Efficient Retrieval over Documents Encrypted by Attributes in Cloud Computing

ABSTRACT

- Secure document storage and retrieval is one of the hottest research directions in cloud computing.
- Though many searchable encryption schemes have been proposed, few of them support efficient retrieval over the documents which are encrypted based on their attributes.
- In this paper, a hierarchical attribute-based encryption scheme is first designed for a document collection.
- A set of documents can be encrypted together if they share an integrated access structure.
- Compared with the ciphertext-policy attribute-based encryption (CP-ABE) schemes, both the ciphertext storage space and time costs of encryption/decryption are saved.

CONTINUE

- Then, an index structure named attribute-based retrieval features (ARF) tree is constructed for the document collection based on the TF-IDF model and the documents' attributes.
- A depth-first search algorithm for the ARF tree is designed to improve the search efficiency which can be further improved by parallel computing.
- Except for the document collections, our scheme can be also applied to other datasets by modifying the ARF tree slightly.

EXISTING SYSTEM

- Secure document storage and retrieval is one of the hottest research directions in cloud computing.
- Though many searchable encryption schemes have been proposed, few of them support efficient retrieval over the documents which are encrypted based on their attributes.
- MORE and more people and enterprises are motivated to outsource their local document management systems to the cloud which is a promising information technique (IT) to process the explosive expanding of data.

CONTINUE

- Cloud computing can collect and reorganize a huge amount of IT resources and apparently, the cloud servers can provide more secure, flexible, various, economic and personalized services compared with the local servers.
- A huge challenge of outsourcing the data to the cloud is how to protect the confidentiality of the data properly while maintaining their searchability .

PROPOSED SYSTEM

- A practical hierarchical attribute-based document collection encryption scheme is proposed in which the documents are organized and controlled based on attributes. The proposed scheme can greatly decrease the storage and computing burdens.
- We map the documents to vectors in which both the keywords and associated attributes are considered. The ARF tree is proposed to organize the document vectors and support time-efficient document retrieval. In addition, a depth-first search algorithm is designed.

CONTINUE

- A thorough simulation is performed to illustrate the security, efficiency and effectiveness of our scheme.
- Specifically, the proposed encryption scheme performs very well in both time and storage efficiency.

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 consider a new encrypted document retrieval scenario in which the data owner wants to control the documents in fine-grained level.
- To support this service, we first design a novel hierarchical attribute-based document encryption scheme to encrypt a set of documents together that share an integrated access structure.
- Further, the ARF tree is proposed to organize the document vectors based on their similarities.

CONTINUE

- At last, a depth-first search algorithm is designed to improve the search efficiency for the data users which is extremely important for large document collections.

REFERENCE

[1] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” IEEE Internet Computing, vol. 16, pp. 69–73, Jan. 2012.

[2] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Security and Privacy, 2000. SandP 2000. Proceedings. 2000 IEEE Symposium on, pp. 0–44, 2002.

[3] E. J. Goh, “Secure indexes,” Cryptology ePrint Archive, http:// eprint.iacr.org/2003/216., 2003.

CONTINUE

[4] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: improved definitions and efficient constructions,” in ACM Conference on Computer and Communications Security, pp. 79– 88, 2006.

[5] J. Li, Y. Shi, and Y. Zhang, “Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage,” International Journal of Communication Systems, vol. 30, no. 1, 2017.

[6] Y. Miao, J. Ma, X. Liu, X. Li, Q. Jiang, and J. Zhang, “Attributebased keyword search over hierarchical data in cloud computing,” IEEE Transactions on Services Computing, vol. PP, no. 99, pp. 1–1, 2017.