A Key-Policy Attribute-Based Temporary Keyword Search scheme for Secure Cloud Storage

ABSTRACT

- Today, cloud computing plays an important role in our daily life, because it provides efficient, reliable and scalable resources for data storage and computational activities at a very low price.
- The cloud providers are not fully trusted. So, it is necessary to outsource data in the encrypted form.
- In the attribute-based keyword search (ABKS) schemes, the authorized users can generate some search tokens and send them to the cloud for running the search operation.
- These search tokens can be used to extract all the cipher texts which are produced at any time and contain the corresponding keyword.

CONTINUE

- Since this may lead to some information leakage, it is more secure to propose a scheme in which the search tokens can only extract the cipher texts generated in a specified time interval.
- In this paper, we introduce a new cryptographic primitive called key-policy attribute-based temporary keyword search (KPABTKS) which provide this property.
- we formally prove that our proposed scheme achieves the keyword secrecy property and is secure against selectively chosen keyword attack (SCKA) both in the random oracle model and under the hardness of Decisional Bilinear Diffie-Hellman (DBDH) assumption.

EXISTING SYSTEM

- The cloud providers are not fully trusted. So, it is necessary to outsource data in the encrypted form.
- In the attribute-based keyword search (ABKS) schemes, the authorized users can generate some search tokens and send them to the cloud for running the search operation.
- These search tokens can be used to extract all the cipher texts which are produced at any time and contain the corresponding keyword.
- Since this may lead to some information leakage, it is more secure to propose a scheme in which the search tokens can only extract the cipher texts generated in a specified time interval.

DISADVANTAGES

- Information leakage is occurred .
- It have less secure.
- Execution Time is high

PROPOSED SYSTEM

- We introduce the novel notion of KP-ABTKS, and propose a concrete construction for this new cryptographic primitive which can be applied in the cloud storage services.
- The proposed concrete scheme is designed based on bilinear pairing. In the proposed KP-ABTKS, each user is identified with an access control policy.
- We formally define two security definitions for KPABTKS in the standard model. One of them defines its security against selectively chosen keyword attack (KPABTKS-SCKA), and the other one defines the keyword secrecy of KP-ABTKS.

CONTINUE

- We evaluate the performance of the proposed construction of KP-ABTKS in terms of both computational complexity and the execution time. The performance evaluation shows the practical aspects of our proposal.

ADVANTAGES

- Each data user can generate a search token which is valid only for a limited time interval.
- It provides more security and no data are leaked.
- Efficiently retrieve the search data.

SYSTEM REQUIREMENTS

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

SYSTEM REQUIREMENTS

SOFTWARE REQUIREMENTS

- Operating System : Windows95/98/2000/XP
- Application Server : Tomcat5.0/6.X
- Front End : HTML, Java, Jsp
- Scripts : JavaScript.
- Server side Script : Java Server Pages.
- Database : Mysql

CONCLUSION

- Securing cloud storage is an important problem in cloud computing. We addressed this issue and introduced the notion of key-policy attribute-based temporary keyword search (KPABTKS).
- According to this notion, each data user can generate a search token which is valid only for a limited time interval. We proposed the first concrete construction for this new cryptographic primitive based on bilinear map. We formallyshowed that our scheme is provably secure in the random oracle model.
- The complexity of encryption algorithm of our proposal is linear with respect to the number of the involved attributes.

REFERENCE

[1] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology-Eurocrypt 2004. Springer, 2004, pp. 506–522.

[2] Q. Zheng, S. Xu, and G. Ateniese, "Vabks: Verifiable attribute-based keyword search over outsourced encrypted data," in INFOCOM, 2014 Proceedings IEEE. IEEE, 2014, pp. 522–530.

[3] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology EUROCRYPT 2005. Springer, 2005, pp. 457–473.

[8] E.-J. Goh et al., "Secure indexes." IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.