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

ABSTRACT

- With the advent of cloud computing, more and more people tend to outsource their data to the cloud.
- As a fundamental data utilization, secure keyword search over encrypted cloud data has attracted the interest of many researchers recently.
- However, most of existing researches are based on an ideal assumption that the cloud server is “curious but honest”, where the search results are not verified.
- In this paper, we consider a more challenging model, where the cloud server would probably behave dishonestly.

CONTINUE

- Based on this model, we explore the problem of result verification for the secure ranked keyword search.
- Different from previous data verification schemes, we propose a novel deterrent-based scheme.
- With our carefully devised verification data, the cloud server cannot know which data owners, or how many data owners exchange anchor data which will be used for verifying the cloud server's misbehavior.
- With our systematically designed verification construction, the cloud server cannot know which data owners' data are embedded in the verification data buffer, or how many data owners' verification data are actually used for verification.

CONTINUE

- All the cloud server knows is that, once he behaves dishonestly, he would be discovered with a high probability, and punished seriously once discovered.
- Furthermore, we propose to optimize the value of parameters used in the construction of the secret verification data buffer.

EXISTING SYSTEM

- 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.
- With the advent of cloud computing, more and more people tend to outsource their data to the cloud.
- As a fundamental data utilization, secure keyword search over encrypted cloud data has attracted the interest of many researchers recently.

CONTINUE

- However, most of existing researches are based on an ideal assumption that the cloud server is “curious but honest”, where the search results are not verified.

PROPOSED SYSTEM

- In this paper, we consider a more challenging model, where the cloud server would probably behave dishonestly.
- Based on this model, we explore the problem of result verification for the secure ranked keyword search. Different from previous data verification schemes, we propose a novel deterrent-based scheme.
- With our carefully devised verification data, the cloud server cannot know which data owners, or how many data owners exchange anchor data which will be used for verifying the cloud server's misbehavior.

CONTINUE

- With our systematically designed verification construction, the cloud server cannot know which data owners' data are embedded in then 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.
- Furthermore, we propose to optimize the value of parameters used in the construction of the secret verification data buffer.

HARDWARE REQUIREMENTS

- Processor - Pentium –III
- Speed - 1.1 Ghz
- RAM - 256 MB(min)
- Hard Disk - 20 GB
- Floppy Drive - 1.44 MB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

SOFTWARE REQUIREMENTS

- Operating System : Windows 8
- Front End : Java /DOTNET
- Database : Mysql/HEIDISQL

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.

CONTINUE

- 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.

REFERENCE

[1] 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.

[2] 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.

[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.

CONTINUE

[4] 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.

[5] 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.