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

COPY RIGHT

ELSEVIER
SSRN

IJIEMR Transactions, online available on 6th Mar 2018. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-03

Title: EFFICIENT FILE SEARCH OVER ENCRYPTED CLOUD DATA

Volume 08, Issue 03, Pages: 27–30.

Paper Authors

MR.C.RAVI KISHORE REDDY, M.SRILAKSHMI
Vignan's Lara Institute of Technology & Science

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

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

EFFICIENT FILE SEARCH OVER ENCRYPTED CLOUD DATA

MR.C.RAVI KISHORE REDDY[1], M.SRILAKSHMI[2]

Assistant Professor[1], Department of M.C.A, Vignan's Lara Institute of Technology & Science

M.C.A Student[2],Department of M.C.A,Vignan's Lara Institute of Technology & Science

Abstract: In first, most of the existing schemes only consider the scenario with the single data owner. Second, they need secure channels to guarantee the secure transmission of secret keys from the data owner to data users. Third, in some schemes, the data owner should be online to help data users when data users intend to perform the search, which is inconvenient. Searchable encryption allows cloud users to outsource the massive encrypted data to the remote cloud and to search over the data without revealing the sensitive information. Many schemes have been proposed to support the keyword search in a public cloud. However, they have some potential limitations. To enable users to quickly sort out the information of interests from large encrypted data, searchable encryption has been proposed and enriched by many schemes. Instead of decrypting the whole data, these schemes allow users to search over the encrypted data and only decrypt the corresponding files. Searchable encryption schemes have been proposed to solve the problems caused when the data owner shares the data with multiple users.

Introduction

Cloud computing has promoted the success of big data applications such as medical data analyses. With the abundant resources provisioned by cloud platforms, the QoS (quality of service) of services that process big data could be boosted significantly. However, due to unstable network or fake advertisement, the QoS published by service providers is not always trusted. Therefore, it becomes a necessity to evaluate the service quality in a trustable way, based on the services' historical QoS records. However, the evaluation efficiency would be low and cannot meet users' quick response requirement, if all the records of a service are recruited for quality evaluation.Moreover, it may lead to 'Lagging Effect' or low evaluation accuracy, if all the records are treated equally, as the invocation contexts of different records are not exactly the same. In view of these challenges, a novel approach named Partial-HR (Partial Index Terms—big data, cloud, context-aware service evaluation, historical QoS record, weight Historical Records-based service evaluation approach) is put forward in this paper. In Partial-HR, each historical QoS record is weighted based on its service invocation context. Afterwards, only partial important records are employed for quality evaluation. Finally, a group of experiments are deployed to validate the feasibility of our proposal, in terms of evaluation accuracy and efficiency.The existing work either only considers partial context elements, or lacks quantitative weight model for historical QoS records. Therefore, it becomes a challenging task to develop a quantitative weight model that

considers all the context elements, for evaluating the quality of big data services accurately and efficiently. In view of this challenge, a novel service evaluation approach Partial-HR is proposed in this paper. Partial-HR not only considers all the important context elements of service invocation (i.e., invocation time, input size and user location), but also satisfies the Volatility Effect and Marginal Utility. Through Partial-HR, we can select partial important historical QoS records for service evaluation, so that the evaluation accuracy and efficiency could be improved. Through a set of experiments, we validate the feasibility of our proposal.In cloud environment, the advertised QoS information of big data services is not always trusted. Therefore, it becomes a necessity to evaluate the service quality based on historical QoS records. Today, many researchers have studied this problem and given their proposals. In the problem of QoS credibility is firstly put forward, and the historical QoS records are suggested to be considered for evaluating the real quality of service. In the literature the service's QoS credibility is calculated, by comparing the historical QoS data with the SLA (Service Level Agreement) promised by service providers. Afterwards, it became popular to utilize the historical QoS records of services for various trustable service-oriented applications, such as service recommendation, service evaluation, service selection and service composition. However, in the above literatures, the weight problem of different historical QoS records is discussed.Due to the unstable network or fake advertisement, the QoS information of services that process big data in cloud, is not always trustable as advertised by service providers. Therefore, it becomes a necessity to evaluate the service quality in a trustable way, based on the historical QoS records. However, it may lead to low efficiency if all the records are considered in service quality evaluation. Moreover, evaluation accuracy would be low if all the historical QoS records are treated equally, as their service invocation contexts are not exactly the same. In view of these challenges, a novel evaluation approach named Partial-HR is proposed in this paper, which not only considers the service invocation context, but also satisfies 'Volatility Effect' and 'Marginal Utility' simultaneously. Through a set of experiments, we validate the feasibility of Partial-HR in terms of evaluation accuracy and efficiency. In the future, we will introduce more context elements into our weight model for historical QoS records, so as to further improve the evaluation accuracy of big data ser-vices in cloud.

Existing system:

In existing system, most of the existing schemes only consider the scenario of a single data owner. Rather than only one data owner, most cloud providers in reality serve multiple data owners who are able to share their data with each other. Since the data sharing is becoming increasingly important on the user side, how to let data users quickly and securely find out the information of interests from multiple data owners' data becomes a challenge problem. Due to the massive transmissions of secret

keys, it is not reasonable to directly extend the existing schemes from one data owner to multiple data owners.

Proposed system

In this paper, we propose a novel searchable scheme which supports the multi-owner keyword search without secure channels. More than that, our scheme is a non-interactive solution, in which all the users only need to communicate with the cloud server. Furthermore, the analysis proves that our scheme can guarantee the security even without secure channels. Unlike most existing public key encryption based searchable schemes, we evaluate the performance of our scheme, which shows that our scheme is practical. We provide secure and privacy-preserving access control to users, which guarantees any member in group to anonymously utilize the cloud resource. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur.

Modules:

- Group Manager Module
- Group Member Module
- Cloud Module
- Admin Module

1. Group Manager Module:

(a). In our scheme, we consider that the manager is an initiator who creates a group.

(b). The manager takes charge of the group management, including adding a new user and removing a revoked user.

(c). Each user in the group is considered as an authorized user, which means that the user simultaneously plays two roles: a data owner and a data user. As a data owner, the user can share his encrypted data with other authorized users in the group.

2. Group Member Module:

(a). As a data user, the user can search over the encrypted data of others in the group. After the manager permits a new user to join the group, the new user needs to upload the public key to the cloud server.

(b). Then the manager publishes a notification to the cloud server, which informs each authorized user to download the public key of the new user and generate a re-encryption key for the new user.

(c). After that, the new user can enjoy searching over the encrypted data of others in the group.

3. Cloud Module:

(a). The rapid growth of cloud users has affirmed that cloud storage services are becoming the inseparable part of people's life.

(b). Despite of the removal of secure channels, these solutions are still far from being deployed in a real public cloud. Most cloud providers in reality serve multiple data owners who are able to share their data with each other.

(c). the cryptographic primitive called proxy re-encryption is utilized to help data owners delegate the ability of search to data users via the cloud server, without revealing any additional information.

4. Admin Module:

(a). User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and

ensure the confidentiality against the revoked users.

ALGORITHM

1. **SKE.Gen** (1k) →K: Inputs a security parameter 1k, the key generation algorithm **SKE.Gen** outputs a key K.

2. **SKE.Enc** (K, m) →c: Inputs a key K and a message m, the encryption algorithm **SKE.Enc**outputs a ciphertext.
3. **SKE.Dec** (K, c) →m: Inputs a key K and a ciphertext$c$, the decryption algorithm **SKE.Dec**outputs a message.

Conclusion:

In this paper, we propose a novel public key based keyword search scheme, which supports multi-owner keyword search without secure channels. Moreover, our scheme supports non-interactivity, which means that each data owner and data user in the group can complete his individual tasks without interacting with each other. Instead, each of users in the group only needs to interact with the cloud server. Furthermore, although the removal of secure channels, our scheme can still guarantee the secure keyword search, which will not reveal any additional information to the cloud server nor the eavesdropper. Finally, the experimental results demonstrate that our scheme is an efficient public key based solution.

References

[1] W.H Sun, W.J Lou, Y.T Hou, and H Li, "Privacy-preserving keyword search over encrypted data in cloud computing," in Secure Cloud

[2] D.X Song, D Wagner, and A Perrig, "Practical techniques for searches on encrypted data," in
Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 44–55.

[3] D Boneh, C.G DI, R Ostrovksy, and G Persiano,"Public key encryption with keyword search," in Advances in Cryptology-Eurocrypt 2004.Springer, 2004, pp. 506–522.

[4] R Curtmola, J Garay, S Kamara, and R Ostrovsky,"Searchable symmetric encryption: improved definitions and efficient constructions," in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006,pp. 79–88.

[5] J Li, Q Wang, C Wang, N Cao, K Ren, and W.J Lou, "Fuzzy keyword search over encrypteddata in cloud computing." in Computer Communications (INFOCOM), IEEE, 2010, pp. 1-5.