verification.**

I. INTRODUCTION

Cloud computing is defined as using the computing resources (hardware and software) that are delivered to user as a service on request over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

Services Models:

Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. Cloud provides tremendous benefits including easy access, decreased costs, quick deployment, and flexible resource management . Enterprises of all sizes can leverage the cloud to increase innovation and collaboration. Although cloud computing brings a lot of benefits, for privacy concerns, individuals and enterprise users are reluctant to outsource their sensitive data, including private photos, personal health records, and commercial confidential documents, to the cloud. Because once sensitive data are outsourced to a remote cloud, the corresponding data owner directly loses control of these data. The Apple's iCloud leakage of celebrity photo in 2014 has furthered our concern regarding the cloud's data security. Encryption on sensitive data before outsourcing is an alternative way to preserve data privacy against adversaries. However, data encryption becomes an obstacle to the utilization of traditional applications, e.g., plaintext based keyword search. To achieve efficient data retrieval from encrypted data, many researchers have recently put efforts on secure keyword search over encrypted data. A compromised cloud server would return false search results to data users for various reasons: 1) The cloud server may return forged search results. 2) The cloud server may return incomplete search results in peak hours to avoid suffering from performance bottlenecks. There are some researches that focus on search results verification. However, these methods cannot be applied to verify the top-k ranked search results in the cloud computing environment, where numerous data owners are involved. The Data owners encrypts their files and provide an index value to the file along with the verification data and upload it into the cloud server. Trapdoor is generated to user on requesting the cloud server by the Data user. File decryption keys are exchanges between the data owner and data user.

For file encryption and decryption, AES (Advanced Encryption Standards) algorithm is implemented here. The pseudo code for AES key Expansion is given below.

```
KeyExpansion(byte key[16], word w[44])
 {
   word temp
      for(i = 0; i < 4; i + +)
        w[i] = (key[4*i], key[4*i + 1], key[4*i + 2], key[4*i + 3]);
     for(i = 4; i < 44; i + +)
  {
    temp = w[i – 1];
```

```
        if ( i mod 4 = 0)
            temp = SubWord(RotWord(temp)) ⊕ Rcon[i/4];
            w[i] = w[i-4] ⊕ temp
  }
}
```

To generate the Trapdoor, MD5 algorithm is implemented here.

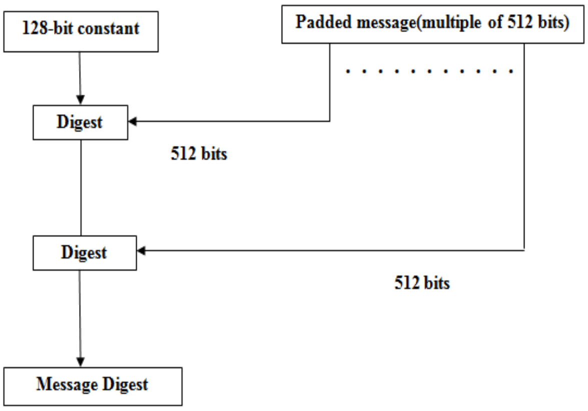


Fig. 1: Structure of MD5 Algorithm

II. PROPOSED SYSTEM :

There are many instances where the cloud server probably misbehave an misuse the user data. Based on this problem we proposed system which provide high security for the user data. Here the user uploads his files by encrypting them. Thereby generating a trapdoor for his file to provide much security. If the user suspects the cloud server as dishonest then he can perform a secret verification. This verification scheme is different from other as it involves secure ranked keyword search. By our verification the cloud server cannot know which data owners' data are embedded in the verification data, or how many data owners' verification data are actually used for verification.

III. SYSTEM ARCHITECTURE:

The system architecture consists of data owner, cloud server and the data user. The functionality of each module is explained here. The cloud server may be honest or dishonest. Based on the cloud server behavior we can decide whether verification should be performed or not

Data Owners:

Data owner uploads files into the cloud server which can be verified and deleted by the data owner. They extracts keywords from his file collection and constructs He exchanges these file IDs and relevance scores as anchor data with other data owners uniformly at random.

Data Users:

Authorized data user wants to perform a ranked (top-*k*) secure keyword search over these encrypted files, he first generates his trapdoor (encrypted keyword) by requesting the cloud server and submits it to the cloud server. After Server Response, authorized data user decrypts his search results

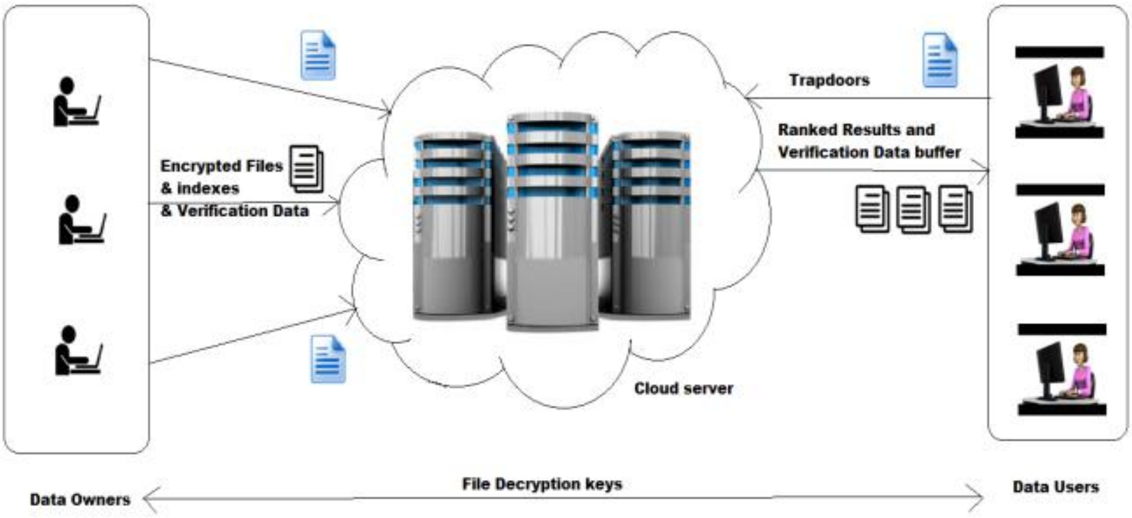


Fig. 2: Architecture of verifying secure ranked keyword search result in cloud computing

Cloud Server:

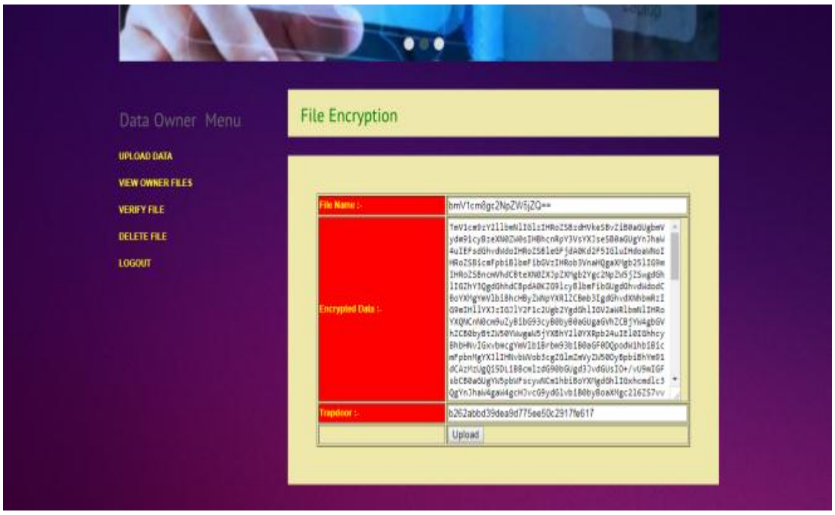
Each data owner outsources his encrypted files to the cloud server. On receiving the search request from user, the cloud server searches locally and returns the top-*k* relevant data files. The authorized data user decrypts his search results. He sends the trapdoor and secret key as response to the data user.

Verification:

A data user can verify the correctness of search results belonging to a specific data owner. The encryption of the string is used as each owner's verification data. Data users construct a verification request, and indicate the size of verification data buffer. Cloud server operates on the encrypted data and returns the verification data. Finally, data users decrypt the returned search results and verify whether misbehavior occurs.

IV. RESULTS

During the whole process of verification, the cloud server only conducts computation on cipher-texts. Therefore, he does not know how many data owners' verification data are actually used for verification, or which data owners' data are embedded in the verification data buffer.



File Name :- bmV1cm8gc2NpZW5jZQ==

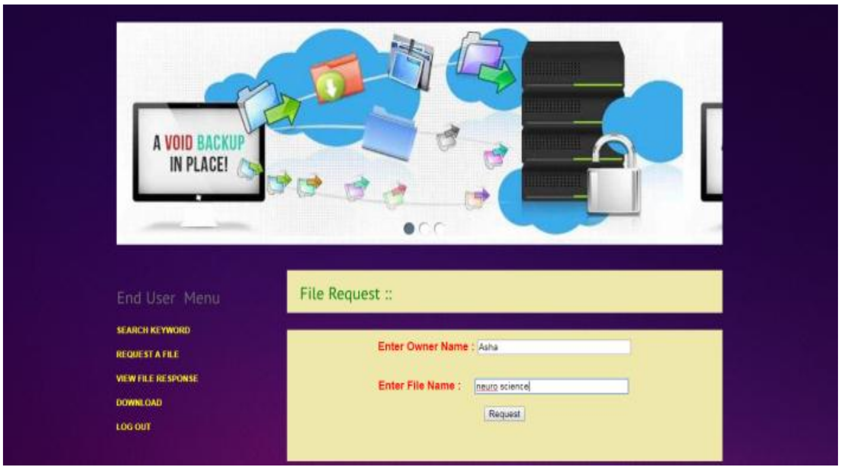
Encrypted Data :-

```
TmV1cm9zY2llbmNlIGlzIHRoZSBzdHVkeSBvZiB0aGUgbmV
ydm91cyBzeXN0ZW0sIHBhcnRpY3VsYXJseSB0aGUgYnJhaW
4uIEFsdGhvdWdoIHRoZSBleGFjdA0Kd2F5IGluIHdoaWNoI
HRoZSBicmFpbiBlbmFibGVzIHRob3VnaHQgaXMgb25lIG9m
IHRoZSBncmVhdCBteXN0ZXJpZXMgb2Ygc2NpZW5jZSwgdGh
lIGZhY3QgdGhhdCBpdA0KZG9lcyBlbmFibGUgdGhvdWdodC
BoYXMgYmVlbiBhcHByZWNpYXRlZCBmb3IgdGhvdXNhbmRzI
G9mIHllYXJzIGJlY2F1c2Ugb2YgdGhlIGV2aWRlbmNlIHRo
YXQNCnN0cm9uZyBibG93cyB0byB0aGUgaGVhZCBjYW4gbGV
hZCB0byBtZW50YWwgaW5jYXBhY2l0YXRpb24uIEl0IGhhcy
BhbHNvIGxvbmcgYmVlbiBrbm93biB0aGF0DQpodW1hbiBic
mFpbnMgYXJlIHNvbWVob3cgZGlmZmVyZW50DyBpbiBhYW91
dCAzMzUgQ1SDL1B0cmlzdG90bGUgd3JvdGUsIO+/vU9mIGF
sbCB0aGUgYW5pbWFscywNCm1hbiBoYXMgdGhlIGxhcmdlc3
QgYnJhaW4gaW4gcHJvcG9ydGlvbiB0byBoaXMgc2l6ZS7vv
```

Trapdoor :- b262abbd39dea9d775ee50c2917fe617

Fig. 4: Encrypted data of the data owner to upload a file into the cloud server.

The data owner uploads his file into the cloud server. Before uploading the file data owner encrypts his file using an encryption algorithm and cloud server provide a trapdoor to ensure security for owner file. The above fig.4 shows the encrypted data of the file with a trapdoor.



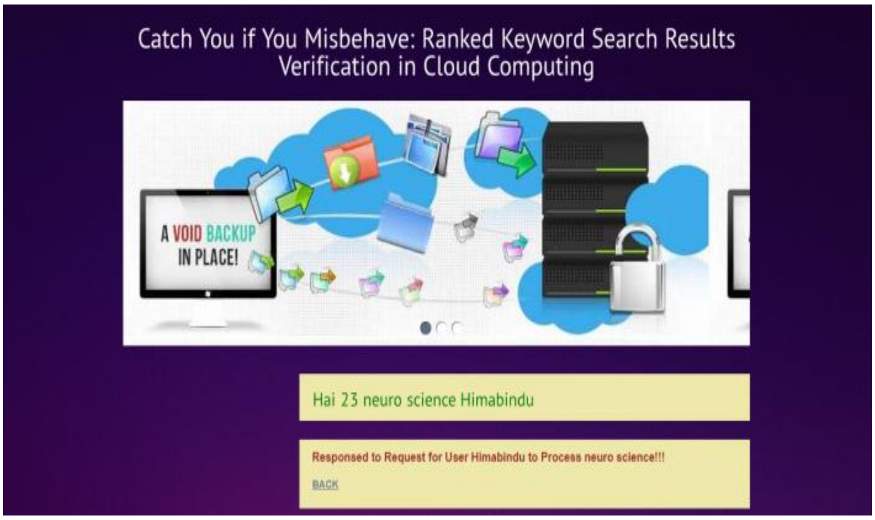
File Request ::

Enter Owner Name : Asha

Enter File Name : neuro science

Fig. 5: Requesting a File by Data user.

To download a file from the cloud server the data user should first search the file in the cloud using a keyword. If the files related to the user keyword is present then cloud sends the owner details to user and then the user request the file by owner name and file name as shown in above fig.5.



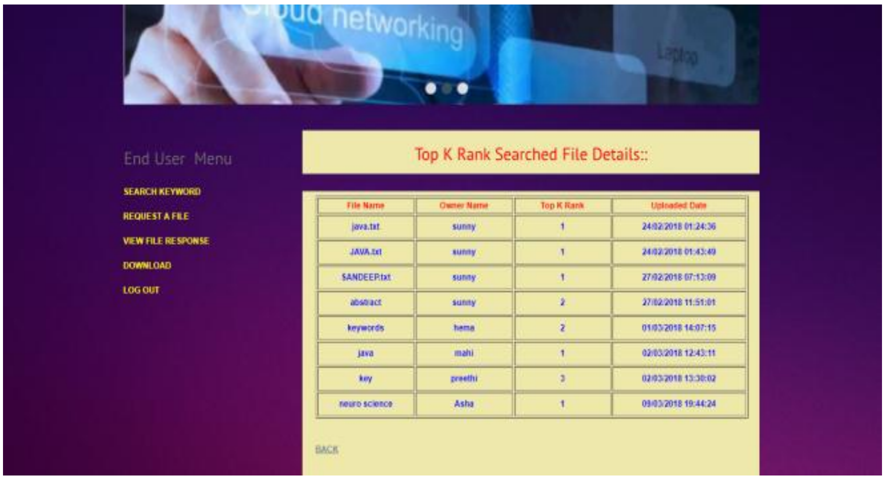
Catch You if You Misbehave: Ranked Keyword Search Results Verification in Cloud Computing

Hai 23 neuro science Himabindu

Responsed to Request for User Himabindu to Process neuro science!!!

Fig. 6: File response send to cloud server.

Once the request is send to the cloud server by the user the response is created by cloud by proccesing the request.

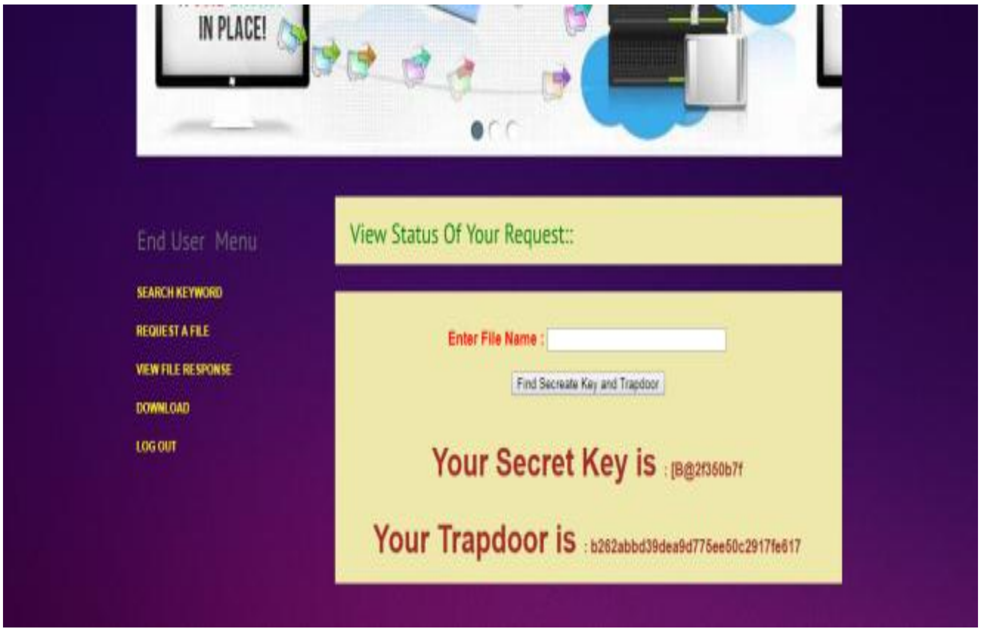


Top K Rank Searched File Details::

File Name	Owner Name	Top K Rank	Uploaded Date
java.txt	sunny	1	24/02/2018 01:24:36
JAVA.txt	sunny	1	24/02/2018 01:43:49
SANDEEP.txt	sunny	1	27/02/2018 07:13:09
abstract	sunny	2	27/02/2018 11:51:01
keywords	hema	2	01/03/2018 14:07:15
java	mahi	1	02/03/2018 12:43:11
key	preethi	3	02/03/2018 13:30:02
neuro science	Asha	1	09/03/2018 19:44:24

Fig. 7: Top-K ranked files.

The cloud server can view the top-K ranked files. Rank is given to each file based on the no. of downloads.



View Status Of Your Request::

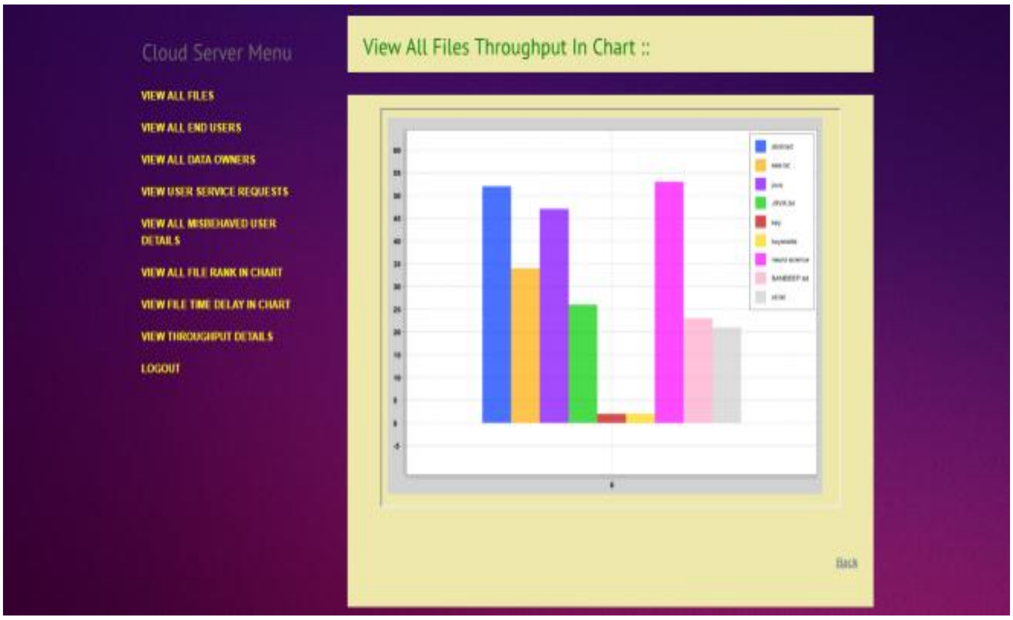
Enter File Name :

Your Secret Key is : [B@2f350b7f

Your Trapdoor is : b262abbd39dea9d775ee50c2917fe617

Fig. 8: Trapdoor and Secret Key generated by cloud server to download files.

The data owner after receiving the response from the cloud server he can download the file by using the secret key and Trapdoor which is provided by the cloud. Without using this secret key and trapdoor if user tries to download then cloud recognize the user as misbehaved user.


Cloud Server Menu
VIEW ALL FILES
VIEW ALL END USERS
VIEW ALL DATA OWNERS
VIEW USER SERVICE REQUESTS
VIEW ALL MISBEHAVED USER DETAILS
VIEW ALL FILE RANK IN CHART
VIEW FILE TIME DELAY IN CHART
VIEW THROUGHPUT DETAILS
LOGOUT
Back

View All Files Throughput In Chart ::

Fig. 9: Through-put generated for files in cloud server.

Here we can view the through-put of the downloaded files using the graphs for each file that is uploaded in cloud server.

V. CONCLUSION:

Verification for the secure ranked keyword search was performed, where cloud servers would probably behave dishonestly. During the whole process of verification, the cloud server is not clear of which data owners, or how many data owners exchange anchor data used for verification, he also does not know which data owners' data are embedded in the verification data buffer or how many data owners'. When any action is detected as suspicious, data owners can dynamically update the verification data stored on the cloud server. The files uploaded to the cloud are encrypted so it provide much security for user files and it is impossible to misbehave here.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A view of cloud computing,” *Communication of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[2] C. Zhu, V. Leung, X. Hu, L. Shu, and L. T. Yang, “A review of key issues that concern the feasibility of mobile cloud computing,” in *Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing*. IEEE, 2013, pp. 769–776.

[3] Ritz, “Vulnerable icloud may be the reason to celebrity photo leak.” [Online]. Available: http://marcritz.com/icloud-flaw-leak/ encrypted cloud data,” in *Proc. IEEE INFOCOM’11*, Shanghai, China, Apr. 2011, pp. 829–837.

[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] A. Ibrahim, H. Jin, A. A. Yassin, and D. Zou, “Secure rank ordered search of multi-keyword trapdoor over encrypted cloud data,” in *Proc. IEEE Asia-Pacific Conference on Services Computing (APSCC’12)*, Guilin, China, Dec. 2012, pp. 263–270.

[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.

[7] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, “Fuzzy keyword search over encrypted data in cloud computing,” in *Proc. IEEE INFOCOM’10*, San Diego, CA, Mar. 2010, pp. 1–5.

[8] W. Zhang, Y. Lin, S. Xiao, Q. Liu, and T. Zhou, “Secure distributed keyword search in multiple clouds,” in *Proc. IEEE/ACM IWQOS’14*, Hongkong, May 2014, pp. 370–379.

[9] Q. Chen, H. Hu, and J. Xu, “Authenticating top-k queries in location-based services with confidentiality,” *Proceedings of the VLDB Endowment*, vol. 7, no. 1, 2013.[28] H. Hu, J. Xu, Q. Chen, and Z. Yang, “Authenticating location based services without compromising location privacy,” in *Proceedings of the 2012 ACM SIGMOD International Conference on Management of Data*. ACM, 2012, pp. 301–312.

[10] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. Hou, and H. Li, “Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking,” *TPDS*, 2013.

[11] Q. Chen, H. Hu, and J. Xu, “Authenticating top-k queries in location-based services with confidentiality,” *Proceedings of the VLDB Endowment*, vol. 7, no. 1, 2013.