International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Verification of Ranked Keyword Search in Cloud Computing

Monika Patil[1], S. V. Bodake[2]

[1, 2]Department of Computer Engineering, PVPIT College of Engineering, Bavdhan Pune

Abstract: ***In the recent era of cloud computing, Many people move towards the outsource their information to the cloud. As a fundamental data use, secure keyword search over encrypted cloud data has attracted the interest of many researchers recently .This is the reason researchers assume that the cloud server is curious and honest ,where the search results are not confirmed .In this paper we describe that if cloud server misbehave and working dishonestly then catch them. Base on this model, we investigate the issue of result verification for the secure ranked keyword search. Not the same as past information verification schemes, we propose a novel obstacle based scheme. With our carefully devised verification data, the cloud server can't know which data owner, or what number of data owner exchange anchor data which will be utilized for verifying the cloud server's misbehavior .With our methodically designed verification construction, the cloud server can't know which Data Owner data are embedded in the verification data buffer, or what no of Data Owner's verification data are really utilized for verification. All cloud server knows that, if he acts dishonestly at number of times then he must be punished. we propose to optimize the estimation of parameters utilized as a part of the development of the secret verification data buffer At last, with careful investigation and extensive experiments, we confirm the accuracy and efficiency of our proposed schemes.***

Keywords: Cloud computing, dishonest cloud server, data verification, deterrent

1. Introduction

With the advent of cloud computing, more and more people tend to outsource their data to the cloud. Cloud computing provides tremendous benefits including easy access, decreased costs, quick deployment, and flexible resource management Most of existing researches are based on an ideal assumption that the cloud server is “curious but honest” Secure keyword search over encrypted cloud data has attracted the interest of many researchers recently. As it is a believed that Cloud server will never misbehave but sometimes it can. Existing schemes share a common assumption, i.e., data owners foresee the order of search results. However, in practical applications, numerous data owners are involved; each data owner only knows its own partial order. Without knowing the total order, these data owners cannot use the conventional schemes to verify the search results. A compromised cloud server would return false search results to data users for various reasons; the cloud server may return forged search results. For example, the cloud may rank an advertisement higher than others, since the cloud can profit from it, or the cloud would return random large files to earn money, since the cloud adopts the ‘pay as you consume’ model. The cloud server may return incomplete search results in peak hours to avoid suffering from performance bottlenecks.

2. Literature Survey

[1] Secure ranked keyword search over encrypted cloud data:
Traditional searchable encryption schemes allow users to securely search over encrypted data through keywords, these techniques support only boolean search, without capturing any relevance of data files. This approach suffers from two main drawbacks when directly applied in the context of Cloud Computing. On the one hand, users, who do not necessarily have pre-knowledge of the encrypted cloud data, have to post process every retrieved file in order to find ones most matching their interest; On the other hand, invariably retrieving all files containing the queried keyword further incurs unnecessary network traffic, which is absolutely undesirable in today’s pay-as-you-use cloud paradigm. To solve the problem of effective yet secure ranked keyword search over encrypted cloud data is proposed. Ranked search greatly enhances system usability .

[2] Fuzzy keyword search over encrypted data in cloud computing:
Traditional searchable encryption schemes allow a user to securely search over encrypted data through keywords and selectively retrieve files of interest, these techniques support only exact keyword search. This paper formalized and solve the problem of effective fuzzy keyword search over encrypted cloud data while maintaining keyword privacy. Fuzzy keyword search greatly enhances system usability by returning the matching files when users’ searching inputs exactly match the predefined keywords or the closest possible matching files based on keyword similarity semantics, when exact match fails.

[3] Efficient multi-keyword ranked query on encrypted data in the cloud:
In order to protect the data privacy, sensitive data is usually encrypted before outsourced to the cloud server, which makes the search technologies on plaintext unusable. This model propose a multi-keyword ranked search scheme over the encrypted cloud data, which simultaneously meets a set of strict privacy requirements.

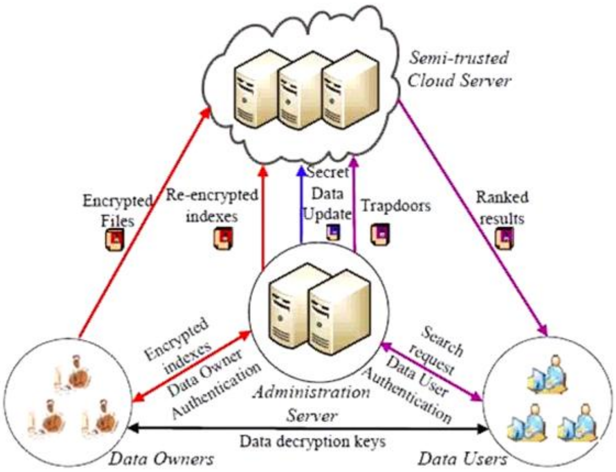
[4] Privacy-preserving multi keyword fuzzy search over encrypted data in the cloud:
Enabling keyword search directly over encrypted data is a desirable technique for effective utilization of encrypted data

outsourced to the cloud. Existing solutions provide multi keyword exact search that does not tolerate keyword spelling error, or single keyword fuzzy search that tolerates typos to certain extent. The current fuzzy search schemes rely on building an expanded index that covers possible keyword misspelling, which lead to significantly larger index file size and higher search complexity. The proposed scheme achieves fuzzy matching through algorithmic design rather than expanding the index file. It also eliminates the need of a predefined dictionary and effectively supports multiple keyword fuzzy search without increasing the index or search complexity.

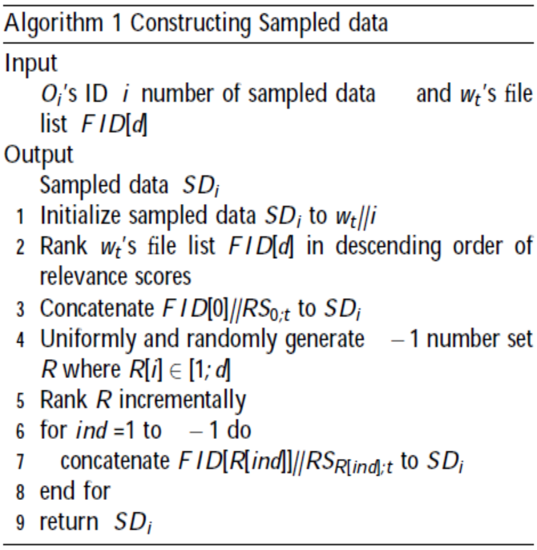
3. Proposed System

Proposed scheme allow data owners to construct the verification data efficiently. The cloud server should also return the verification data without introducing heavy costs. Additionally, data users can verify the search result efficiently. Deter the cloud server from behaving dishonestly. Once the cloud server behaves dishonestly, the scheme should detect it with a high probability.

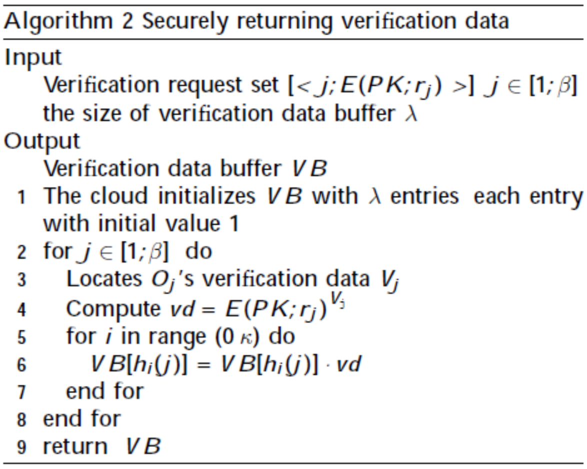
4. System Architecture



5. Algorithm



```
Algorithm 1 Constructing Sampled data
Input
    $O_i$'s ID  $i$  number of sampled data     and $w_t$'s file list  $FID[d]$
Output
    Sampled data  $SD_i$
Initialize sampled data $SD_i$ to $w_t||i$
Rank $w_t$'s file list $FID[d]$ in descending order of relevance scores
Concatenate $FID[0]||RS_{0;t}$ to $SD_i$
Uniformly and randomly generate   $-1$ number set $R$ where $R[i] \in [1; d]$
Rank $R$ incrementally
for $ind$ =1 to   $-1$ do
    concatenate $FID[R[ind]]||RS_{R[ind];t}$ to $SD_i$
end for
return  $SD_i$
```



```
Algorithm 2 Securely returning verification data
Input
    Verification request set $[< j; E(PK; r_j) >]$ $j \in [1; \beta]$
    the size of verification data buffer $\lambda$
Output
    Verification data buffer $VB$
The cloud initializes $VB$ with $\lambda$ entries  each entry with initial value 1
for $j \in [1; \beta]$  do
    Locates $O_j$'s verification data $V_j$
    Compute $vd = E(PK; r_j)^{V_j}$
    for $i$ in range (0 $\kappa$) do
        $VB[h_i(j)] = VB[h_i(j)] \cdot vd$
    end for
end for
return  $VB$
```

6. Mathematical Model

S is the system
S= {I, O, F, K, Success, Failure}

Where,
I = Set of Input
I={I1, I2, I3}
Where,

I1=Login user ID
I2=Login password
I3=File
I4=Keyword to search
I5=Remark
K= Secret key

O=Set of Outputs
O= {O1, O2, O3, O4, O5}
Where,
O1=Authentication Message
O2=Encrypted File
O3= Search result
O4= Verification result
O5= Remark the cloud

F=Set of Functions
F={F1, F2, F3, F4,F5}

Where,
F1=Authentication
O1←F1(I1, I2)

F2=Encryption
O2←F2(I3,K)

F3= Search files based on keyword
O3←F3(I4)

F4= Result of verification
O4←F4(O3)
F5= Cloud behavior

O5←F5(I5)
Success=

1) Authentication successful.
2) Application start.
3) Encrypt the data.
4) Return the result based on keywords.
5) Owner verified the data and provide data to user.
Failure=
1) Authentication failed.
2) Application not started.
3) Doesn’t give the result.
4) Owner doesn’t verify the data.

7. Conclusion

In this paper, we explore the problem of verification for the secure ranked keyword search, under the model where cloud servers would probably behave dishonestly. Different from previous data verification schemes, we propose a novel deterrent-based scheme. 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' verification data are actually used for verification. All the cloud server knows is that, once he behaves dishonestly, he would be discovered with a high probability, and punished seriously once discovered. Additionally, when any suspicious action is detected, data owners can dynamically update the verification data stored on the cloud server. Furthermore, our proposed scheme allows the data users to control the communication cost for the verification according to their preferences, which is especially important for the resource limited data users. Finally, with thorough analysis and extensive experiments, we confirm the efficacy and efficiency of our proposed schemes.

References

[1] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data, ” in Proc. IEEE Distributed Computing Systems (ICDCS’10), Genoa, Italy, Jun. 2010, pp. 253– 262.

[2] Q. Zheng , S. Xu, and G. Ateniese, “Vabks: Verifiable attributebased keyword search over outsourced encrypted data, ” in Proc. IEEE INFOCOM’14, Toronto, Canada, May 2014, pp. 522–530.

[3] Z. Xu, W. Kang, R. Li, K. Yow, and C. Xu, “Efficient multi-keyword ranked query on encrypted data in the cloud, ” in Proc. IEEE Parallel and Distributed Systems (ICPADS’12), Singapore, Dec. 2012, pp. 244–251.

[4] 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.

[5] B. Wang, S. Yu, W. Lou, and Y. T. Hou, “Privacy-preserving multi keyword fuzzy search over encrypted data in the cloud, ” in IEEE INFOCOM, Toronto, Canada, May 2014, pp. 2112–2120.

[6] 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.

[7] 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.

[8] Ritz, “Vulnerable icloud may be the reason to celebrity photo leak. ” [Online]. Available: http: //marcritz. com/icloud-flaw-leak/

[9] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data, ” in Proc. IEEE Distributed Computing Systems (ICDCS’10), Genoa, Italy, Jun. 2010, pp. 253– 262.

[10] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted cloud data, ” in Proc. IEEE INFOCOM’11, Shanghai, China, Apr. 2011, pp. 829–837.

[11] 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.